

Práctica 4

Gestión de Redes

Gestión segura y Documentación e Informes

- Cuanto más grande es una red más compleja es su gestión por ello se hace necesario implementar mecanismos de gestión lo más automatizados posibles de modo que mediante autenticación previa y con un mínimo número de cambios en los dispositivos y archivos de configuración se pueda acceder y volcar dicha información vía FTP y/o TFTP.
- Es necesario realizar *logs* de todas las tareas de gestión y configuración de los dispositivos.
- Hay disponibles distintos protocolos para realizar las tareas de monitorización entre ellos SNMP.
- Mediante SNMP podemos gestionar dispositivos remotamente.
- Cuando se gestiona y *loguea* información hay dos vías
 - OOB (Fuera de Banda): En este caso la información fluye a través de una red de gestión dedicada en la cual no hay tráfico de producción.
 - En Banda: La información fluye a través de la red de producción, internet o ambos canales.

Gestión segura y Documentación e Informes (y II)

- En el caso de OOB el servidor de terminal se conecta a todos los dispositivos a través de los puertos de consola de cada dispositivo gestionado y monitorizado.
- En el caso “En Banda” si el trafico fluye por Internet es necesario filtrar y cifrar la información.
- Gestión OOB:
 - Es apropiada para grandes empresas.
 - Proporciona altos niveles de seguridad
- En cuanto a la modalidad “En Banda”:
 - Se suele emplear en redes pequeñas.
 - Para garantizar la seguridad, se emplean los protocolos IPsec SSH y SSL cuando es posible.

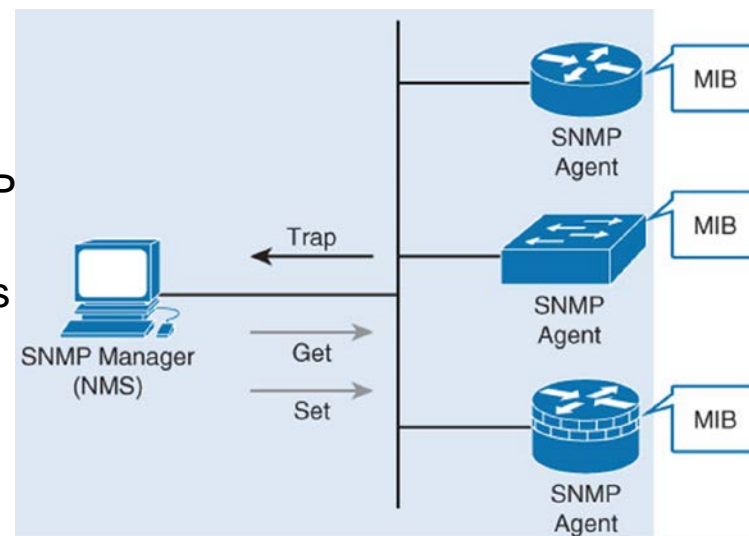
Usar Syslog para proporcionar seguridad en la red (y II)

- Las implementaciones Syslog contienen dos tipos de sistemas:
 - Servidores Syslog: Son las maquinas que aceptan y procesan los mensajes de LOG que provienen de los clientes,
 - Clientes Syslog: Routers o cualquier otro tipo de equipamiento que generan y transmiten mensajes de LOG a los Servidores de SYSLOG.
- Si se quieren emplear servidores de SYSLOG centralizados una solución es emplear “CiscoSecurity Information & Event Manager (SIEM)” que son dispositivos dedicados que se encargan de recibir y analizar mensajes de syslog procedentes de muchas fuentes.
- Pasos necesarios para configurar SYSLOG:
 1. Establecer la máquina destino de los mensajes de LOG con el comando
`logging host [host_name | ip_address]`
 2. Establecer el nivel de severidad (trap) mediante el comando `logging trap level`. Es opcional.
 3. Establecer el interfaz fuente de los mensajes de LOG mediante el comando (no disponible en *Packet Tracer*):
`logging source-interface interface-type interface-number`
 4. Habilitar el *logging* con el comando:
`logging on.`

Si no está deshabilitado, no se mandan mensajes y sólo los recibe la consola.

Usando SNMP

- SNMP se emplea para monitorizar y gestionar nodos, servidores, estaciones de trabajo, routers, switches, hubs y dispositivos de seguridad.
 - Es un protocolo de capa de aplicación que permite analizar el rendimiento de la red
 - A través del protocolo SNMP se puede obtener información de los agentes y cambiar o establecer información en dichos agentes, por lo tanto es necesario controlar el acceso mediante este protocolo a los dispositivos de red
- Componentes:
 - **SNMP manager** o **NMS** (Network Magement System): Gestor que recopila la información SNMP mediante comandos GET y aplica configuraciones a los dispositivos administrados usando comandos SET
 - **SNMP agent**: Cliente que reside en el nodo administrado y responde al NMS con la información de la MIB local
 - **Management Information Base (MIB)**: Base de datos local que almacena información de gestión. El gestor debe conocer la estructura de dicha base de información.



Usando SNMP

- SNMP ha ido evolucionando a lo largo de los años y, actualmente, hay tres versiones:
 - SNMPv1: Es la versión original
 - Se utilizan “**community names**” para la autenticación, que se intercambian en claro
 - Obsoleta
 - SNMPv2: Implementa mejoras de seguridad, rendimiento, confidencialidad y comunicaciones
 - Existen diferentes variantes: La estándar de *facto* es SNMPv2c
 - Utiliza el mismo sistema de **community names** para implementar mecanismos de seguridad
 - SNMPv3: Añade mejoras de seguridad y administración remota
 - Proporciona autenticación, integridad y cifrado.
 - La seguridad en esta versión se organiza en niveles:
 - noAuthNoPriv
 - authNoPriv
 - authPriv

Usando SNMP

- SNMPv1 y v2 son protocolos no seguros: Aceptan comandos y peticiones desde sistemas de gestión NMS en base al **community name**
 - Este parámetro se emplea para autenticar mensajes entre la estación de gestión y el agente de modo que se permita el acceso a la información MIB, en texto claro
- Tipos de **community name**:
 - Sólo Lectura (RO): Proporcionan acceso de lectura exclusivamente a todos los objetos de la MIB. (Método GET)
 - Lectura/Escritura (RW): Proporcionan acceso de R/W a los objetos de las MIB. (Métodos GET y SET)
- Recomendaciones:
 - Utilizar **community names** largas y complejas
 - Cambiar las **community names** periódicamente
 - Activar el acceso de sólo lectura.
 - Si se activa el acceso de escritura, proteger SNMP mediante ACLs
 - Utilizar comunidades diferentes para los **traps**

Configuración SNMP

- Para definir una comunidad en un agente SNMP se utiliza el comando **snmp-server**

- Sintaxis:

```
Router(config)# snmp-server community community-name { ro | rw }
```

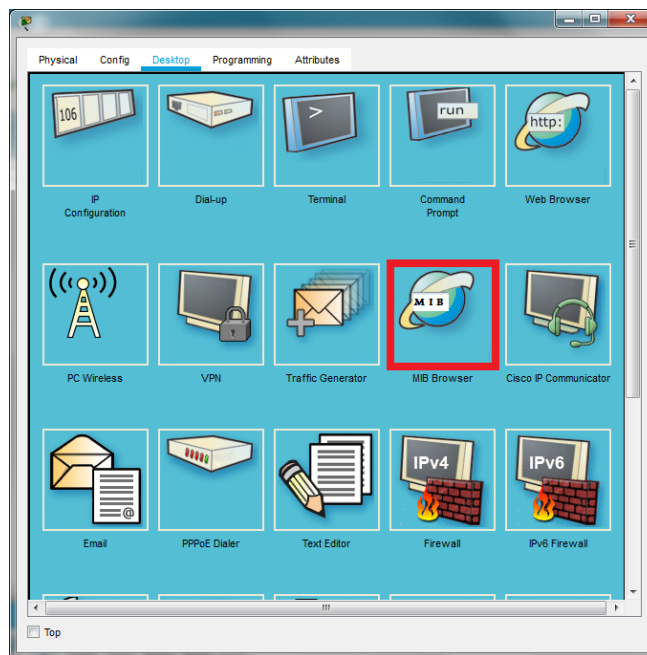
- Ejemplos:

```
R1(config)# snmp-server community communityR1RO ro
```

```
R1(config)# snmp-server community communityR1RW rw
```

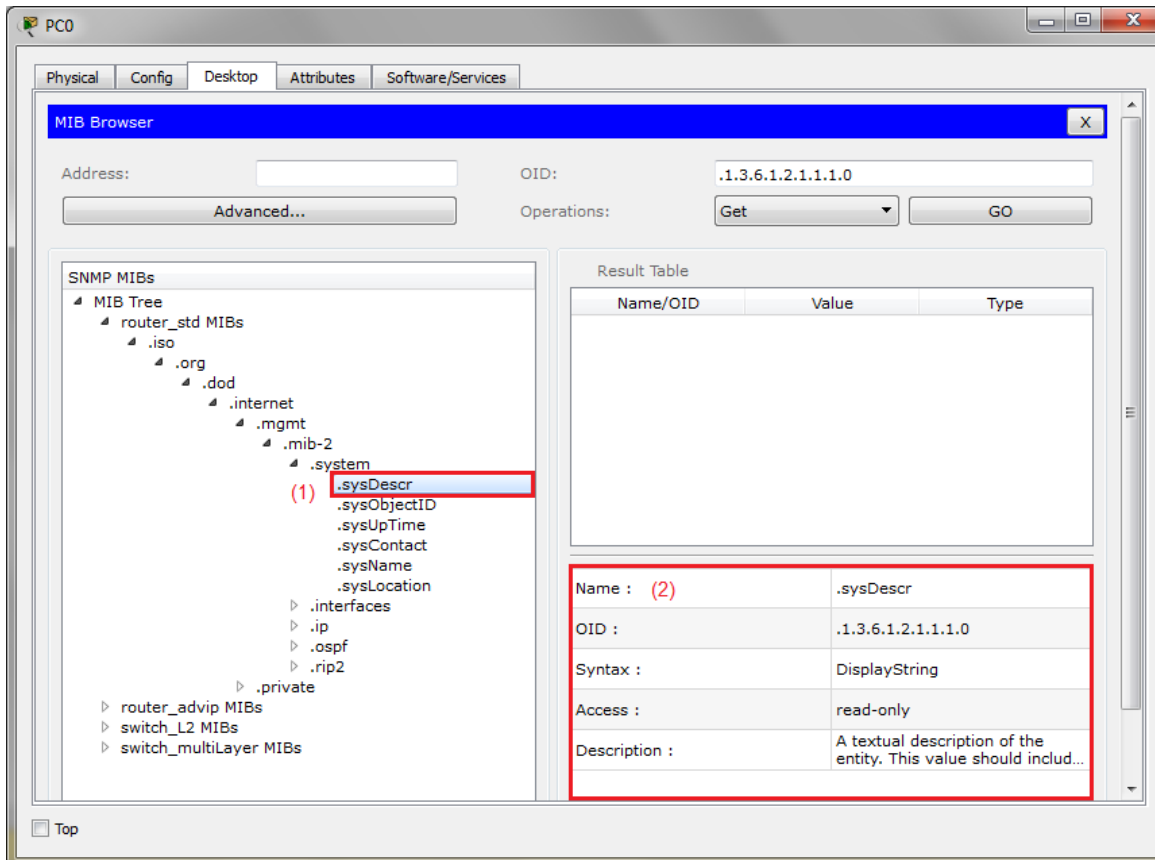

Usando SNMP

- *Packet Tracer* incluye la herramienta de *MIB Browser* en la pestaña *Desktop*.
- *MIB Browser* permite:
 - Navegar por el árbol de registro `iso` de la MIB
 - Obtener y modificar el valor de los objetos de la MIB mediante SNMP



Usando SNMP

- Ejemplo de navegación por el árbol de registro `iso` con *MIB Browser*: objeto `sysDescr` del grupo `system`



The screenshot shows the MIB Browser application window. The left pane displays the 'SNMP MIBs' tree, with the path `.iso > .org > .dod > .internet > .mgmt > .mib-2 > .system > .sysDescr` highlighted. A red box and the number (1) are placed next to `.sysDescr`. The right pane shows the 'Result Table' with the following data:

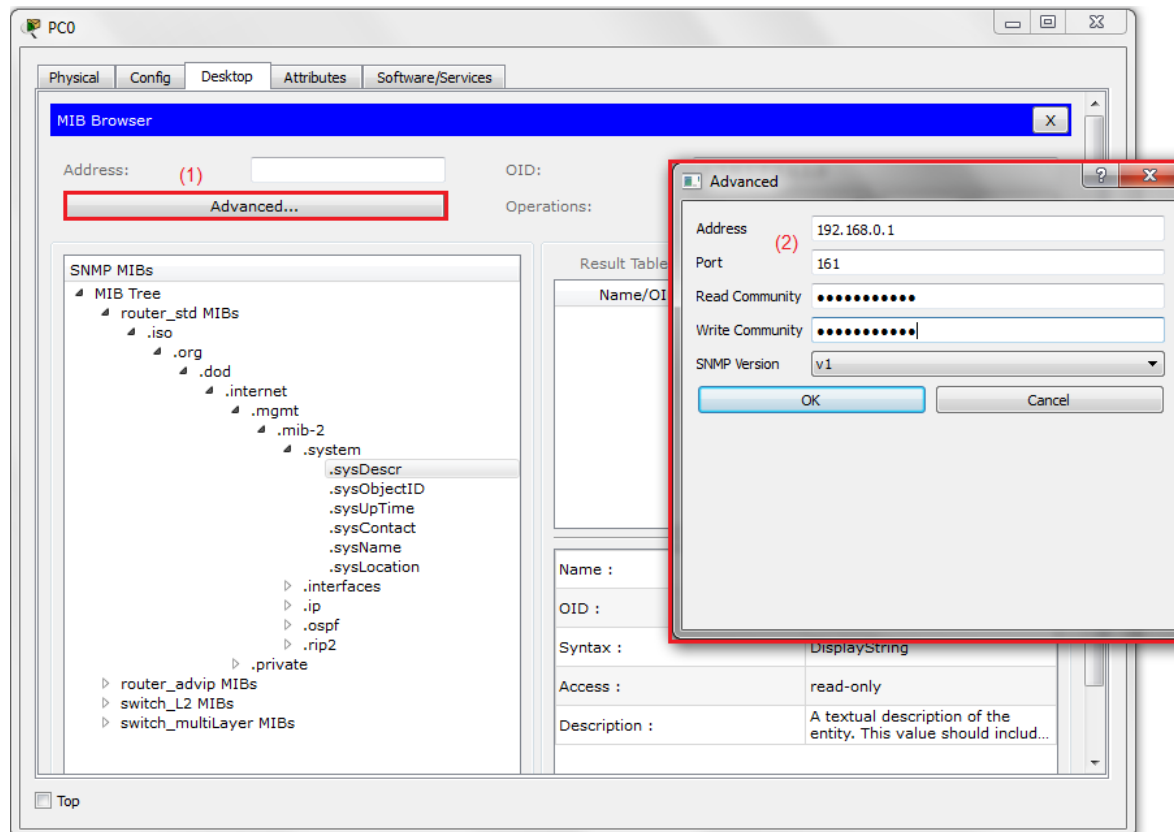
Name/OID	Value	Type
Name : (2)	.sysDescr	
OID :	.1.3.6.1.2.1.1.1.0	
Syntax :	DisplayString	
Access :	read-only	
Description :	A textual description of the entity. This value should includ...	

NOTA: En *Packet Tracer* 7.1.1, 7.2.1 y 7.3 los campos *Syntax*, *Access* y *Description* aparecen vacíos.

IMPORTANTE: Dicha información se puede consultar en documentos RFC .

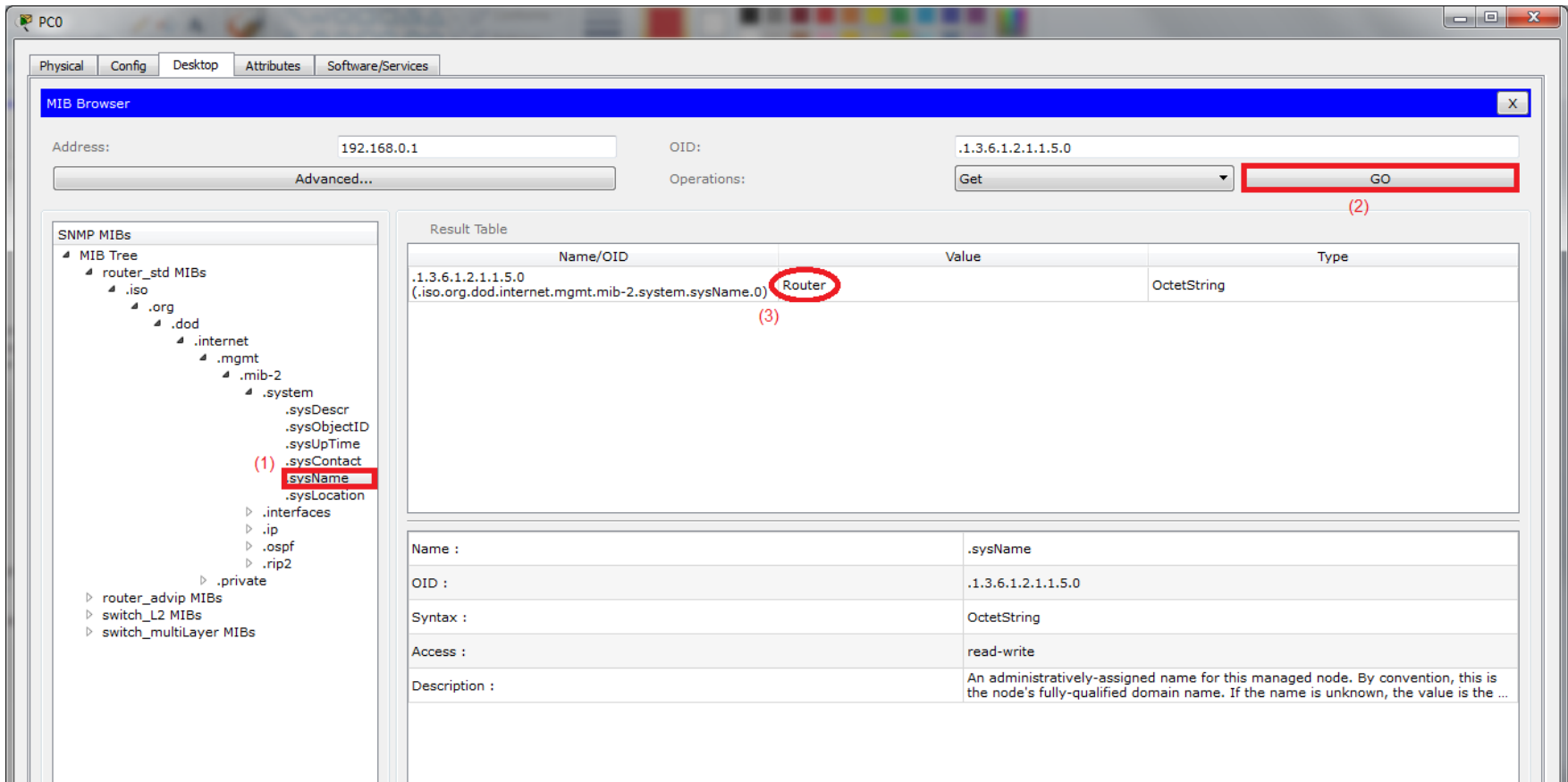
Usando SNMP

- Configuración de acceso al agente en *MIB Browser*.



Usando SNMP

- Obtención desde *MIB Browser* del valor del objeto escalar `sysName` del grupo `system` con identificador de instancia `1.3.6.1.2.1.1.5.0`



The screenshot shows the MIB Browser application window. The Address field is set to 192.168.0.1 and the OID field is set to .1.3.6.1.2.1.1.5.0. The Operations dropdown is set to Get. The GO button is highlighted with a red box and labeled (2). The left pane shows the SNMP MIBs tree, with the path .system > sysName highlighted in red and labeled (1). The right pane shows the Result Table with the following data:

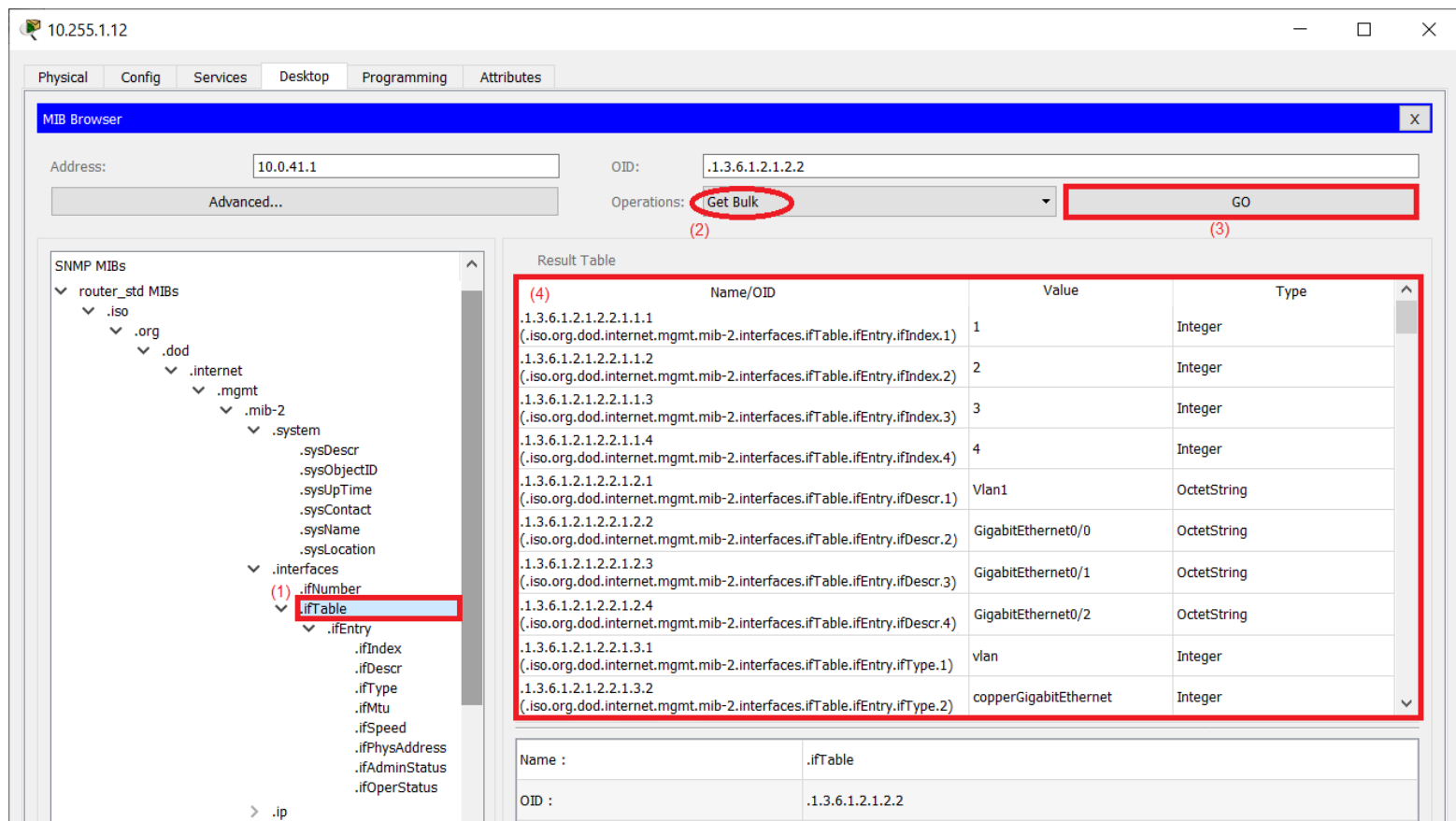
Name/OID	Value	Type
.1.3.6.1.2.1.1.5.0 (.iso.org.dod.internet.mgmt.mib-2.system.sysName.0)	Router	OctetString

The value 'Router' is circled in red and labeled (3). Below the Result Table, there is a detailed view of the selected object:

Name :	.sysName
OID :	.1.3.6.1.2.1.1.5.0
Syntax :	OctetString
Access :	read-write
Description :	An administratively-assigned name for this managed node. By convention, this is the node's fully-qualified domain name. If the name is unknown, the value is the ...

Usando SNMP

- Obtención desde *MIB Browser* de contenido de la tabla *ifTable* del grupo *interfaces* con identificador de instancia *1.3.6.1.2.1.2.2*



The screenshot shows the MIB Browser interface with the following configuration:

- Address:** 10.0.41.1
- OID:** 1.3.6.1.2.1.2.2
- Operations:** Get Bulk (highlighted with a red circle and labeled (2))
- GO** button (highlighted with a red rectangle and labeled (3))

The left pane shows the MIB tree with the following path highlighted:

- SNMP MIBs
 - router_std MIBs
 - .iso
 - .org
 - .dod
 - .internet
 - .mgmt
 - .mib-2
 - .system
 - .sysDescr
 - .sysObjectID
 - .sysUpTime
 - .sysContact
 - .sysName
 - .sysLocation
 - .interfaces
 - (1) .ifNumber
 - (4) **.ifTable** (highlighted with a red rectangle)
 - .ifEntry
 - .ifIndex
 - .ifDescr
 - .ifType
 - .ifMtu
 - .ifSpeed
 - .ifPhysAddress
 - .ifAdminStatus
 - .ifOperStatus

The right pane shows the Result Table with the following data:

| (4) | Name/OID | Value | Type |
|-----|--|-----------------------|-------------|
| | 1.3.6.1.2.1.2.2.1.1.1
(.iso.org.dod.internet.mgmt.mib-2.interfaces.ifTable.ifEntry.ifIndex.1) | 1 | Integer |
| | 1.3.6.1.2.1.2.2.1.1.2
(.iso.org.dod.internet.mgmt.mib-2.interfaces.ifTable.ifEntry.ifIndex.2) | 2 | Integer |
| | 1.3.6.1.2.1.2.2.1.1.3
(.iso.org.dod.internet.mgmt.mib-2.interfaces.ifTable.ifEntry.ifIndex.3) | 3 | Integer |
| | 1.3.6.1.2.1.2.2.1.1.4
(.iso.org.dod.internet.mgmt.mib-2.interfaces.ifTable.ifEntry.ifIndex.4) | 4 | Integer |
| | 1.3.6.1.2.1.2.2.1.2.1
(.iso.org.dod.internet.mgmt.mib-2.interfaces.ifTable.ifEntry.ifDescr.1) | Vlan1 | OctetString |
| | 1.3.6.1.2.1.2.2.1.2.2
(.iso.org.dod.internet.mgmt.mib-2.interfaces.ifTable.ifEntry.ifDescr.2) | GigabitEthernet0/0 | OctetString |
| | 1.3.6.1.2.1.2.2.1.2.3
(.iso.org.dod.internet.mgmt.mib-2.interfaces.ifTable.ifEntry.ifDescr.3) | GigabitEthernet0/1 | OctetString |
| | 1.3.6.1.2.1.2.2.1.2.4
(.iso.org.dod.internet.mgmt.mib-2.interfaces.ifTable.ifEntry.ifDescr.4) | GigabitEthernet0/2 | OctetString |
| | 1.3.6.1.2.1.2.2.1.3.1
(.iso.org.dod.internet.mgmt.mib-2.interfaces.ifTable.ifEntry.ifType.1) | vlan | Integer |
| | 1.3.6.1.2.1.2.2.1.3.2
(.iso.org.dod.internet.mgmt.mib-2.interfaces.ifTable.ifEntry.ifType.2) | copperGigabitEthernet | Integer |

At the bottom, the Name and OID are confirmed:

 - Name :** .ifTable
 - OID :** 1.3.6.1.2.1.2.2

Usando SNMP

- La herramienta de *MIB Browser* también permite modificar los objetos de la MIB que tienen definido en la cláusula *Access* el valor READ-WRITE.

