RCOMP - Redes de Computadores (Computer Networks)

2023/2024

Theoretical-practical lesson 12

- Simple Network Management Protocol (SNMP).
- Practical activity in Packet Tracer.

SNMP – Simple Network Management Protocol

Within a network infrastructure, active devices like switches and routers are disseminated over a large area, some protocols have been designed to help network administrators managing them remotely.

Management protocols use the network infrastructure itself to establish dialogues and exchange information with each device, and thus centralize all management activities in a single node, usually called the management station.

For the sake of security, network administrators will usually create a separated network for these protocols. This can be achieved by creating a dedicated VLAN inaccessible to standard users. This is undoubtedly a recommended practice.

SNMP uses UDP messages. Each managed device must run an SNMP Agent. The agent is a small UDP server listening for SNMP requests on port number 161.

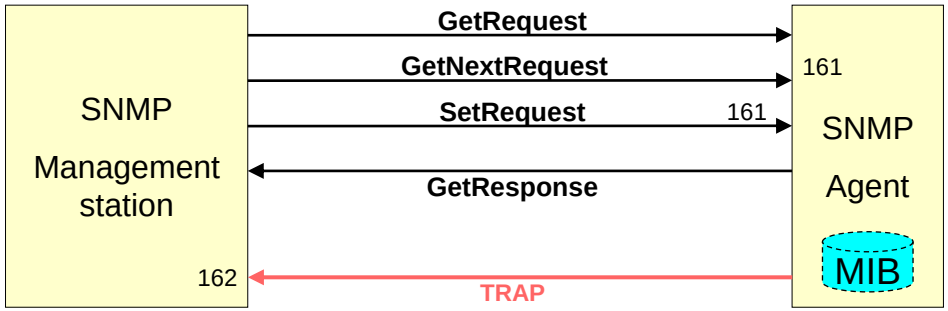
The SNMP agent receives requests from the management station, they may be either queries to the device status (GetRequest) or configuration/status change requests (SetRequest).

Also, SNMP agents may be configured to send unsolicited event notifications called Traps to the management station's UDP port number 162.

SNMP version 1

SNMP version 1 is the most widely supported, but has some significant short comes, for instance regarding security.

SNMPv1 security is based on a possibly secret community name, though it's sent in plain text and can be captured by network sniffers.



Nevertheless, agents can be configured to provide read only access (queries only), that's the most common use for SNMPv1. Therefore, it becomes essentially a status retrieval protocol.

Status data to be queried is organised in a tree structured objects database, each object is in essence a variable that stores a value. This database is called the MIB (Management Information Base).

Objects in the MIB are referred by OID (Object Identifier) and not names. Each object's (OID) content represents some type of information about the device. Some objects are standard for all device types, others only make sense for some device types. Some objects are read-only, others may be changed by SetRequests.

SNMP queries - GetRequest

To retrieve information from an agent, the object's OID whose value we want to get must be known, for instance, every device has as textual description (**.sysDesc**), this is OID: **.1.3.6.1.2.1.1.1**

It comes from: **.iso.org.dod.internet.mgmt.mib-2.system.sysDesc**

Each name/number/OID is a MIB tree branch. In fact, this refers to an object class, the first instance of the object's class is referred by using the zero suffix or no suffix at all, for **.sysDesc**: **.1.3.6.1.2.1.1.1.0** or **.1.3.6.1.2.1.1.1**.

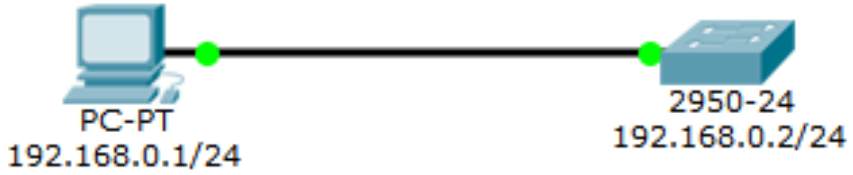
Usually, for most object classes there will be just one instance, but for others there may be several.

Some objects, like those in the **.system** branch (**.1.3.6.1.2.1.1**), are present on every device, but other objects may be present only if they make sense for a particular device, thus each device's MIB is a small subset of all possible MIB objects.

Manufactures can also add new branches to the MIB if they find the data they what to represent requires new objects. Private MIBs are added to the **.private** branch (.1.3.6.1.4). Cisco private MIBs are in .1.3.6.1.4.1.9 branch, this branch OID stands for **.iso.org.dod.internet.mgmt.private.enterprises.cisco**

SNMP practical exercise – Packet Tracer

To take a more direct contact with SNMP operations we will use the Packet Tracer network simulation tool. A single PC connected to a switch is enough for this. As most network devices, this switch has an SNMP agent, we just need to activate it.



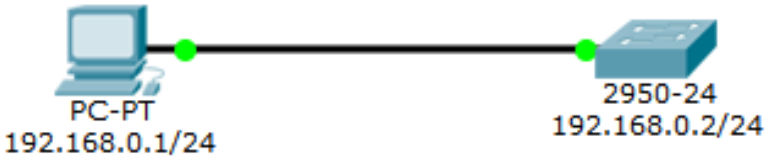
The PC includes a MIB browser, it will be our management station. Before being able to use SNMP, IPv4 addresses must be defined on both nodes. Unlike routers, on switches IP address are assigned to VLANs and not physical interfaces. In the original VLAN configuration of Cisco switches only one VLAN exists (VLANID=1) and is assigned to all ports is access-mode. After settling the PC's IPv4 address, configure the switch as follows:

This defines the node name as **RCOMP-switch** and enables the SNMP agent for read-only access through the **public** community name . The switch IPv4 address is going to be 192.168.0.2/24.

```
hostname RCOMP-switch
snmp-server community public ro
interface vlan 1
 ip address 192.168.0.2 255.255.255.0
 no shutdown
```

SNMP practice – Packet Tracer

Once the PC's IPv4 address is defined as well, we can then start playing with SNMP.



Click on the PC, select Desktop, and then MIB Browser.

Click on Advanced, and settle:

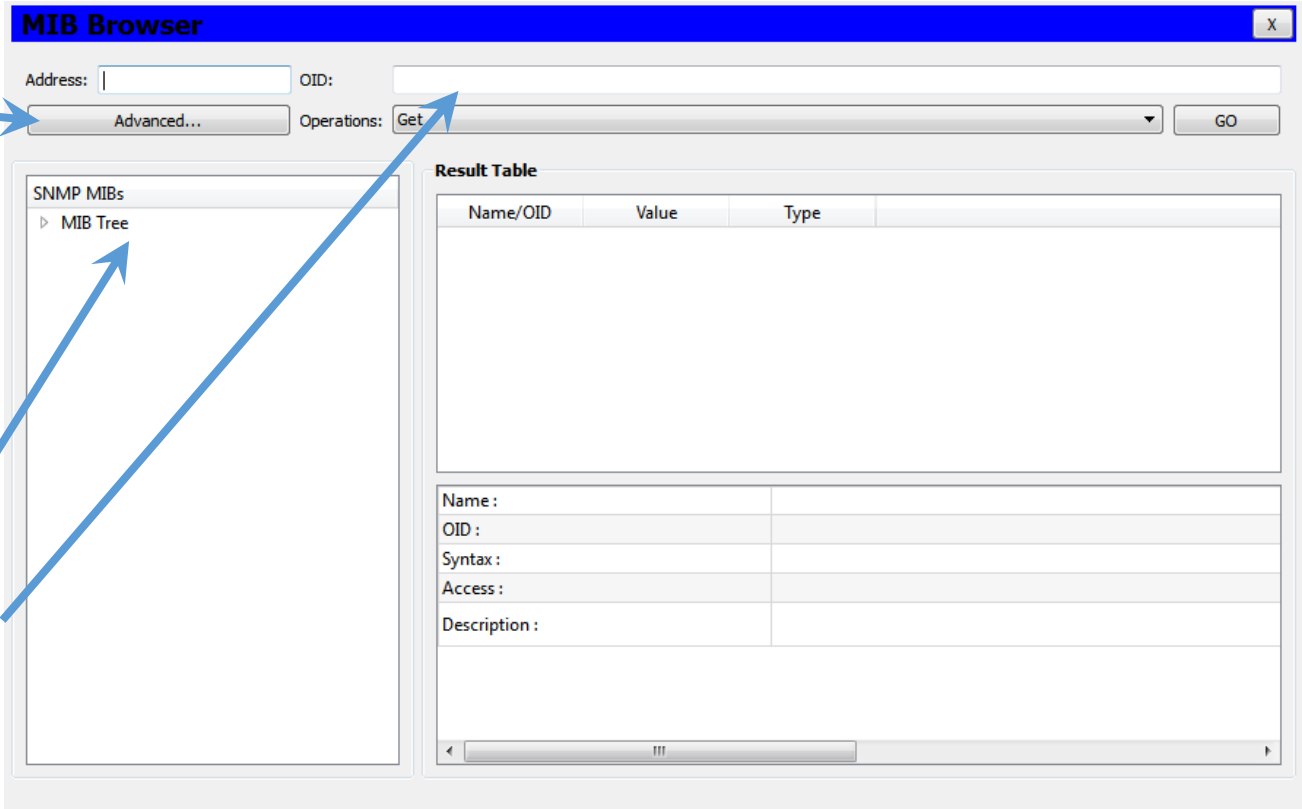
Address: 192.168.0.2

Port: 161

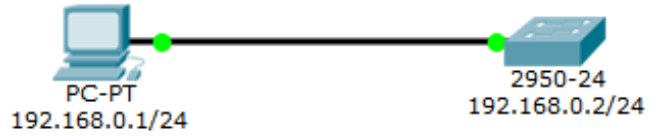
Read Community: public

Now this MIB browser is focused on our switch.

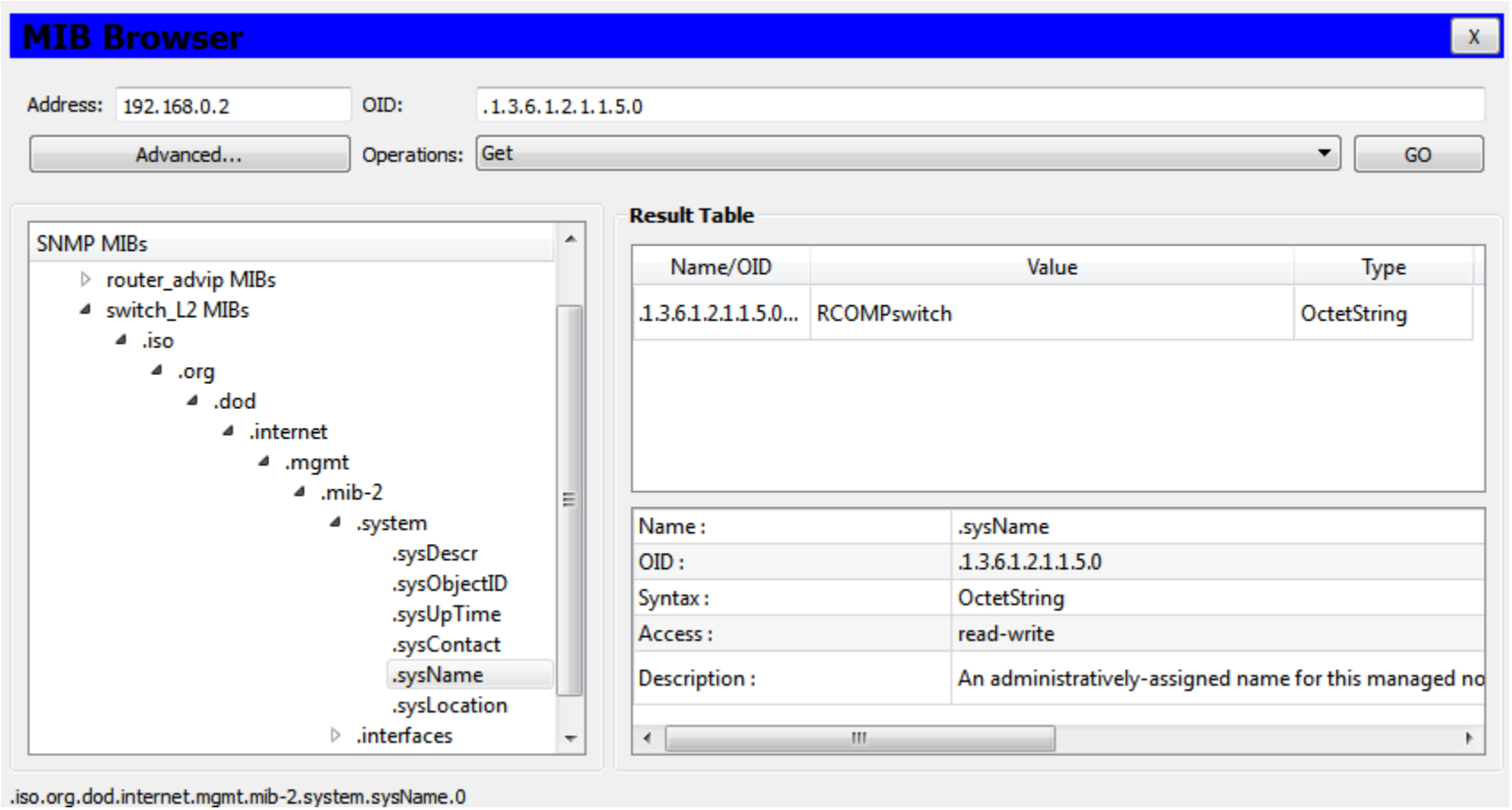
We can either select the OID from the tree, or manually type the object OID.



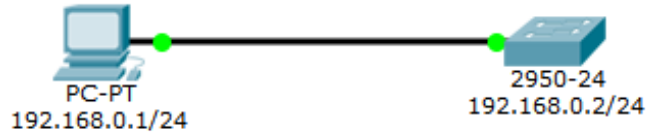
SNMP practice – Packet Tracer



As you may see, several MIBs can be used, each is made of an OID's objects collection appropriate for a specific device type. Expand the **switch_L2 MIBs** up to the **.system** branch and select **.sysName**. Now we have the desired OID, and we can press GO to perform an SNMP GetRequest and retrieve the object's value.



SNMP practice – Packet Tracer



Still on the **.system** branch, select now the **.sysUpTime** and then press GO to perform an SNMP GetRequest and learn for how long is the switch running.

MIB Browser

Address: 192.168.0.2 OID: .1.3.6.1.2.1.1.3.0

Advanced... Operations: Get GO

SNMP MIBs

- MIB Tree
  - router_std MIBs
  - router_advip MIBs
  - switch_L2 MIBs
    - .iso
      - .org
        - .dod
          - .internet
            - .mgmt
              - .mib-2
                - .system
                  - .sysDescr
                  - .sysObjectID
                  - .sysUpTime
                  - .sysContact
                  - .sysName

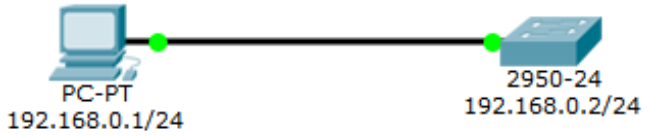
Result Table

Name/OID	Value	Type
.1.3.6.1.2.1.1.3.0...	0 hours 19 minutes 13 seconds	TimeTicks

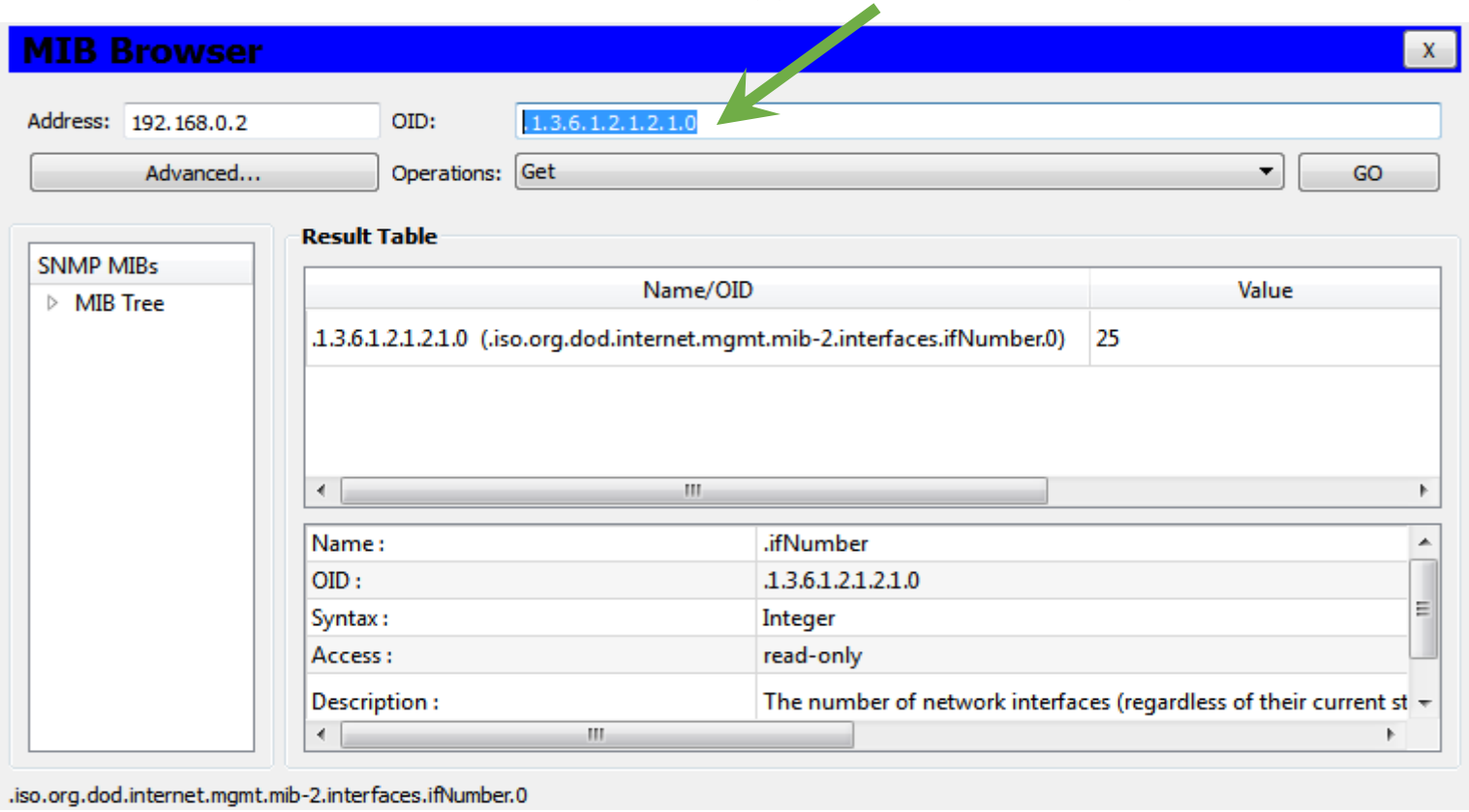
Name :	.sysUpTime
OID :	.1.3.6.1.2.1.1.3.0
Syntax :	TimeTicks
Access :	read-only
Description :	The time (in hundredths of a second) since the n

.iso.org.dod.internet.mgmt.mib-2.system.sysUpTime.0

SNMP practice – Packet Tracer



The MIB is just an OID collection, if we know the OID for the desired object we can use it directly, for instance to get the number of network interfaces on a device we can use OID **.1.3.6.1.2.1.2.1.0**. Just type this OID and press GO:



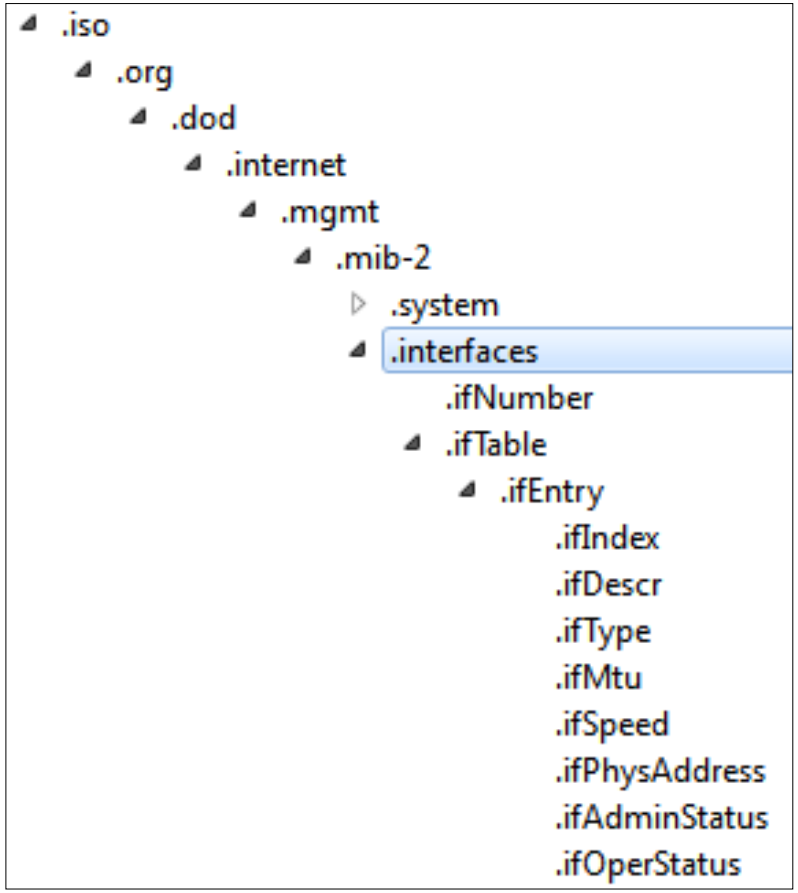
We got 25 interfaces for this switch; they are 24 physical interfaces and the VLAN interface we have created to establish the switch IPv4 address.

SNMP practice – Packet Tracer

On Packet Tracer devices' MIBs are only a sample of real devices' MIBs. Yet, one branch we can explore further is **.iso.org.dod.internet.mgmt.mib-2.interfaces** (.1.3.6.1.2.1.2).

We already know **.ifNumber** holds the number of network interfaces on the device. Every interface is represented in a table (**.ifTable**), each table entry (**.ifEntry**) contains several objects. The number of entries in the table is the number of network interfaces (**.ifNumber**).

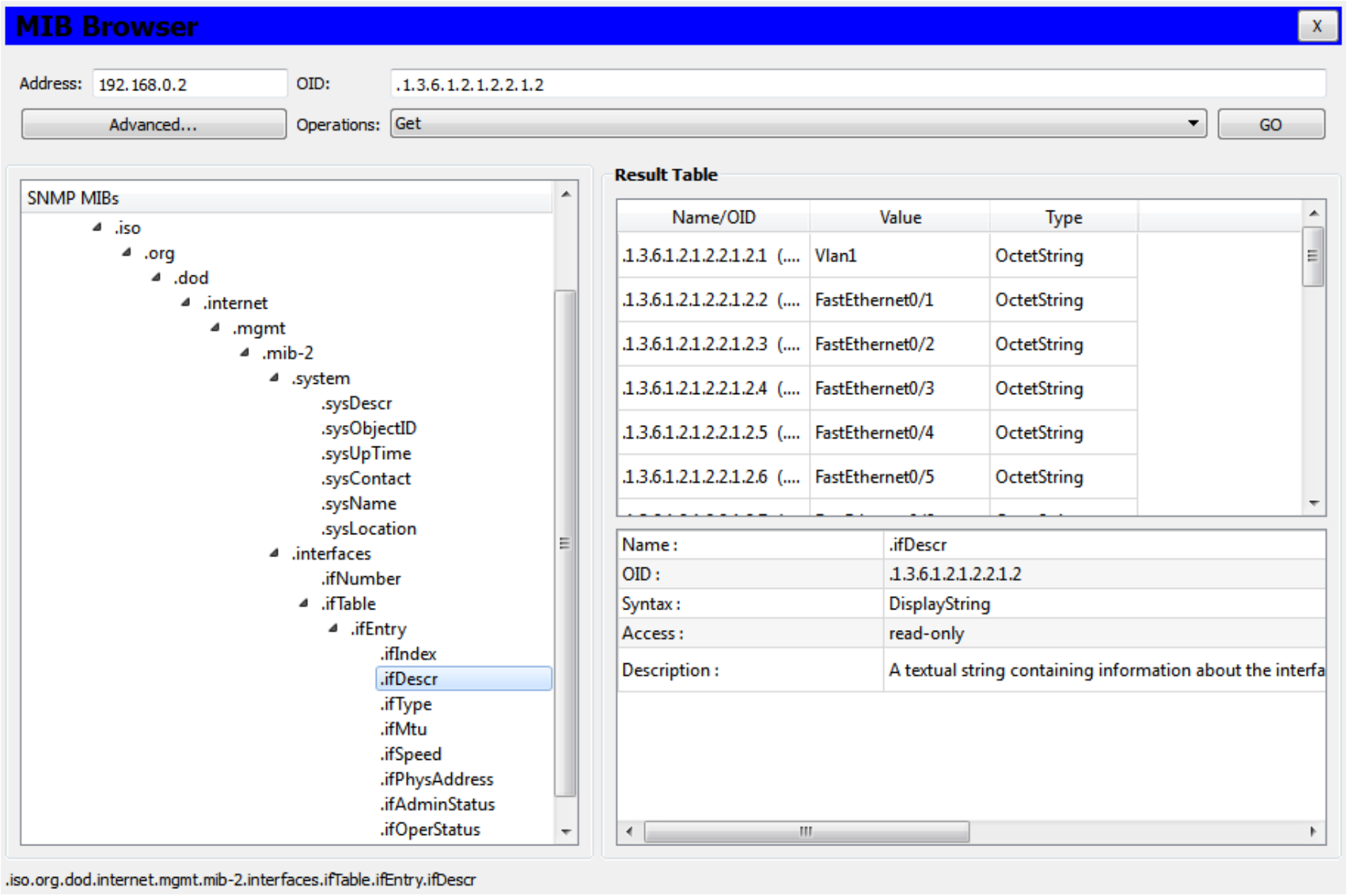
Neither **.ifTable** nor **.ifEntry** are accessible, but objects in **.ifEntry** can be retrieved by OID if we use a prefix representing the entry's number. In **.ifTable** the entry number is stored in **.ifIndex** and goes from 1 up to the number of network interfaces (**.ifNumber**).



For instance **.ifDescr** OID is **.1.3.6.1.2.1.2.2.1.2**, thus the second network interface's description is **.1.3.6.1.2.1.2.2.1.2.2**, this can also be represented as **.ifDescr.2**.

SNMP practice – Packet Tracer

If we send an SNMP GetRequest for **.ifDesc** we get a list of values in the table:



SNMP practice – Packet Tracer

On a real device MIB, each entry in an interfaces table has several other objects, not present in Packet Tracer devices:

```
1.3.6.1.2.1.2.2.1.1 - ifIndex
1.3.6.1.2.1.2.2.1.2 - ifDescr
1.3.6.1.2.1.2.2.1.3 - ifType
1.3.6.1.2.1.2.2.1.4 - ifMtu
1.3.6.1.2.1.2.2.1.5 - ifSpeed
1.3.6.1.2.1.2.2.1.6 - ifPhysAddress
1.3.6.1.2.1.2.2.1.7 - ifAdminStatus
1.3.6.1.2.1.2.2.1.8 - ifOperStatus
1.3.6.1.2.1.2.2.1.9 - ifLastChange
1.3.6.1.2.1.2.2.1.10 - ifInOctets
1.3.6.1.2.1.2.2.1.11 - ifInUcastPkts
1.3.6.1.2.1.2.2.1.12 - ifInNUcastPkts
1.3.6.1.2.1.2.2.1.13 - ifInDiscards
1.3.6.1.2.1.2.2.1.14 - ifInErrors
1.3.6.1.2.1.2.2.1.15 - ifInUnknownProtos
1.3.6.1.2.1.2.2.1.16 - ifOutOctets
1.3.6.1.2.1.2.2.1.17 - ifOutUcastPkts
1.3.6.1.2.1.2.2.1.18 - ifOutNUcastPkts
1.3.6.1.2.1.2.2.1.19 - ifOutDiscards
1.3.6.1.2.1.2.2.1.20 - ifOutErrors
1.3.6.1.2.1.2.2.1.21 - ifOutQLen
1.3.6.1.2.1.2.2.1.22 - ifSpecific
```

SNMPv1 as network monitoring tool

In a real network infrastructure, network administrators are often confronted with the fact many devices to be managed only support SNMPv1, and thus that's the version that can be used.

Main issue around version 1 is security, yet if no read-write communities are established this becomes a privacy only issue, which in most cases is bearable.

In the above scenario, SNMP is used only for devices status retrieval in a monitored network environment. Network monitoring services perform **periodic tests to the network infrastructure components and services**. Network services can be directly tested, for instance check if an HTTP server is replying to HTTP requests.

To check stuffs regarding how nodes are internally operating, for instance disk free space, specific protocols are required. For this purpose, SNMP can be used to obtain devices internal status data and confront it with established desired values. If obtained values are outside the desired values scope an alert is issued notifying network administrators.

As an example, the **.sysUpTime** object could be checked every five minutes and a warning issued if the value in less than five minutes, this would notify network administrators the device has just suffered a restart.

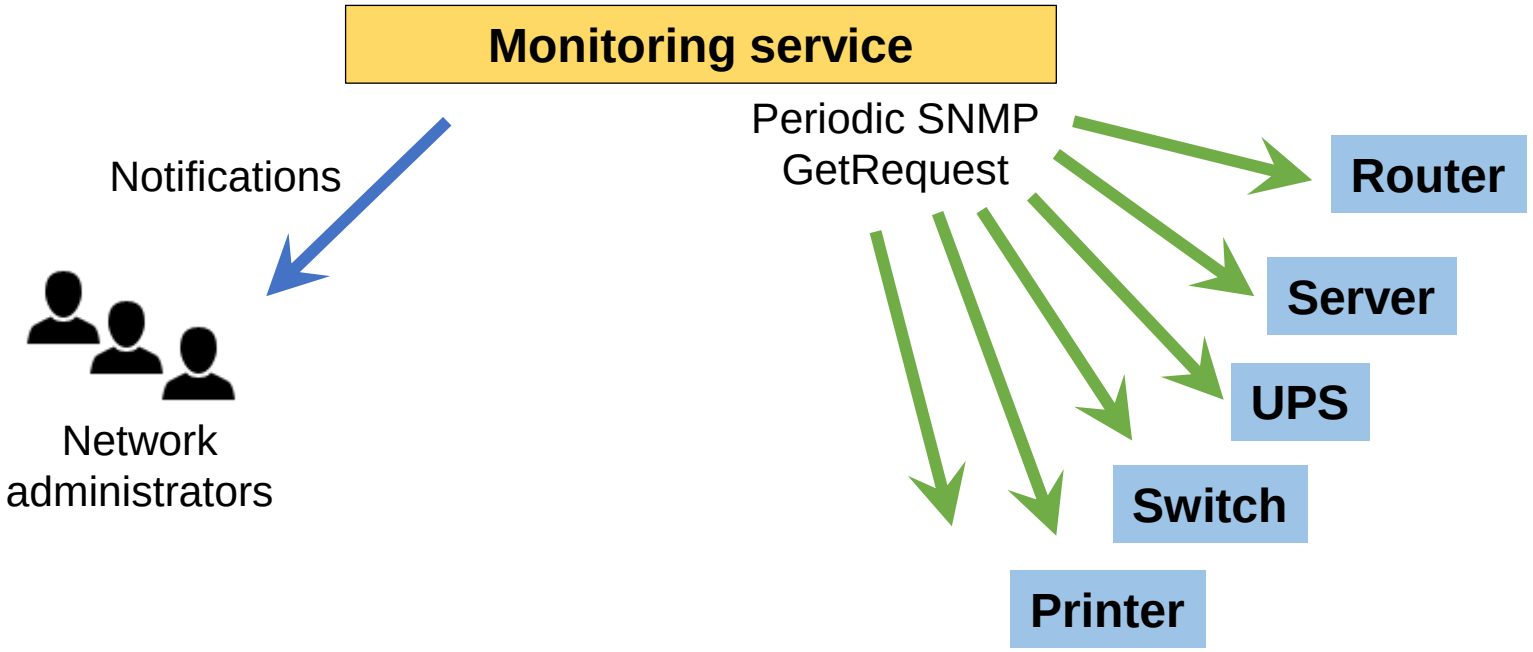
SNMP as network monitoring tool

Even though on Packet Tracer MIBs are rather simplified, in a real device there will be several counters for packets and bytes sent and received in each interface. Two consecutive readings of such counters in a time period provide a measurement of the average traffic during that period. This is one typical use for SNMP as monitoring tool.

Taking full advantage of SNMP requires a deep knowledge of the MIBs made available by each vendor. Most network devices like switches, routers, access-points, network printers and UPSs, have special MIBs that will allow internal status retrieval of data well beyond standard MIBs, examples:

- Printers' tuner status.
- Number of pages printed in a network printer.
- Temperature reading in several device sensors.
- Device fans rotation speed or status.
- Device power supply status, and the battery status for an UPS.
- Disk status.
- Memory status and CPU status.

SNMP as network monitoring tool



The **monitoring service** runs in background with the mission of **periodically checking** if all components are conforming to pre settled requirements, if a deviation is detected, **network administrators are notified**.

Notifications pinpoint issues as soon as they are detected, thus administrators can intervene and solve them in real time. Desirably before users are affected by those issues.