SNMP
Simple Network Management Protocol

11th -15th March 2019

Workshop on Campus Network Best Practices

D.I.K.Solangaarachchi / University of Kelaniya

What is SNMP

SNMP is a standard protocol

Collects data from almost any network attached device

- Routers
- Switches
- Wireless LAN Controllers
- Wireless Access Points
- Servers
- Printers and more

How SNMP Works

- By querying “Objects”

  An object is a property of a device.

  Eg: CPU utilization, Temperature of Switch

- Return value can be used various monitoring activities

  Eg:

  - Alerting
  - Reporting.

SNMP Components

Three key components:

- Managed devices
- Agents
- Network management systems (NMSs)

SNMP Components

A **managed device** resides on a managed network and is usually represented as one of the many nodes of the network.

Such devices can be routers, access servers, switches, bridges, hubs, computer hosts, printers, and even all kinds of IoT devices that "speak" SNMP.

SNMP Components

SNMP-managed device has an **SNMP agent** on it.

An agent is a software module that translates device information into an SNMP-compatible format in order to make the device information available for monitoring with SNMP.

SNMP Components

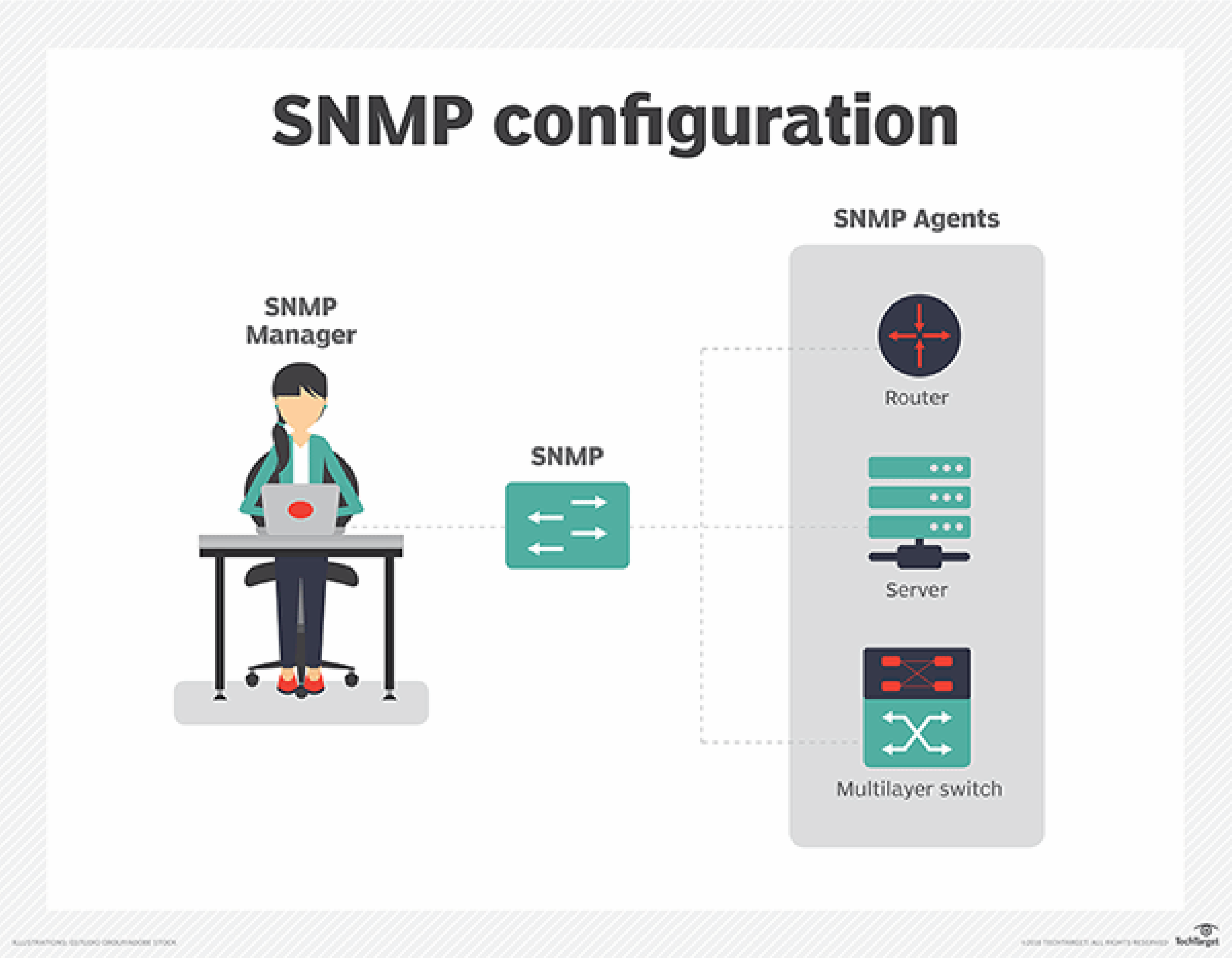
A **network management system** runs monitoring applications.

They provide the bulk of processing and memory resources required for network management.

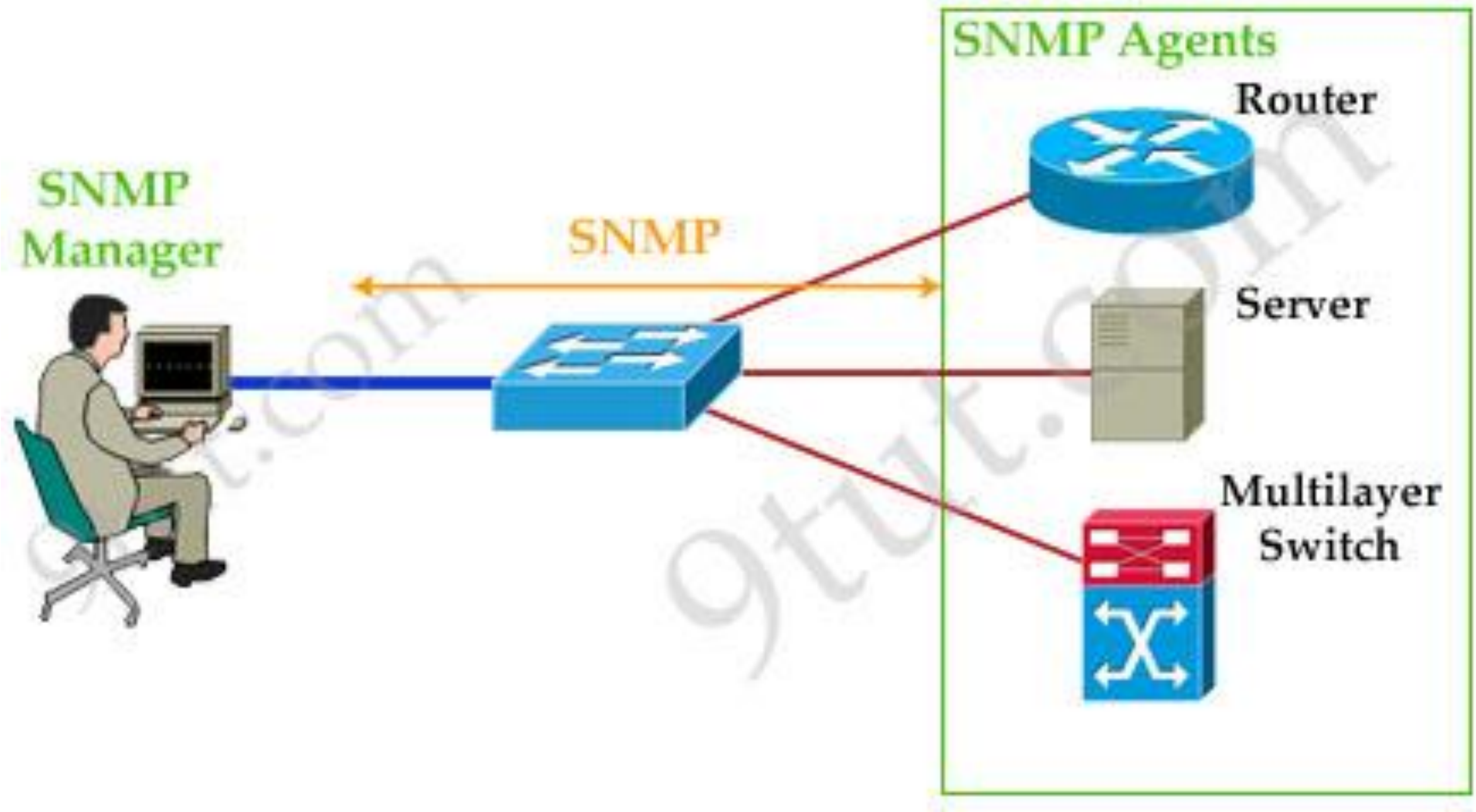
Key functions

- Queries agents
- Gets responses from agents
- Sets variables in agents
- Acknowledges asynchronous events from agents

Manager and Agent



Manager and Agent



Manager and Agent

Manager (the monitoring station)

Sometimes known as the SNMP client

Agent (running on the equipment/server)

Sometimes known as the SNMP server

SNMP Traps

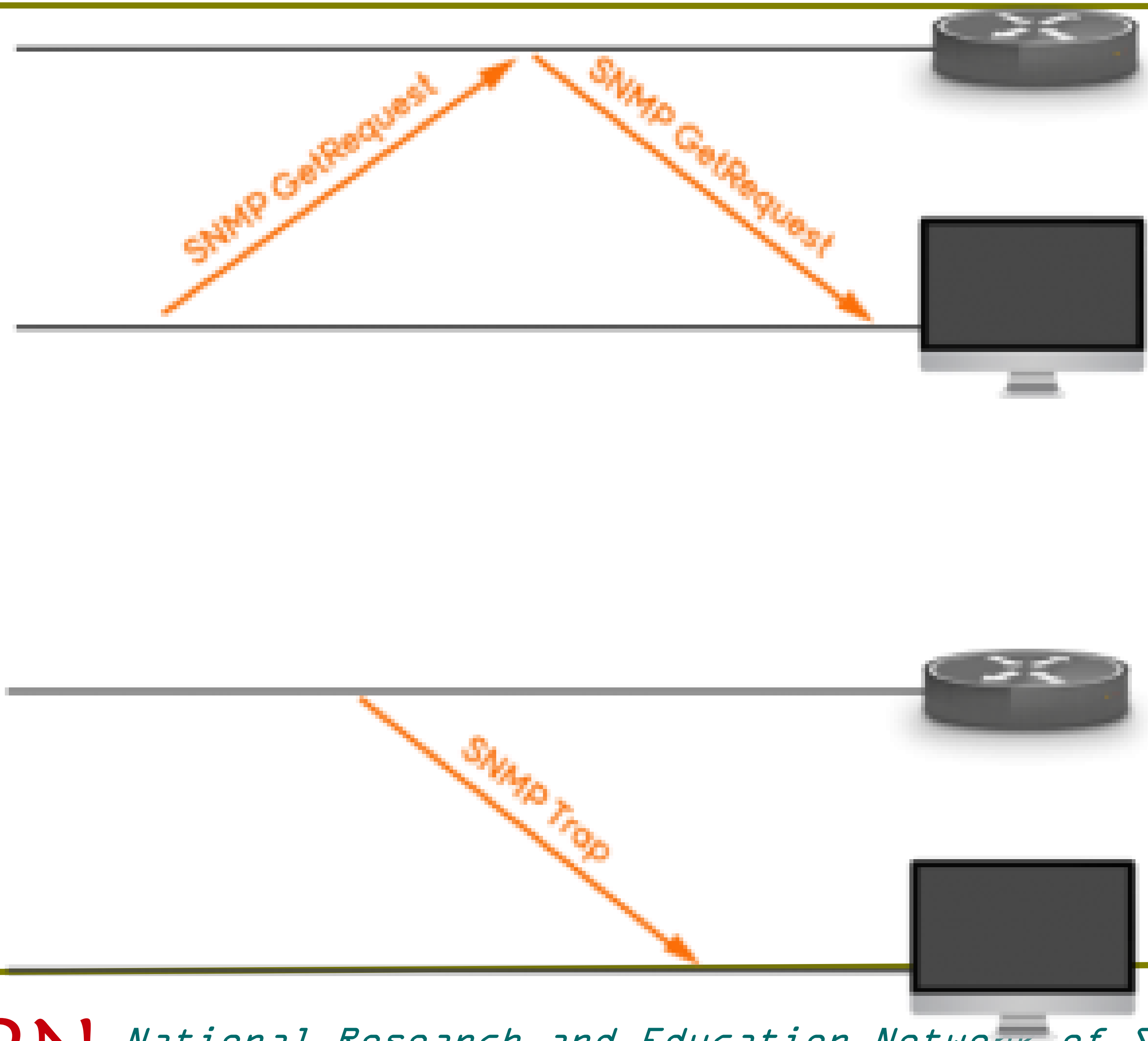
The normal operations of SNMP dictate that the device agent takes a passive role.

It only sends out SNMP messages when prompted by a request from the SNMP manager.

However, if the agent detects an emergency event on the device that it is monitoring, it will send out a warning message to the manager without waiting to be polled for data.

This emergency message is called a trap.

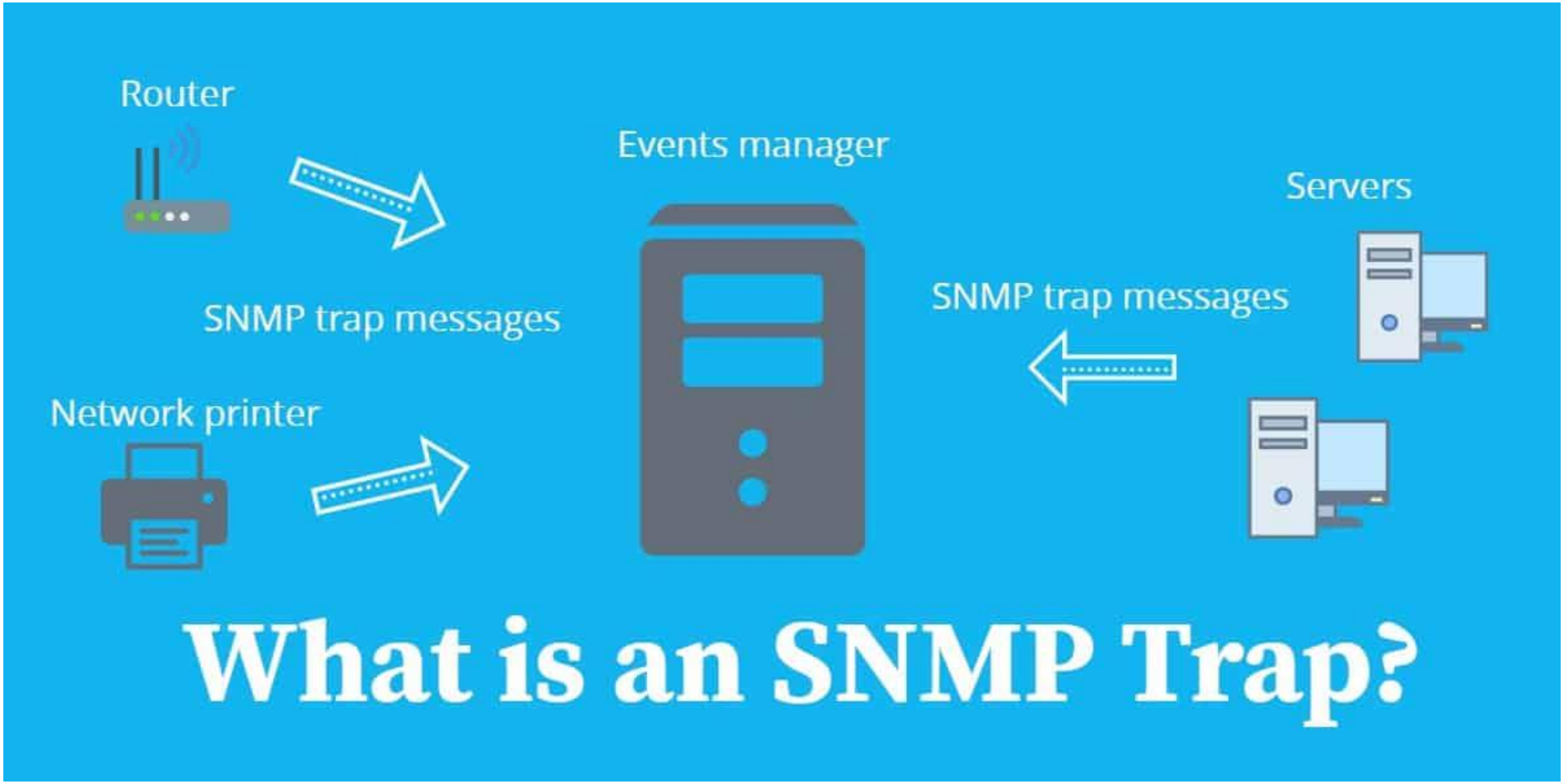
SNMP traps



SNMP Traps

- Eg:
  - linkUpDownNotifications
  - devices.status = 0
  - High memory usage: macros.device_up = 1 AND mempools.mempool_perc >= 90 AND mempools.mempool_descr REGEXP "Virtual.*“
- Traps are unacknowledged
- Informs are acknowledged

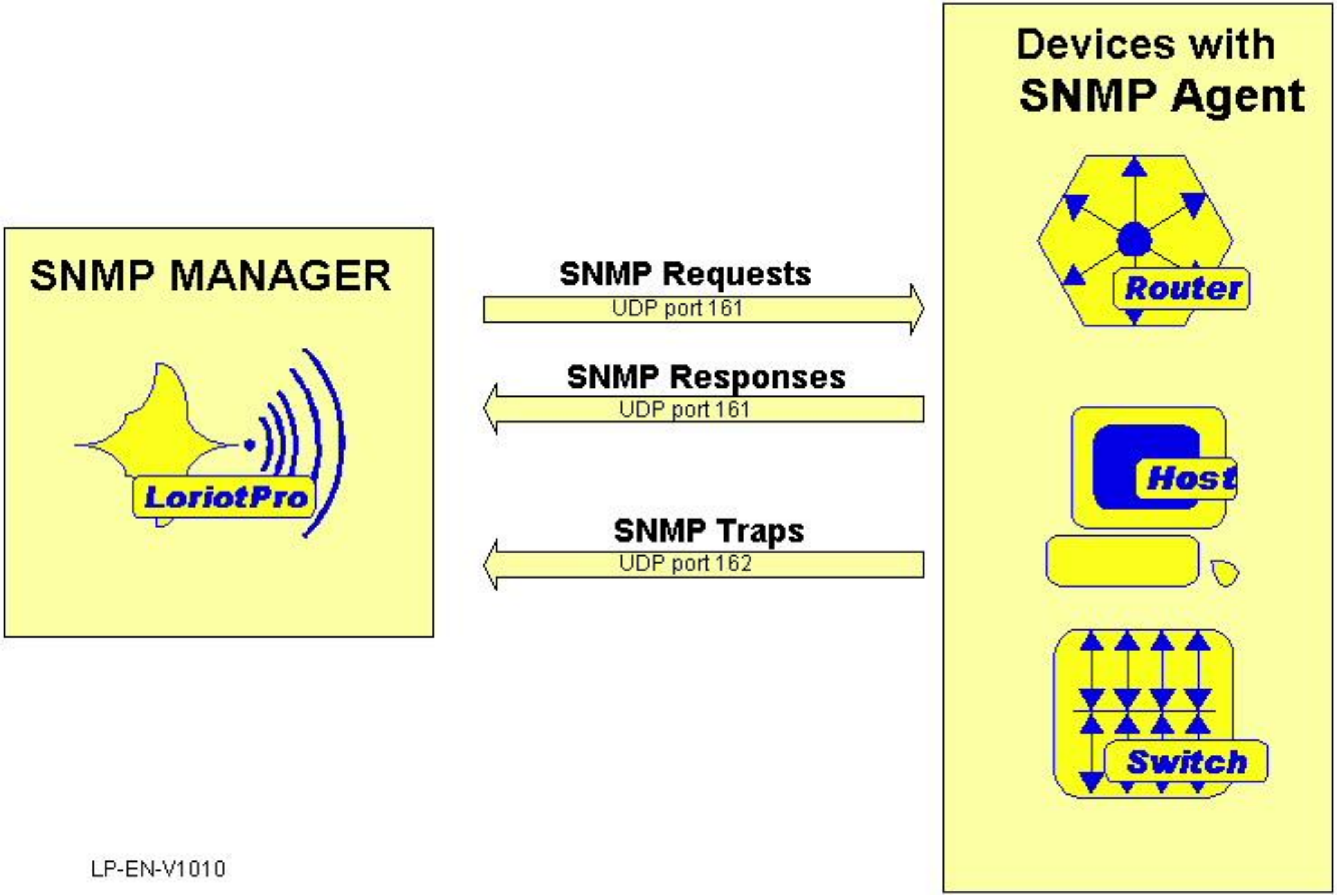
SNMP traps


Router
Events manager
Servers
SNMP trap messages
SNMP trap messages
Network printer
What is an SNMP Trap?

Which port SNMP uses ?

UDP ports 161 and 162

Différence of port 161 and 162



SNMP Versions

Three versions of SNMP

Version 1

- Wasn’t very widely implemented.
- This was released in 1988.

Version 2 (SNMPv2c)

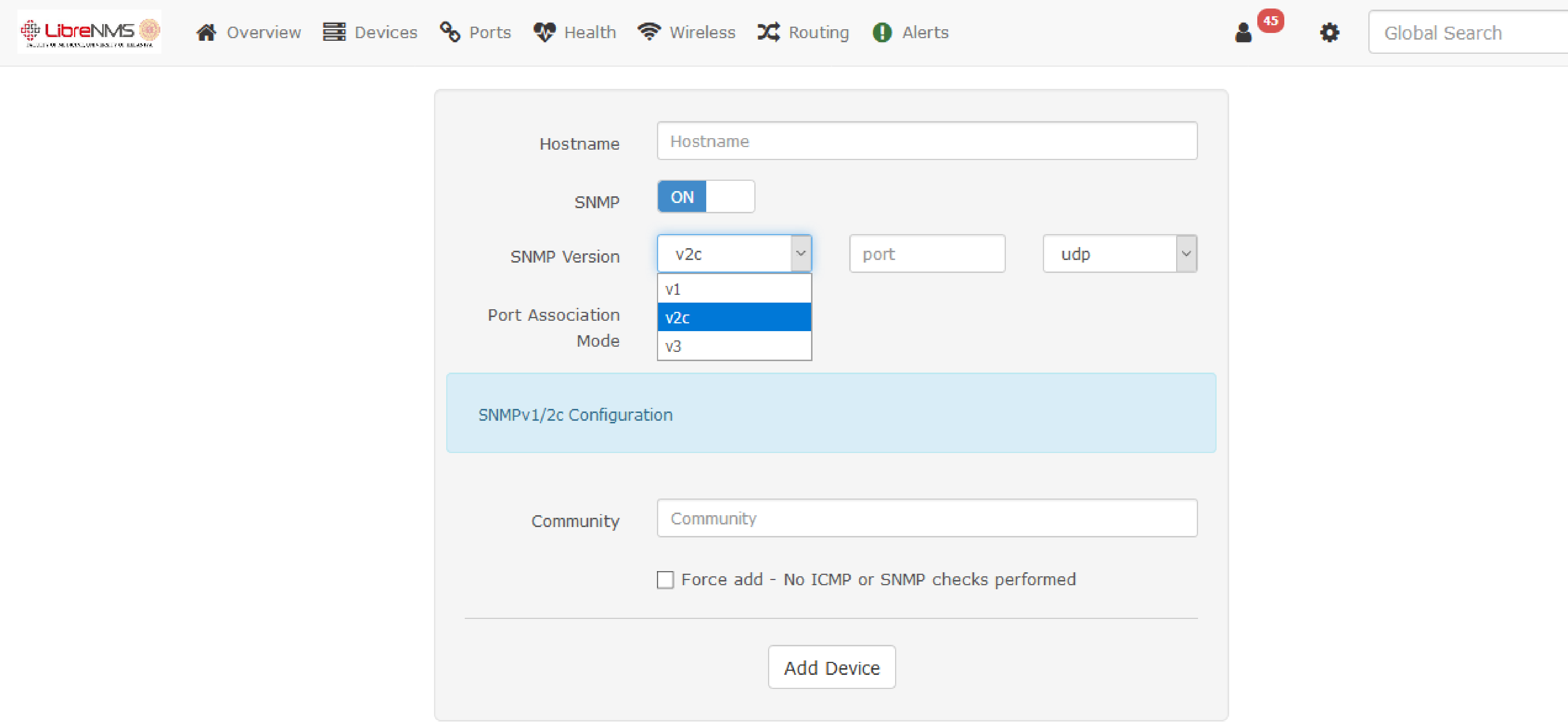
- This was released in 1996 .
- SNMP v2c is considered the de facto network management protocol in the Internet community
- Most of the major network devices are having **SNMPv2c**

SNMP Versions

Version 3

- Latest version
- Includes a different encryption method to protect transmissions of MIB files
- Generally, the leading network monitors are compatible with both version 2 (meaning SNMPv2c) and version 3.

SNMP Versions



Hostname: Hostname

SNMP: ON

SNMP Version: v2c | port | udp

v1
v2c
v3

Port Association Mode

SNMPv1/2c Configuration

Community: Community

□ Force add - No ICMP or SNMP checks performed

Management Information Base (MIB)

Every SNMP agent maintains an information database describing the managed device parameters.

The SNMP manager uses this database to request the agent for specific information and further translates the information as needed for the Network Management System (NMS).

This commonly shared database between the Agent and the Manager is called Management Information Base (MIB).

Management Information Base (MIB)

Decompose DNS

Medicine.kln.ac.lk

Management Information Base (MIB)

A management information base (MIB) is a hierarchical virtual database.

Each MIB is addressed or identified using an object identifier (OID), which is often a device’s setting or status.

The OID uniquely identifies a managed object in the MIB hierarchy

Each managed object is made up of one or more variables called object instances. These, too, are identified by OIDs.

Object Identifiers (OIDs)

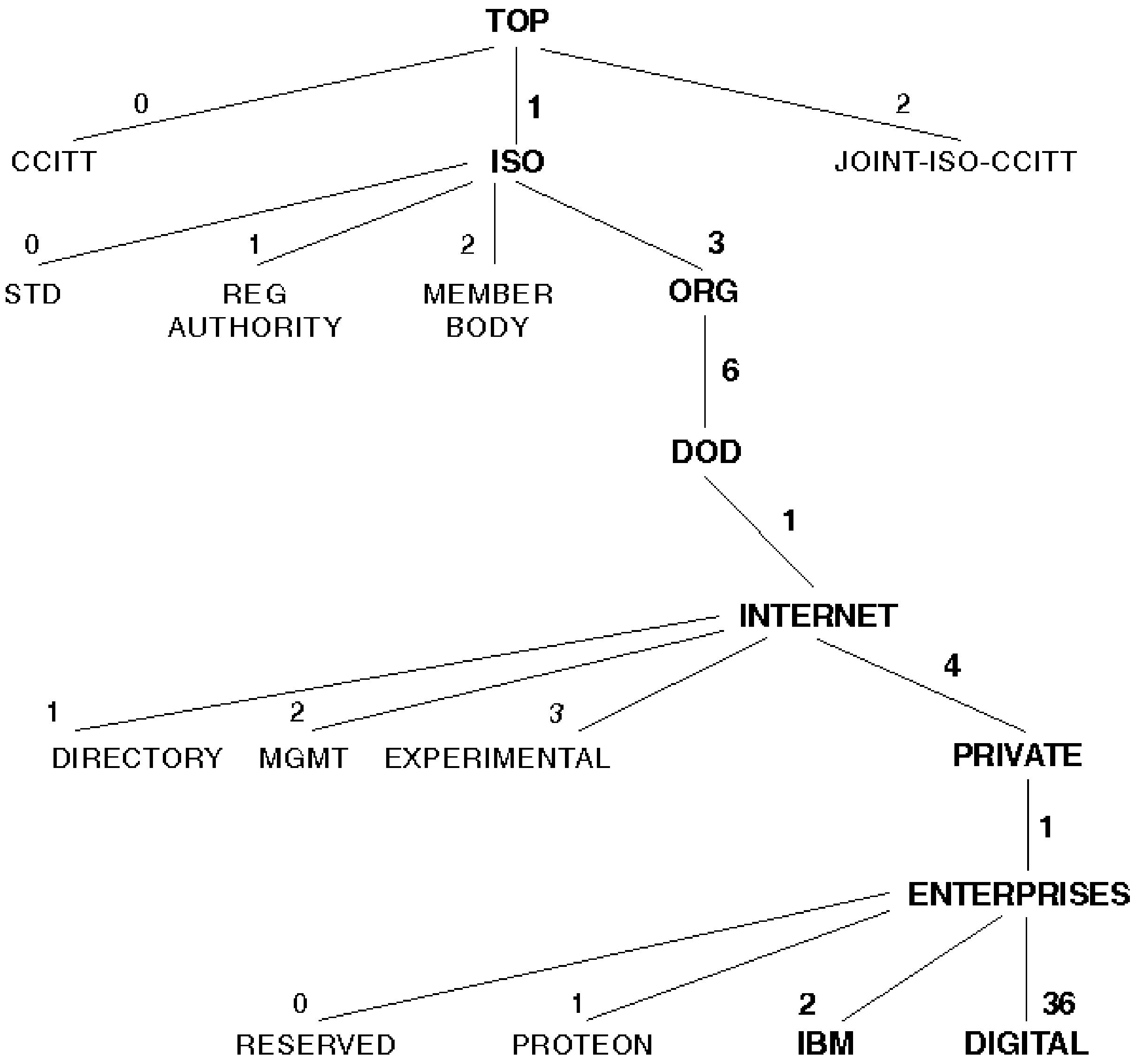
OID are organized into a tree structure that is the MIB

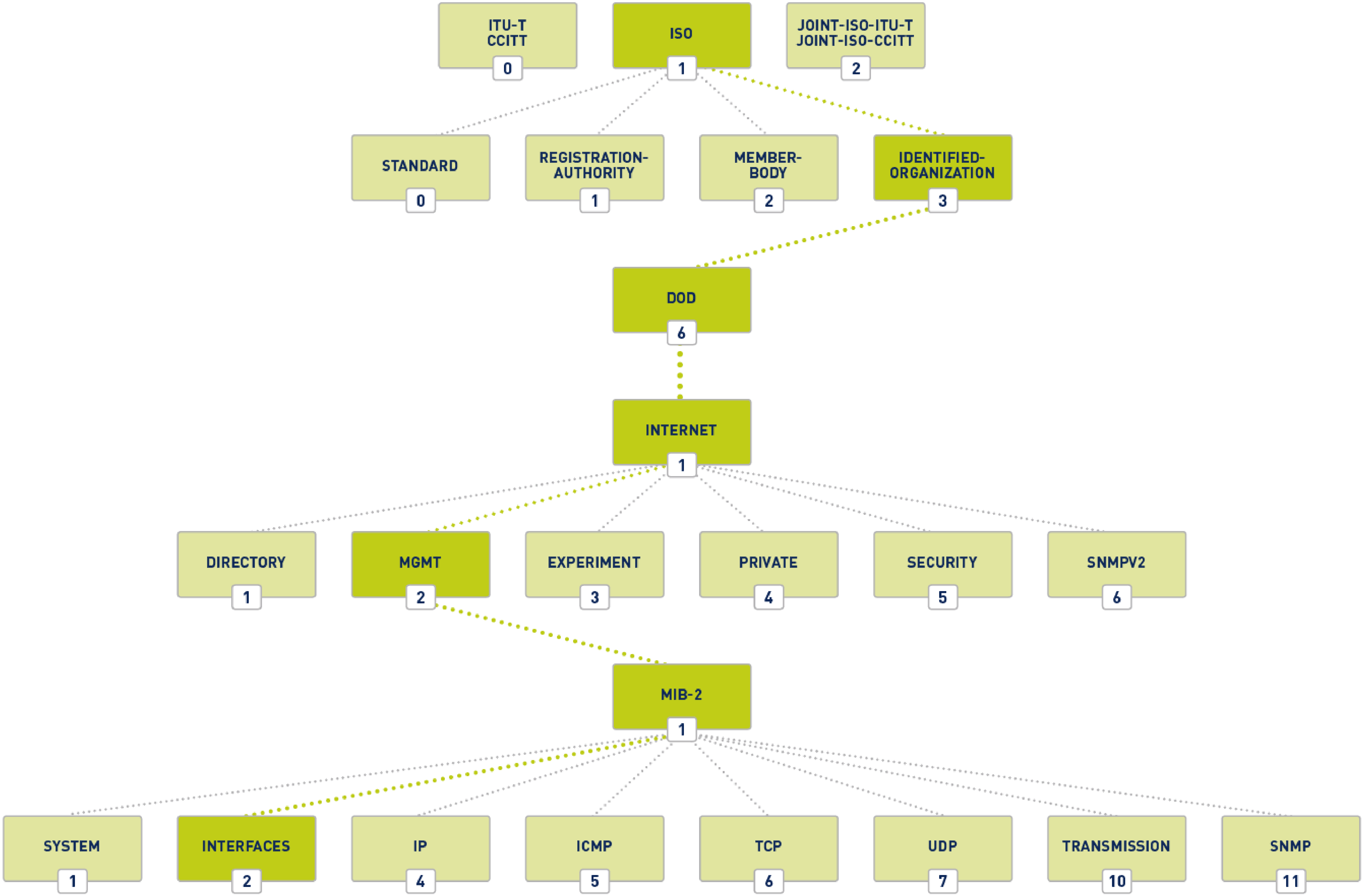
– e.g.

- 1.3.6.1.2.1.1.3

Allocated hierarchically in a tree to ensure uniqueness

Object Identifiers (OIDs)





ITU-T CCITT 0

ISO 1

JOINT-ISO-ITU-T JOINT-ISO-CCITT 2

STANDARD 0

REGISTRATION-AUTHORITY 1

MEMBER-BODY 2

IDENTIFIED-ORGANIZATION 3

DOD 6

INTERNET 1

DIRECTORY 1

MGMT 2

EXPERIMENT 3

PRIVATE 4

SECURITY 5

SNMPV2 6

MIB-2 1

SYSTEM 1

INTERFACES 2

IP 4

ICMP 5

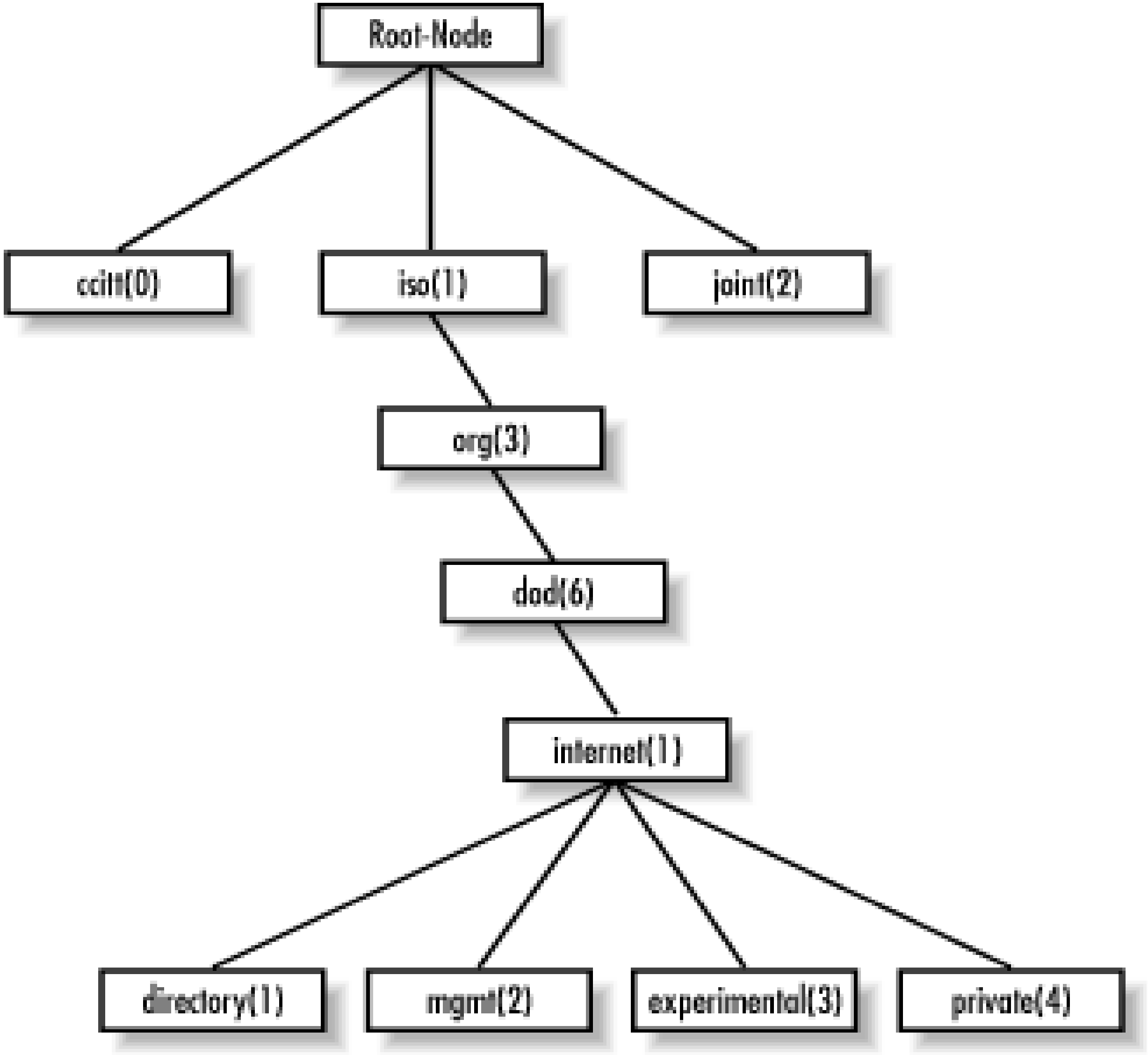
TCP 6

UDP 7

TRANSMISSION 10

SNMP 11

Object Identifiers (OIDs)



Naming OID

Root - the node at the top of the tree

Subtree - anything with children

Leaf node - anything without children

In example, root, the starting point for the tree, is called "Root-Node." Its subtree is made up of *ccitt(0)*, *iso(1)*, and *joint(2)*.

Naming OID

illustration, *iso(1)* is the only node that contains a subtree; the other two nodes are both leaf nodes. *ccitt(0)* and *joint(2)* do not pertain to SNMP.

The *ccitt* subtree is administered by the International Telegraph and Telephone Consultative Committee (CCITT); the *joint* subtree is administered jointly by the International Organization for Standardization (ISO) and CCITT. As we said, neither branch has anything to do with SNMP.

Naming OID

iso(1).org(3).dod(6).internet(1) subtree

which is represented in OID form as *1.3.6.1* or as *iso.org.dod.internet*.

Each managed object has a numerical OID and an associated textual name. The dotted-decimal notation is how a managed object is represented internally within an agent; the textual name, like an IP domain name, saves humans from having to remember long, tedious strings of integers.

MIB tree

The Internet MIB, .1.3.6.1, really only two branches of interest:

Standard MIBs.1.3.6.1.2.1 = .iso.org.dod.internet.mgmt.mib-2

Vendor-specific (proprietary) MIBs.1.3.6.1.4.1 = .iso.org.dod.internet.private.enterprises

Which layer SNMP operates ?

1. Application (layer 7)
2. Data link (layer 2)
3. Network (layer 3)
4. Session (layer 5)

Some SNMP Commands

```
snmpget -Os -c comstring -v 2c IP system.sysName.0
```

```
sysName.0 = STRING: pcopenemr.medicine.kln.ac.lk
```

```
snmpget -v 2 -c comstring IP system.sysUpTime.0
```

```
DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (23714814) 2 days, 17:52:28.14
```

```
snmpget -V
```

SNMP failure: no response?

- The device might be offline or unreachable
- The device might not be running an SNMP agent
- The device might be configured with a different community string
- The device might be configured to refuse SNMP queries from your IP address

In all of these cases you will get no response

Thank You

D.I.K.Solangaarachchi /
FoM,UoK

Email: solanga@kln.ac.lk