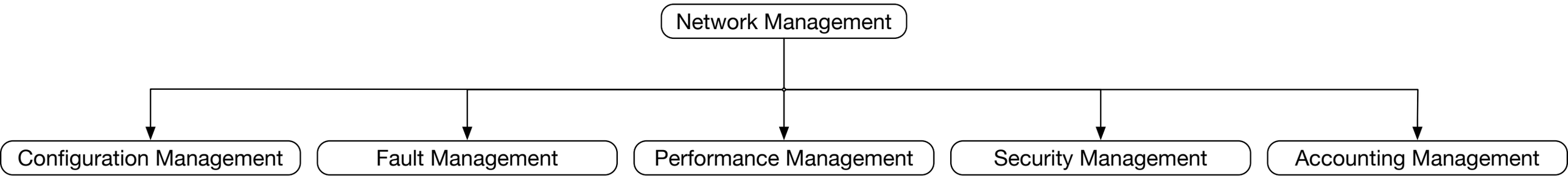
# Network Management

Thomas Schwarz, SJ

# Network Management




ISO taxonomy of Network Management

# Configuration Management

- Large networks are made up of hundreds of entities
  - are in constant flux
- Configuration Management:
  - Keeps track the status and relationship of any and all entity

# Configuration Management

- Reconfiguration Management
  - Hardware reconfiguration
  - Software reconfiguration
  - User-account reconfiguration
    - Adding, deleting accounts and privileges

# Configuration Management

- Documentation Management
  - Hardware Documentation
    - *Maps:* Track each piece of hardware and its connection to the network
      - Can be subdivided: E.g.: logical map of subnets plus subnet maps
    - *Specifications:* Each hardware connected to the network is documented: hardware type, serial number, vendor, time of purchase, warranty, …

# Configuration Management

- Documentation Management
  - Software Documentation
    - All software is documented: type, version, installed, licence, …
  - User Account Documentation
    - OS have user account documentation
    - These files need to be secured and updated

# Fault Management

- Reactive Fault Management
  - Detecting, isolating, correcting and recording faults
- Proactive Fault Management
  - Prevent faults from occurring:
    - Based on component lifetime, history of failures, …

# Performance Management

- Monitor and control network for efficient running
- Use measurable performance quantities:
  - Capacity, traffic, throughput, response time
  - Uses often SNMP

# Security Management

- Control access to the network based on predefined policies

# Accounting Management

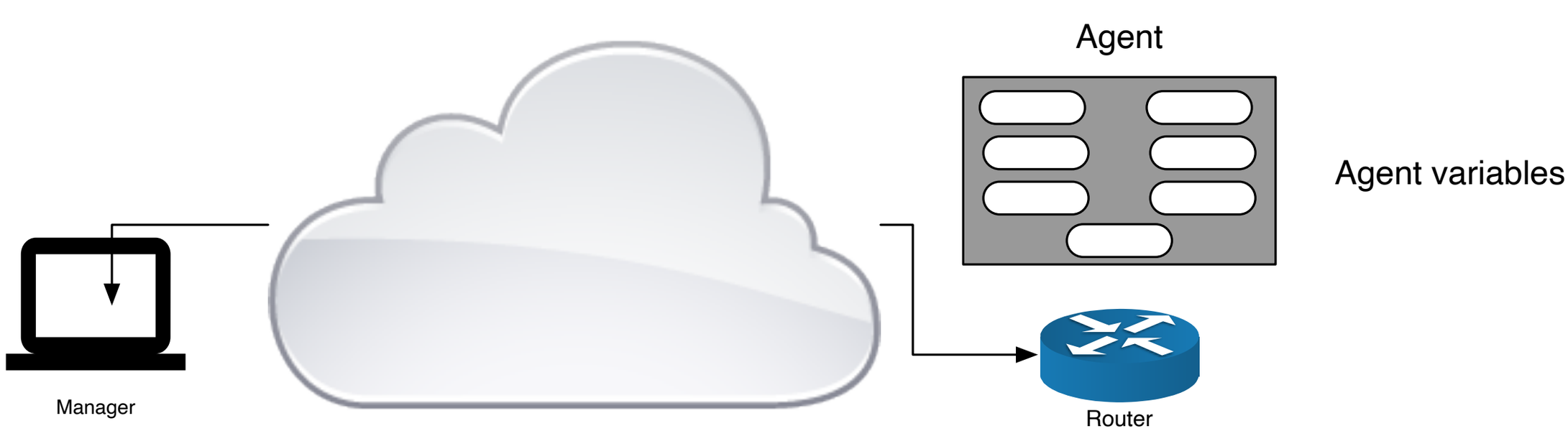
- Control access by users through charges
  - Prevents users from monopolizing limited network resources
  - Prevents users from using the system inefficiently
  - Allows network managers to plan based on the demand for network use

# SNMP:
# Simple Network Management Protocol

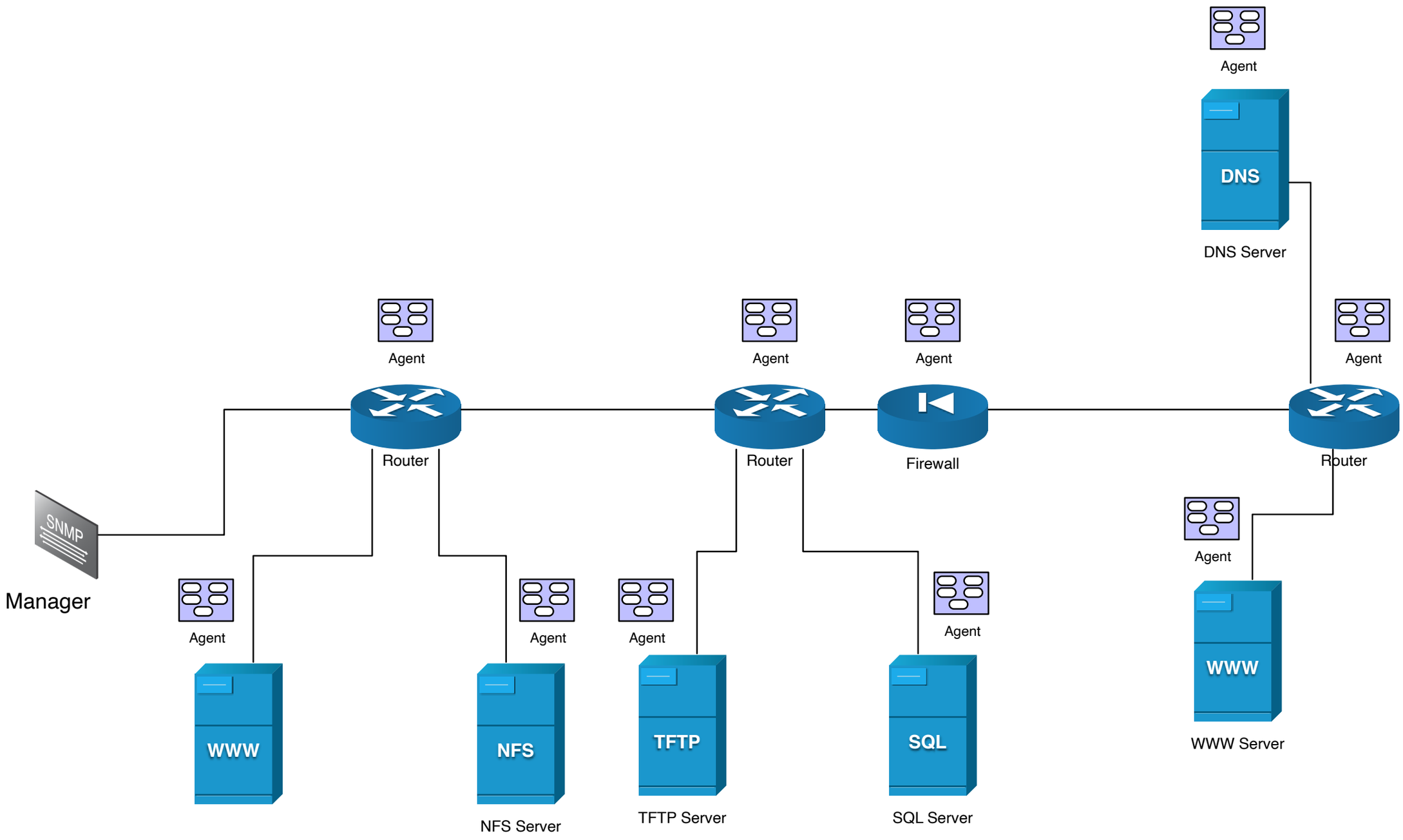
- SNMP provides operations for monitoring and maintaining a network
- Uses TCP/IP
- A manager controls and monitors a set of agents (routers and servers)

# SNMP:
# Simple Network Management Protocol

- The state of an entity is captured in the abstraction of an agent



# SNMP:
# Simple Network Management Protocol



# SNMP:
# Simple Network Management Protocol

- Manager
  - Host that runs the SNMP client program
- Agent:
  - Router or host that runs the SNMP server program
- Management:
  - Simple interactions between a manager and an agent.

# SNMP:
# Simple Network Management Protocol

- SNMP:
  - Uses MIB
    - Management Information Basis
  - and SIB
    - Structure of Information Base

# SNMP:
# Simple Network Management Protocol

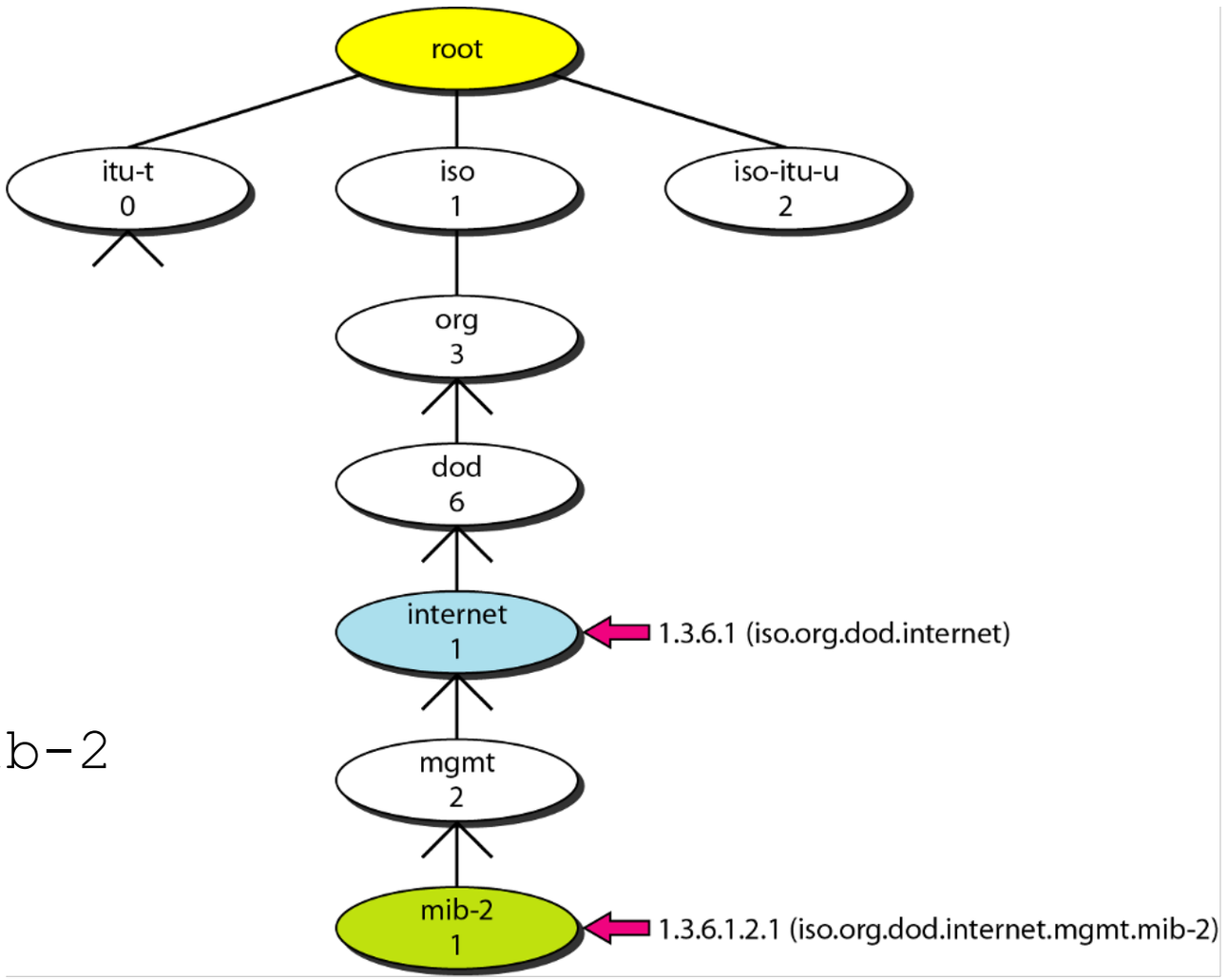
- Structure of Information Management
  - Defines the meaning of the data exchanged
  - Gives independence from OS, etc.
  -

# SNMP:
# Simple Network Management Protocol

- Structure of Management Information (SMI)
  - Guideline for SNMP
  - Functions:
    - To name objects
    - Define the type of data that can be stored in an object
    - To show how to encode data for transmission over the network

# SNMP:
# Simple Network Management Protocol

- To name objects: use Object identifiers
  - Based by a tree structure
  - Encoded with integers




```
iso.org.dod.internet.mgmt.mib-2

1.3.6.1.2.1
```

# SNMP:
# Simple Network Management Protocol

- Second attribute of an object:
  - Type: ASN.1 simple and compound types
  - With additions for SMI:
    - IPaddress
    - Counter32 / Gauge32
    - Counter64
    - TimeTicks
    - Bits
    - Opaque (uninterpreted string)

# SNMP:
# Simple Network Management Protocol

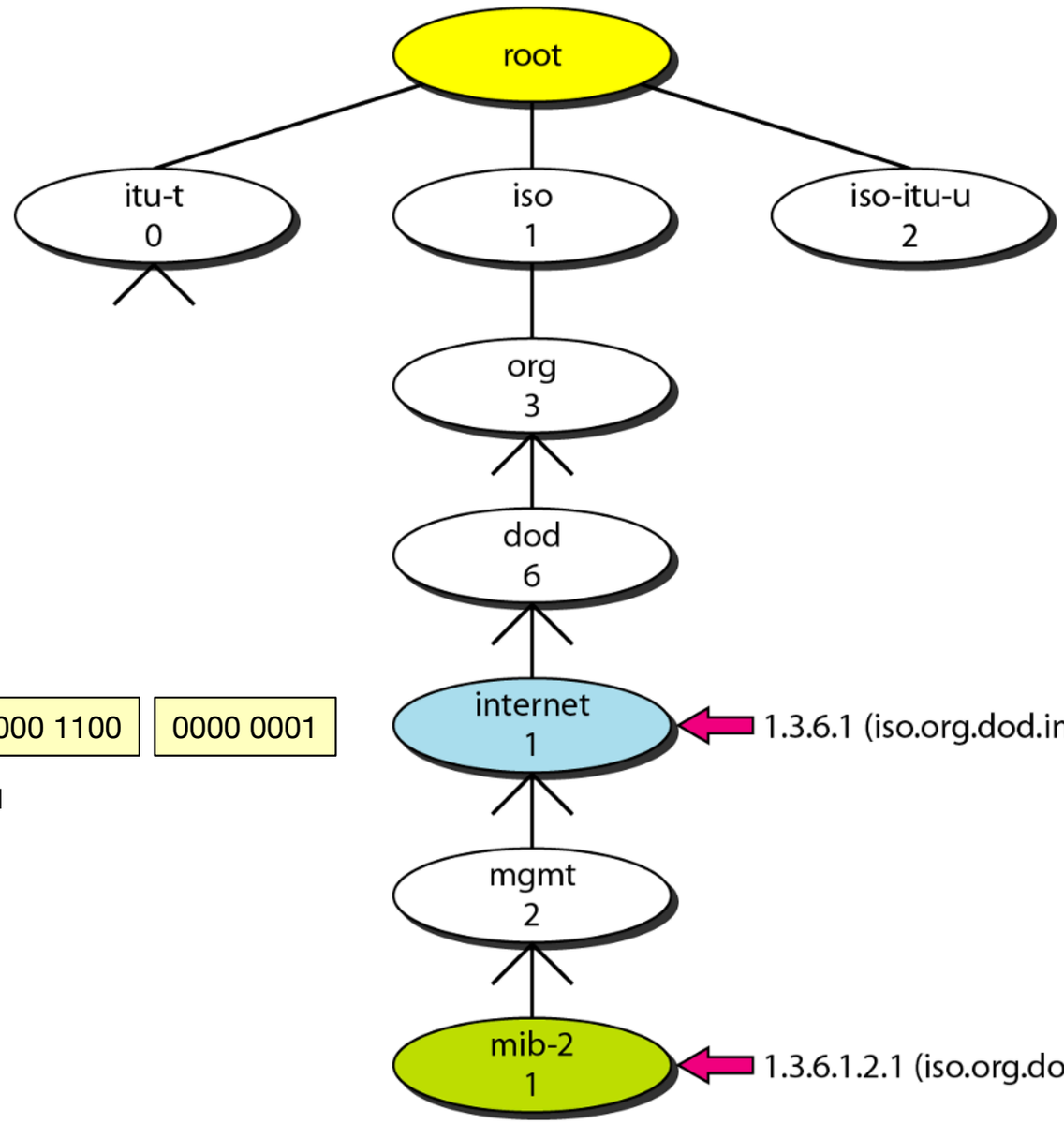
- Second attribute of an object:
  - Type: ASN.1 simple and compound types
  - Compound types:
    - Sequence
      - List in Python
    - Sequence of
      - Array in NumPy

# SNMP:
# Simple Network Management Protocol

- Management Information Base
  - Collection of named objects, types, and relationships in an entity to be managed
  - Each object has an Object Identifier (OID)
    - Manager retrieves value from agent by specifying the OID
    - Example: 1.3.6.1.2.1.1.3 is the SysUptime Object

# SNMP:
# Simple Network Management Protocol

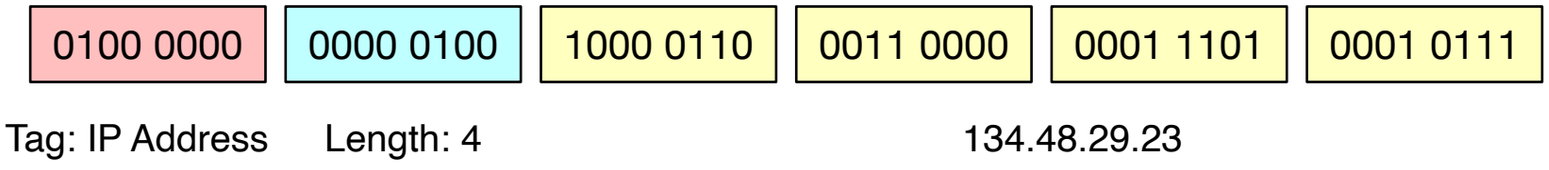
- As seen:
- All SNMP object identifiers start with 1.3.6.1.2.1



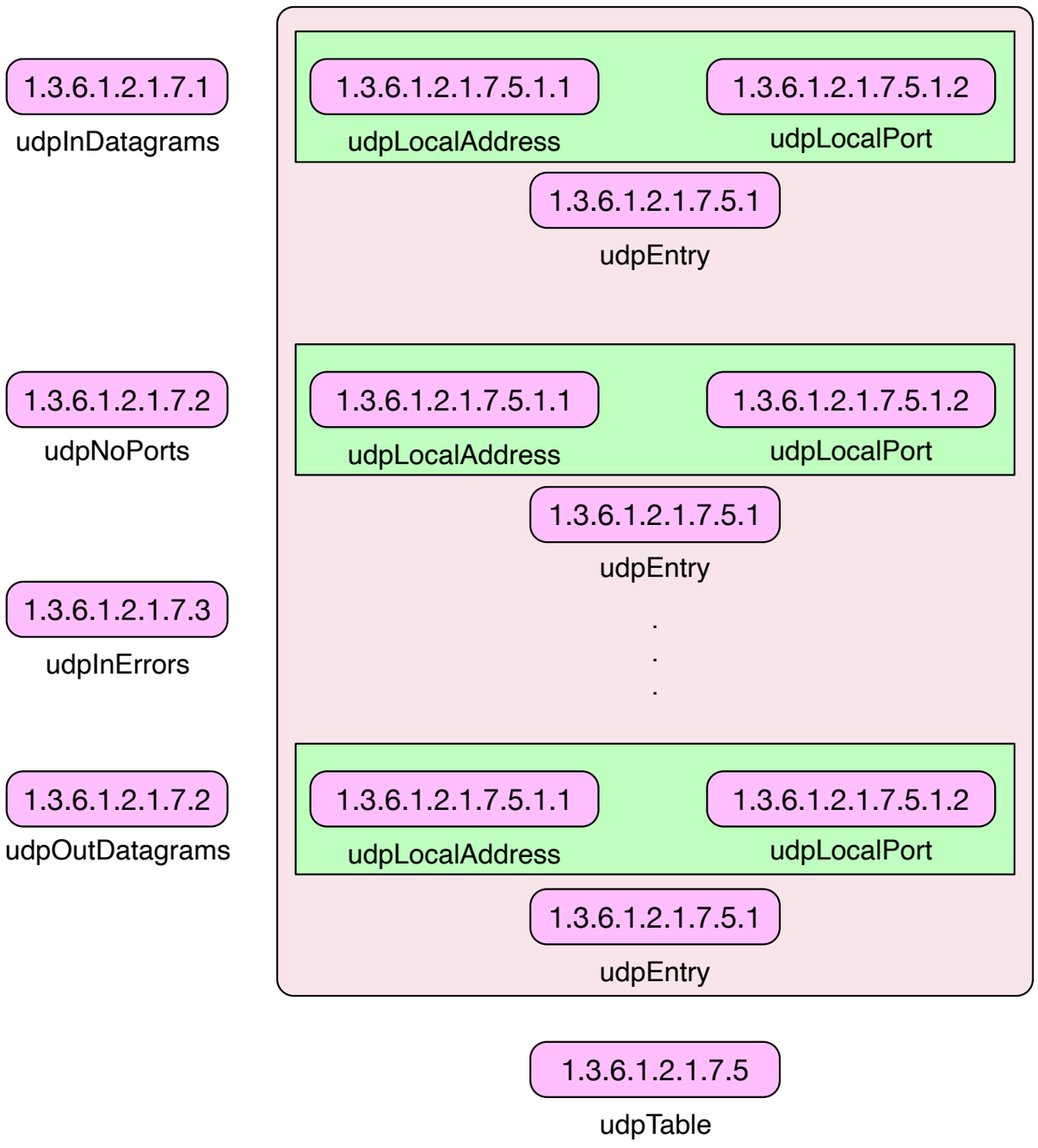

| 0000 0110 | 0000 0100 | 0000 0001 | 0000 0011 | 0000 1100 | 0000 0001 |
|---|---|---|---|---|---|

Tag: IP Address  Length: 4  1.3.6.1

# SNMP:
# Simple Network Management Protocol



# SNMP:
# Simple Network Management Protocol

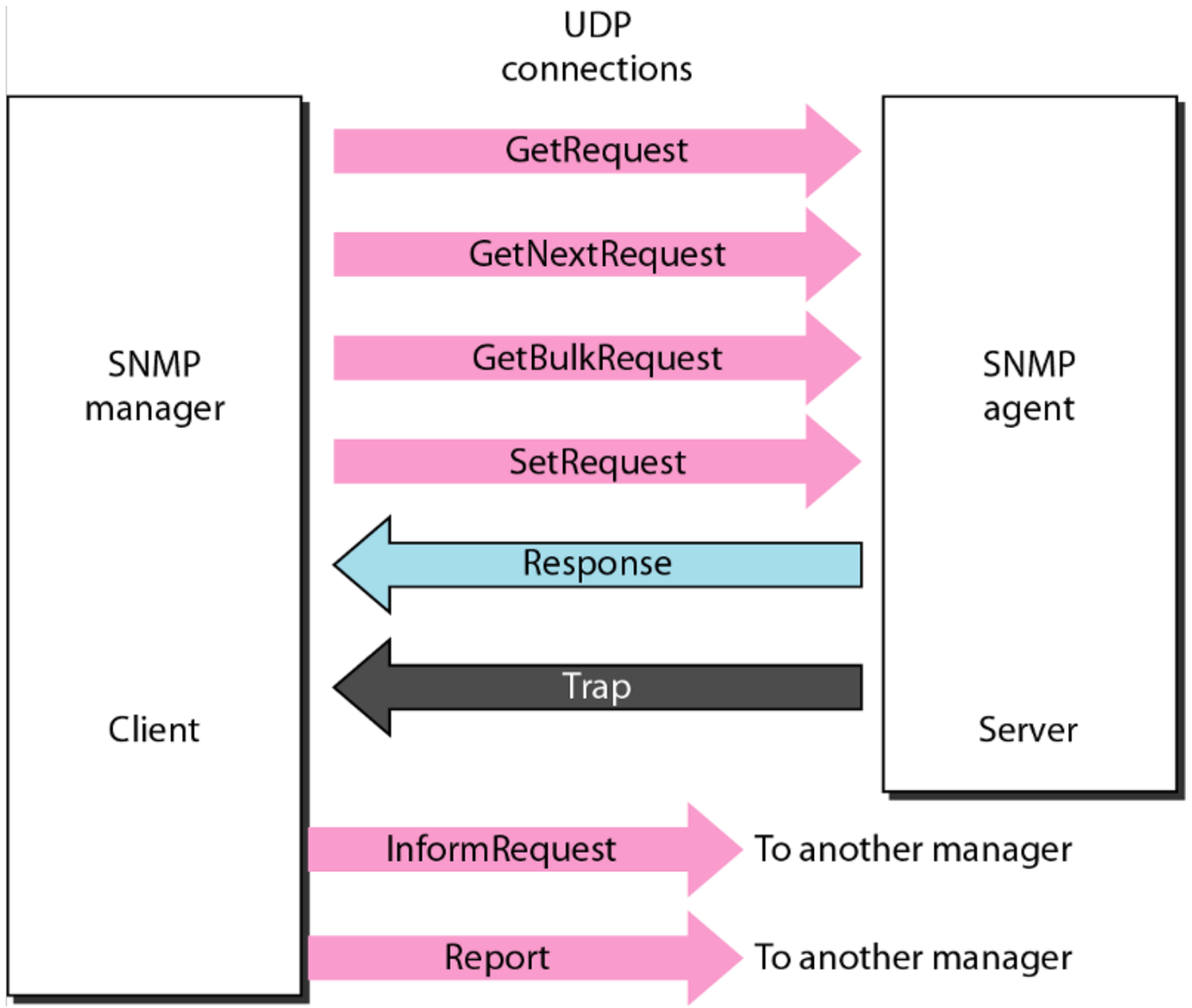



MIB entry for UDP

# SNMP:
# Simple Network Management Protocol

- Agents collect usage data locally and update MIB values accordingly
- Network Management System (NMS) polls / requests the agent
- Agents use traps to inform NMS
  - UDP 161: Used when management stations communicate with agents, e.g. Polling
  - UDP 162: Used when agents send unsolicited Traps to the management station

# SNMP:
# Simple Network Management Protocol

- Currently in Version 3
  - With security, authentication, passwords, etc.
- Before: community strings (common passwords) sent in plain text (version 1, 2)

# SNMP:
# Simple Network Management Protocol