# SNMP AND SYSLOG

M M Zaheer HUSSAIN *Bsc (Hons).IT, MCSE, CCNA*

Network Manager

The Open University of Sri Lanka

E-Mail : nmanager@ou.ac.lk

Mobile : 0777-941336

# Outline

- Definition of SNMP
- SNMP Components
- Overview of MIB
- MIB Structure
- SNMP Commands

- Definition of SYSLOG
- SYSLOG Overview
- SYSLOG Features

- Practical exercise on SNMP & SYSLOG

# SNMP

# Definition of SNMP

- SNMP stands for **Simple Network Management Protocol** and is an application layer protocol for exchanging management information between network devices.

- SNMP Versions
  - v1 : 1988 & community strings (Basic)
  - v2 & v2c : 1993 & community strings (Basic)
  - v3 : 1999 & community strings (more security)

- SNMP is work with UDP ports
  - SNMP Agents port no:161. (Polling)
  - SNMP Managers port no:162. (Traps)

# SNMP Components

- SNMP Manager :

  an application program that contacts an SNMP agent to query or modify the database at the agent.

- Managed Devices;

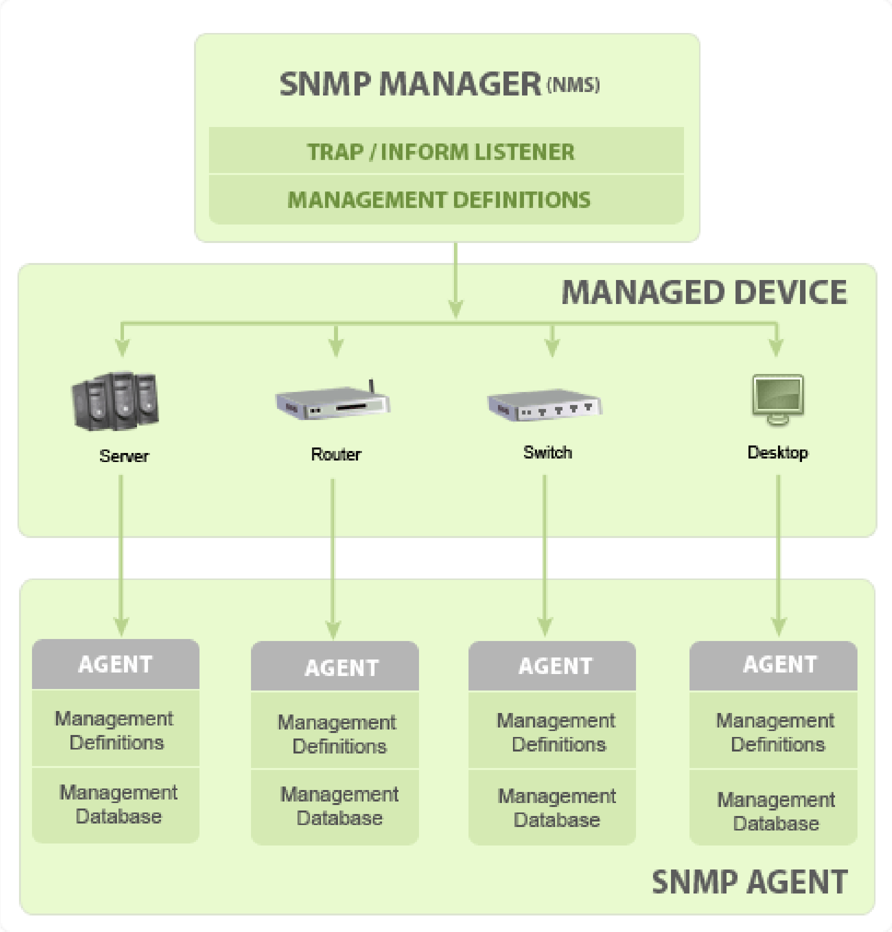
  Part of the network that requires some form of monitoring and management.

- SNMP Agent :

  software that runs on a piece of network equipment and that maintains information about its configuration and current state in a database

- Management Information Base (MIB):

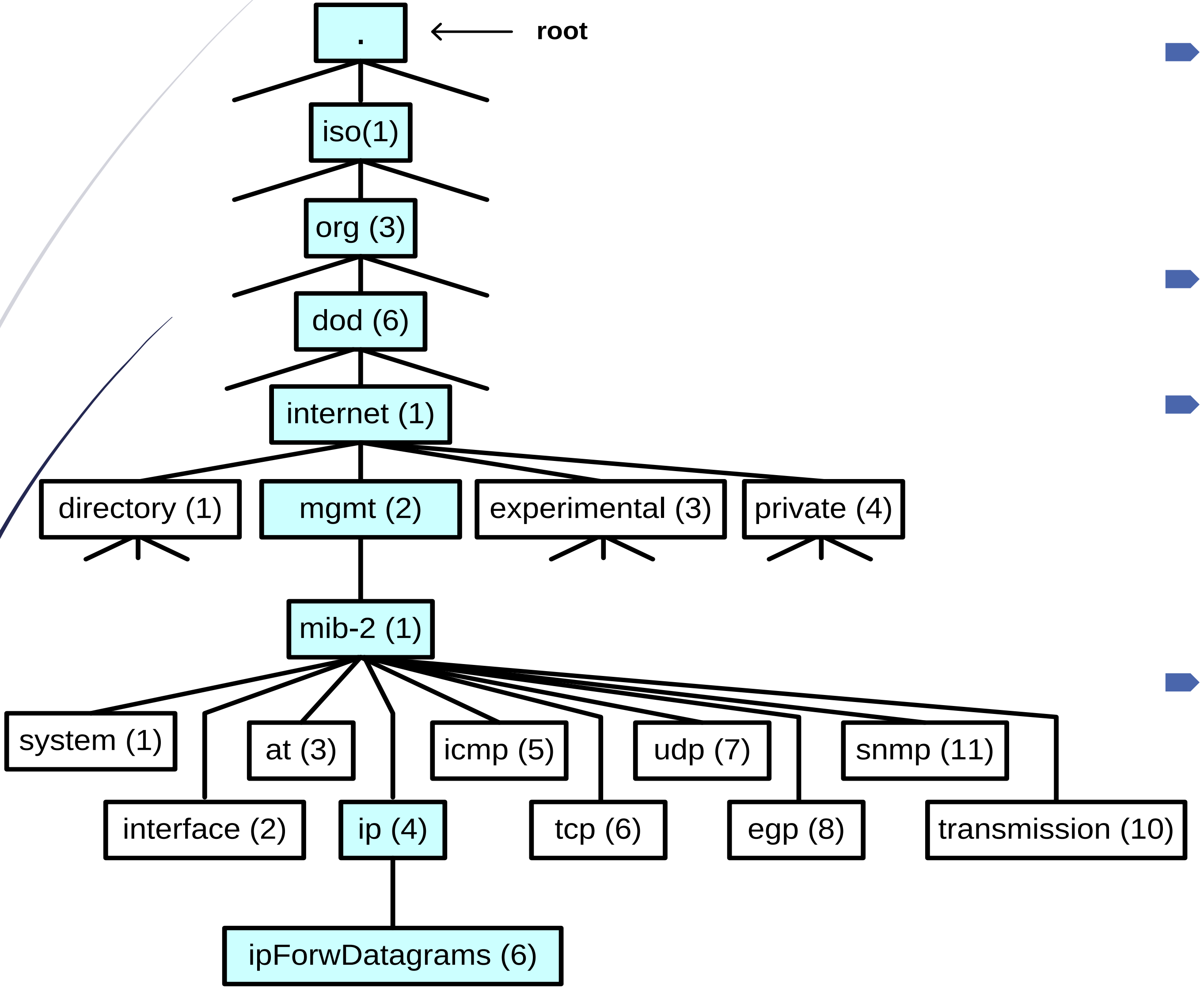
  describes the information in the database.



# Overview of MIB

- The MIBs comprises of managed objects identified by the name Object Identifier (Object ID or OID).
- There are two types of Managed Object or Object ID
  - Scalar : Scalar Object define a single object instance
    - Ex : Device’s vendor name
  - Tabular : Tabular object defines multiple related object instance that are grouped together in MIB tables
    - Ex : CPU utilization of a Quad Processor
- Every Object ID is *organized hierarchically in MIB*. The MIB hierarchy can be represented in a tree structure with individual variable identifier.
- A typical object ID will be a dotted list of integers. For example, the OID in RFC1213 for "*sysDescr*" is *.1.3.6.1.2.1.1.1*

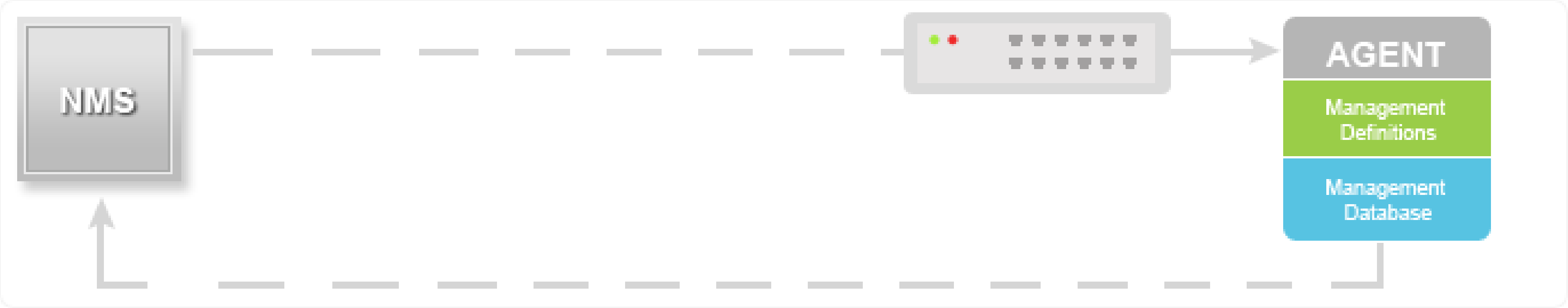
# MIB Structure



- Managed objects are organized in a tree-like hierarchy and the OIDs reflect the structure of the hierarchy.
- Each OID represents a node in the tree.
- The OID 1.3.6.1.2.1 (*iso.org.dod.internet.mgmt.mib-2)* is at the top of the hierarchy for all managed objects of the MIB-II.
- Manufacturers of networking equipment can add product specific objects to the hierarchy.

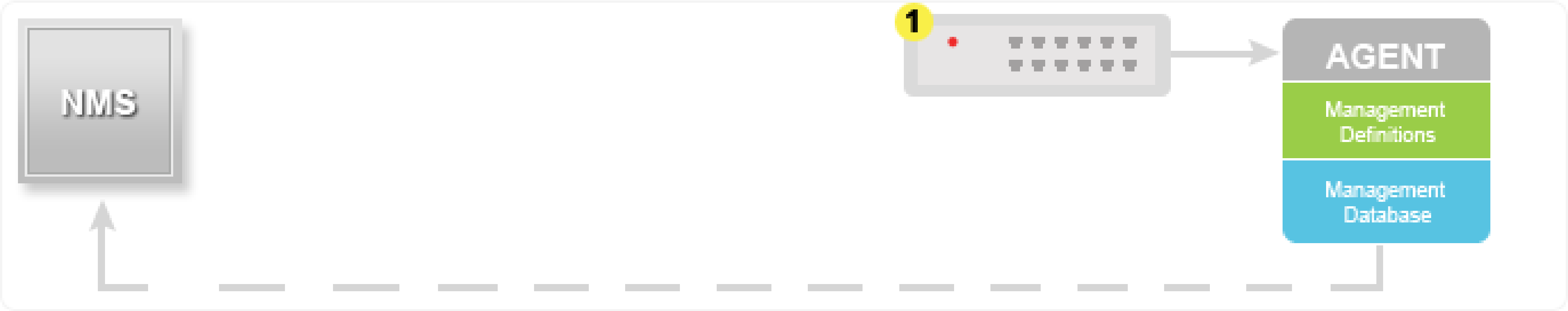
# SNMP Commands

- **Get-request.** Requests the values of one or more objects
- **Get-next-request.** Requests the value of the next object, according to a lexicographical ordering of OIDs.
- **Set-request.** A request to modify the value of one or more objects
- **Get-response.** Sent by SNMP agent in response to a *get-request, get-next-request, or set-request* message.



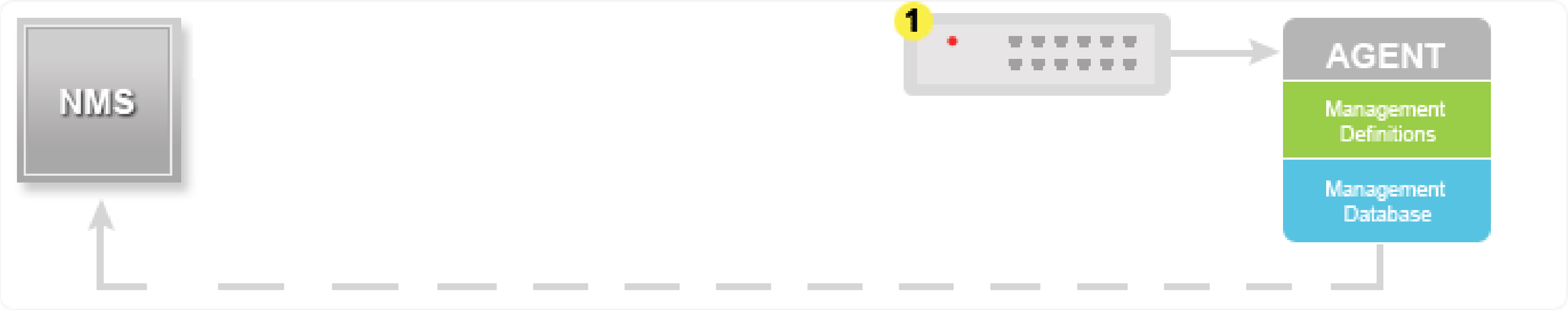
# SNMP Commands

- **Trap.** An SNMP trap is a notification sent by an SNMP agent to an SNMP manager, which is triggered by certain events at the agent.



# SNMP Commands

- **INFORM**: This command is similar to the TRAP initiated by the Agent, additionally INFORM includes confirmation from the SNMP manager on receiving the message.
- **RESPONSE**: It is the command used to carry back the value(s) or signal of actions directed by the SNMP Manager.



# SYSLOG

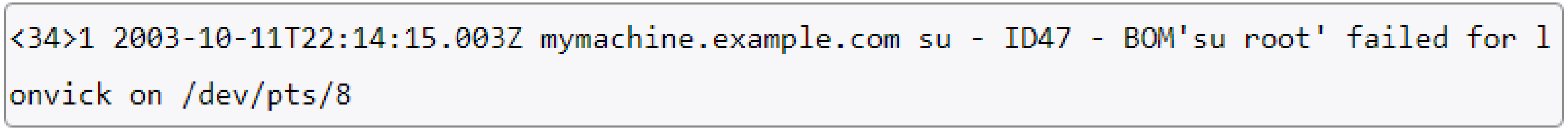
# Definition of SYSLOG

- Syslog is a standard for sending and receiving notification messages–in a particular format–from various network devices.
- The Syslog protocol was initially written by *Eric Allman* and is defined in RFC 3164.
- Syslog uses the UDP and Port 514.

# Standard Format of SYSLOG

- Syslog has a standard definition and format of the log message defined by RFC 5424
- The messages include,
  - Priority
  - Version
  - Timestamp
  - Hostname & IP
  - Severity
  - Application
  - Process id
  - Message id

Example:



```
<34>1 2003-10-11T22:14:15.003Z mymachine.example.com su - ID47 - BOM'su root' failed for l
onvick on /dev/pts/8
```

# SYSLOG Severity levels

| ID | Levels | Meaning |
|---|---|---|
| Emerg | 0 | Panic situations (hardware failure, crash) |
| Alert | 1 | Urgent situations |
| Critical | 2 | Critical situations |
| err | 3 | Non-critical errors. |
| warning | 4 | Warnings. |
| notice | 5 | Might merit investigation. |
| info | 6 | Informational messages. |
| debug | 7 -10 | Debugging (typically enabled temporarily) |

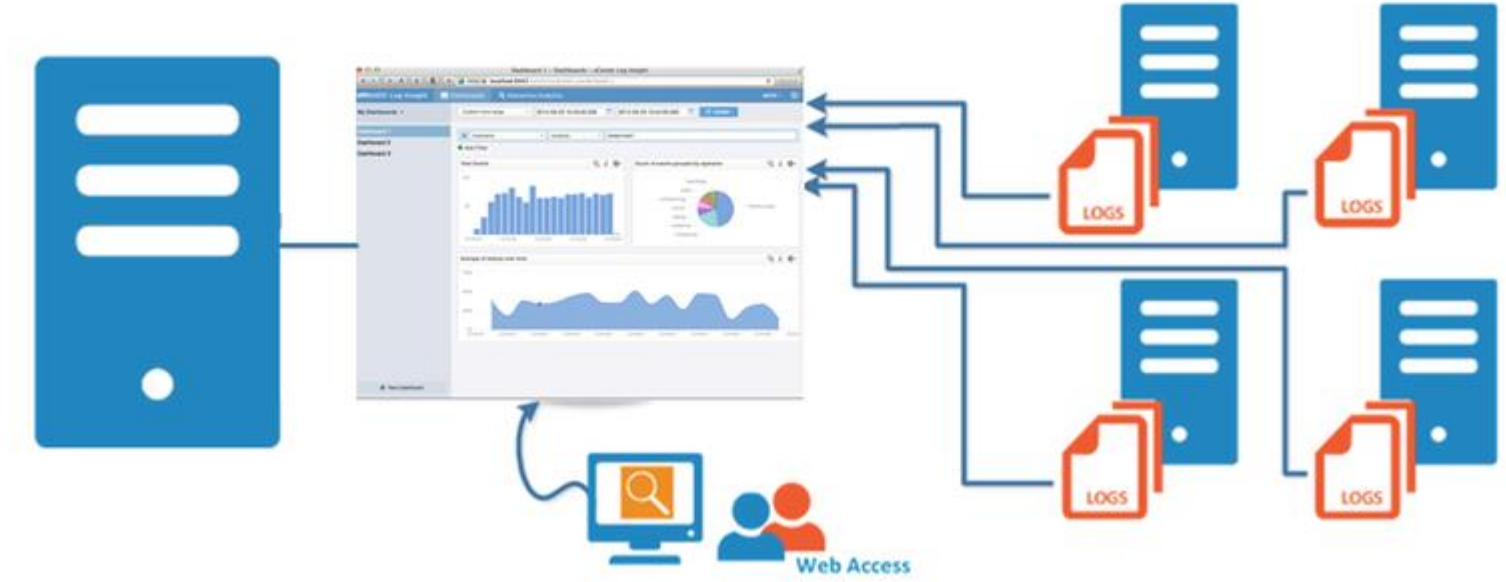
# SYSLOG Facilities

| Facility | Used By |
|---|---|
| kern | The kernel |
| user | User processes (default) |
| mail | Mail servers and related software. |
| daemon | System daemons (except mail, cron) |
| auth | Security and authorization-related commands. |
| lpr | Print server and related commands. |
| cron | Cron daemon. |
| local0-7 | Eight local levels for other programs. |

# SYSLOG Analysis

- The term used for analysis of computer-generated records for helping organizations, businesses or networks in proactively and reactively mitigating different risks.

  Example : centralized syslog server.



# Reference (source):

- https://www.manageengine.com/network-monitoring/what-is-snmp.html
- https://en.wikipedia.org/wiki/Simple_Network_Management_Protocol
- https://en.wikipedia.org/wiki/Syslog

# LIVE DEMO

- Practical exercise
  - SNMP
  - SYSLOG

# Thank You!

Free to reach me

E-Mail : nmanager@ou.ac.lk

Mobile : 0777-941336

LkNOG

LANKA NETWORK OPERATORS GROUP