SNMPv1 Network management:

Organization, Information, communication and functional models

- SNMP organization model
  - SNMP Manager
  - SNMP Agent
  - Network element

- Two tier

    - Manager/Agent interaction

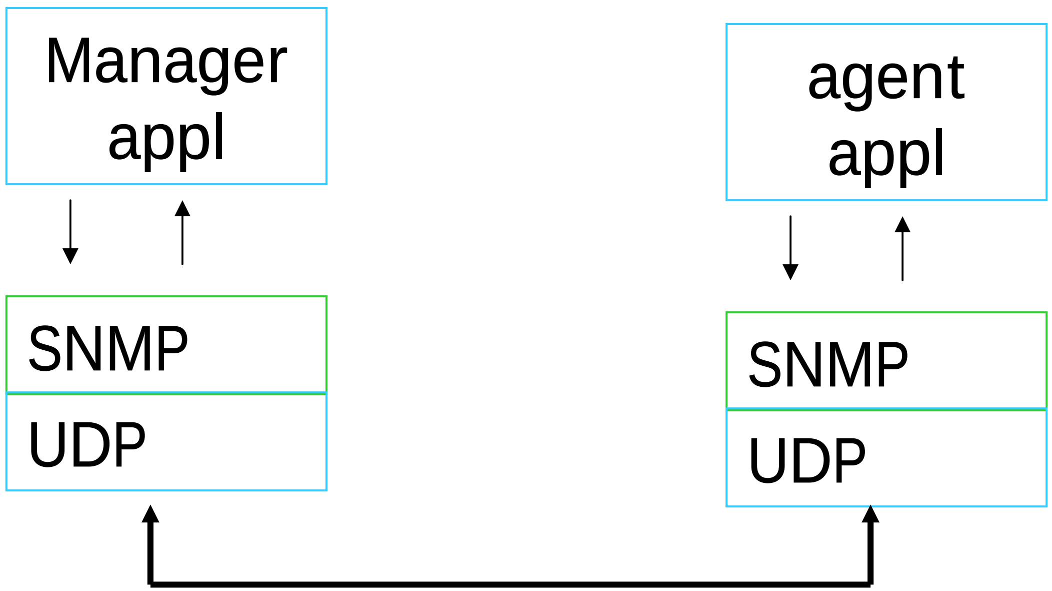
- Multiple managers – one agent

- Three tier – with RMON

- The proxy server organization model

- Dual role of SNMP manager

- SNMP network management Architecture
  - Location in layered network protocol architecture
  - The transport protocol



- SNMP network management Architecture
    - Protocol messages - Five in number
    - Manager initiated
        - Get-request:
        - Get-next-request:
        - Set-request:
    - Agent initiated
        - Get-response:
        - Trap:

- System overview - SNMP network management Architecture

  - Trap:
    - Generic trap: eg
      - coldStart, warmStart, linkUp, linkDown
    - Specific-trap
    - Timestamp

  - Some traps are application specific

- System overview - SNMP network management Architecture

  - Manager databases
    - MIB – information about objects
    - MDB – the (measured) values associated with the objects
    - MIB is compiled in the manager during implementation.
    - Detected object that is not in MIB

      ⇒Marked as unidentifiable

- System overview - SNMP network management Architecture

  - Agent database

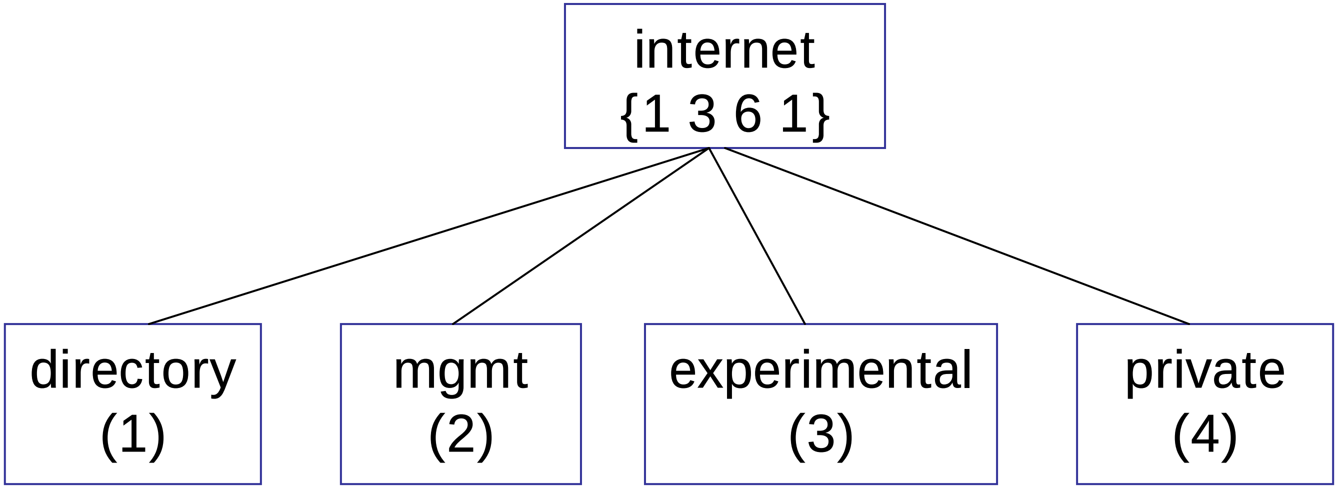
    - Agent has no physical database but also has a MIB compiled in the software module.

The Information Model

(similar to ISO)

- The Information Model
  - SMI: structure of managed information
    - MIB
  - Objects that can be managed by SNMP-compatible NMS include
    - Generic objects defined by IETF
    - Objects defined by private vendors, if they conform to specs
    - Specialized network objects, e.g. FDDI, OSPF, and ATM

- The Information Model
  - SMI - MIB tree
  - The internet MIB

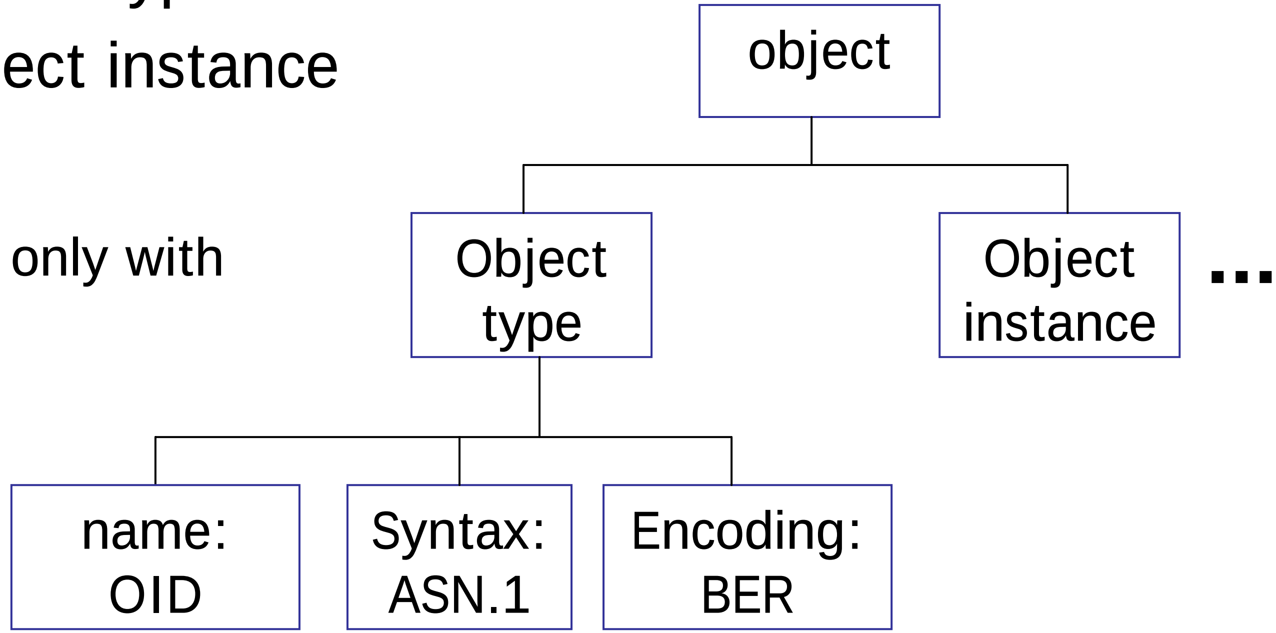


- The Information Model
  - The SMI

A managed objects consists of

- Object type
- Object instance

•SMI is concerned only with object type



- ASN.1

- ASN.1
  - A formal language developed by CCITT and ISO for use with application layers for data transfer between systems.
  - Abstract syntax
    - Set of rules used to specify data types and structures for storage of information
  - Transfer syntax
    - Set of rules for communicating information between systems

- ASN.1

Terminology, symbols and conventions

- ASN.1 is based on BNF

- Entity definitions

  <entity> ::= <definition>

  - <entity> : data type
  - <definition> : construct made of key words, data types and meta-symbols

- ASN.1
  - meta-symbols

::=	-	defined as
|	-	alternatives
{ }	-	list
[ ]	-	tag
( )	-	subtype
..	-	range

- ASN.1
  - Keywords

BEGIN	;start of module
CHOICE	;list of alternatives
DEFINITIONS	;definitions of data types
END	; end of module
EXPORTS	;type that can be exported
IDENTIFIER	;a sequence of non-negative integers
IMPORTS	;types defined in external modules
INTEGER	;negative or non-negative integer

- ASN.1
  - Keywords

NULL	;place holder
OBJECT	; used with IDENTIFIER
OCTET	;8-bit byte of data
SEQUENCE	;ordered list
SEQUENCE OF	;ordered array of repetitive data
SET	;un-ordered list
SET OF	;un-ordered array of repetitive data
STRING	;use with OCTET

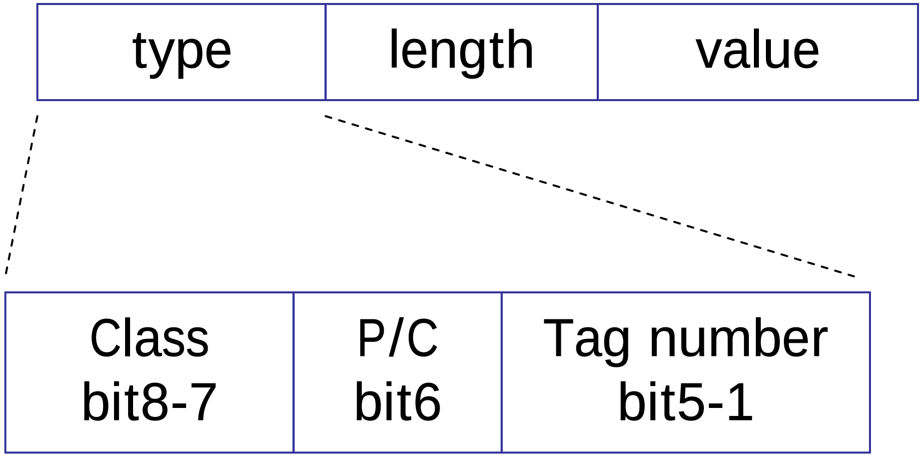
- SNMP-Based ASN.1 Data types

Structure	*Data type*	*comments*
Primitive	INTEGER	;subtype INTEGR(n1..n2)
types	OCTET STRING	;8-bit bytes of data
	OBJECT IDENTIFIER	; position in MIT
	NULL	;place holder
Defined	NetworkAddress	
types	IpAddress	
	Counter	
	Gauge	
	TimeTicks	
	Opaque	
Constructor	SEQUENCE	;list maker
types	SEQUENCE OF	;table maker

- ASN.1 - encoding structure

- *BER – Basic encoding rules*

  TLV – Type Length Value encoding



type	length	value

Class bit8-7	P/C bit6	Tag number bit5-1

class	*value*
universal	00
application	01
Context spec	10
private	11

P/C – primitive/construct

- The Information Model
  - The SMI
  - A managed objects need not just a network element, but could be any object, e.g.
    - the Internet as an organization

- Object name and identifier

- The Information Model :The SMI
  - Every object type uniquely identified by a
    - DESCRIPTOR and
    - OBJECT IDENTIFIER

DESCRIPTOR

- is mnemonic (starts with lower case letter)

OBJECT IDENTIFIER

- is unique name and number in the MIT

- The Information Model :The SMI

Formats for declaration of descriptor for OBJECT IDENTIFIER

e.g

the internet MIB

internet OBJECT IDENTIFIER ::= {1 3 6 1}

internet OBJECT IDENTIFIER ::= {iso org dod 1}

an object in the internet MIB

mgmt OBJECT IDENTIFIER ::= {internet 2}

private OBJECT IDENTIFIER ::= {internet 4}

mib-2 OBJECT IDENTIFIER ::= {mgmt 1}

- The Information Model :The SMI

e.g

the enterprise MIB

enterprise OBJECT IDENTIFIER ::= {private 1}

objects in the enterprise MIB

cisco OBJECT IDENTIFIER ::= {enterprise 9}

hp OBJECT IDENTIFIER ::= {enterprise 11}

3com OBJECT IDENTIFIER ::= {enterprise 43}

cabletron OBJECT IDENTIFIER ::= {enterprise 52}

- The Information Model :The SMI

e.g the enterprise MIB

- Assume that your company, unr-es has been given designation 200 in the enterprise MIB. You manufacture two models of hubs, three models of routers and 2 models of modems. Define DESCRIPTORs for each of those products.

- The Information Model :

- The Structure of managed objects

- The Information Model :
- The Structure of managed objects

characteristics
Object type
Syntax
Description
Access
status

Ex. 1

{system 1}
OCTET STRING
“full name and version”
read-only
mandatory

Ex. 2

{…}
SEQUENCE OF IpAdrEntry
“full name and version”
read-only
mandatory

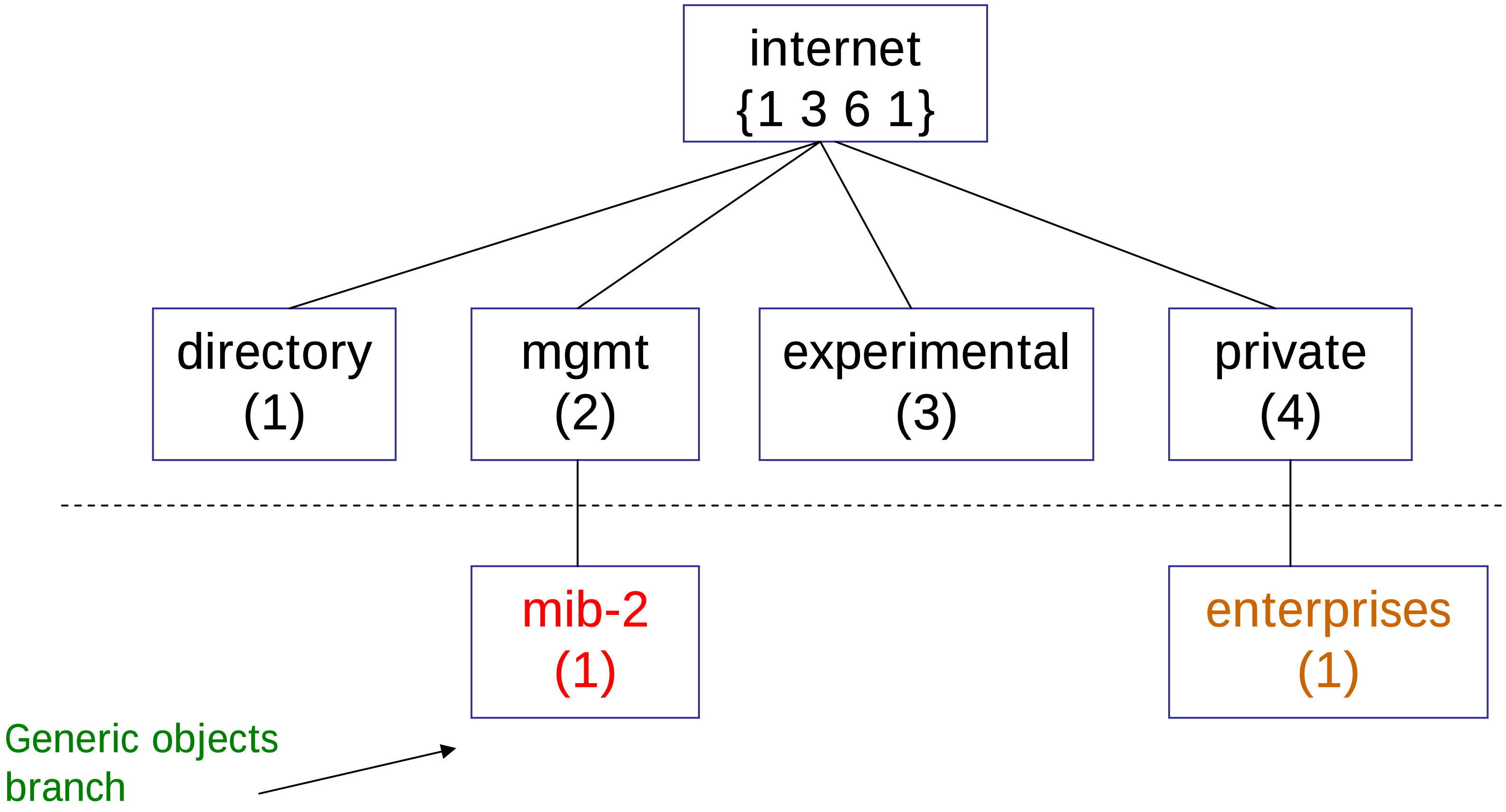
- Exercise
    - Using ASN.1 as appropriate. Provide a definition of the structure of the switch you have used in the practical.

- SNMP Communication model

- Need to know
  - Get-request, set-request

  - Object descriptor
  - Object structure

- The internet MIB group


internet {1 3 6 1}

directory (1)

mgmt (2)

experimental (3)

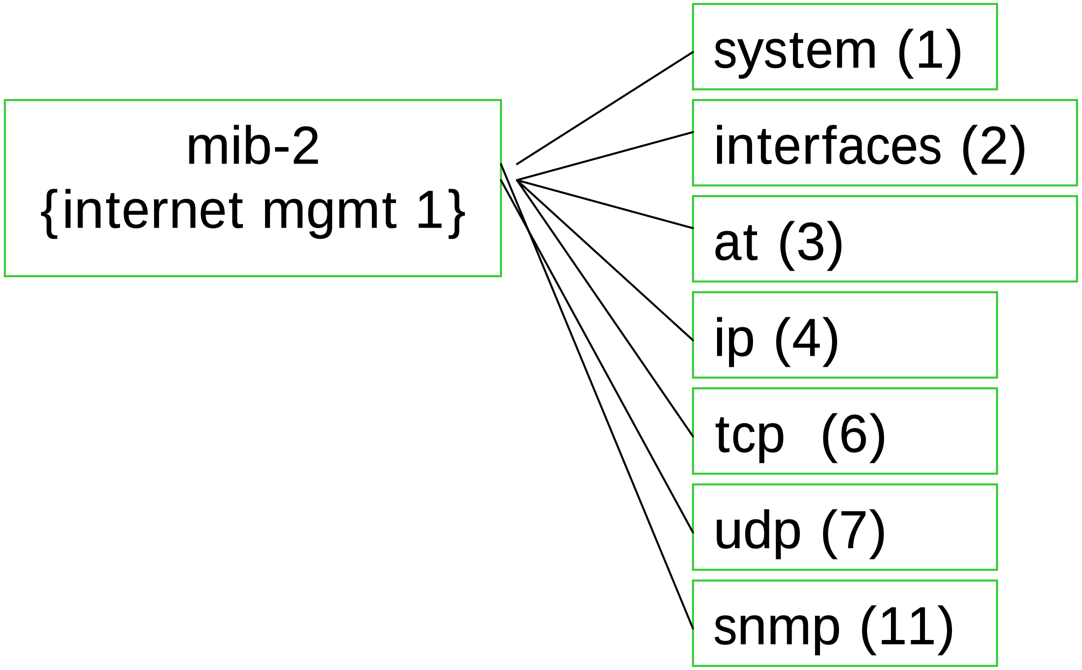
private (4)

mib-2 (1)

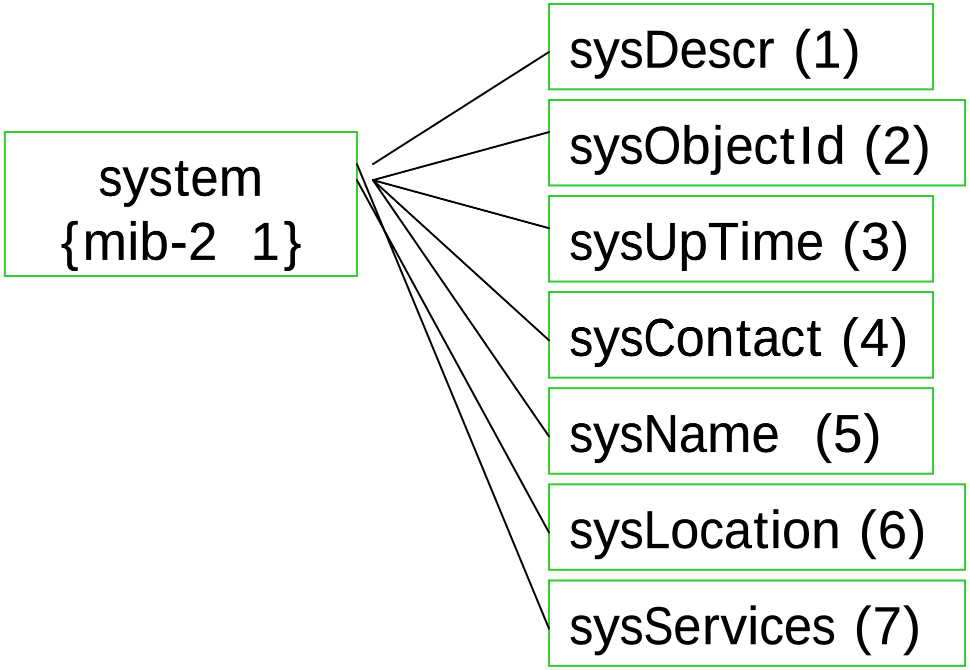
enterprises (1)

Generic objects branch

- The internet mib-2 group



- The system group



The Structure of managed objects:

Formal specification of the object sysDescr

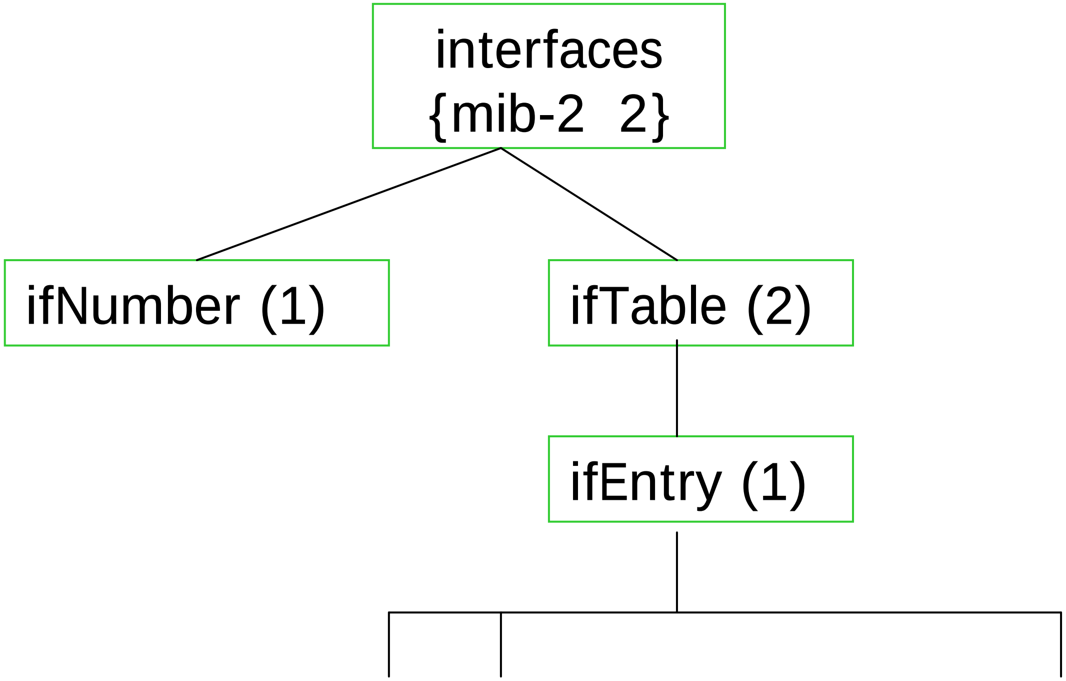
```
    sysDescr OBJECT-TYPE
        SYNTAX       DisplayString (SIZE(0..255))
        ACCESS       read-only
        STATUS       mandatory
        DESCRIPTION      “ ... “
        ::= {system 1}
```

Exercise:

Write the formal specification of the objects

- sysName
- sysLocation
- sysUptime

- The interfaces group



next slide

The Structure of managed objects: ifEntry

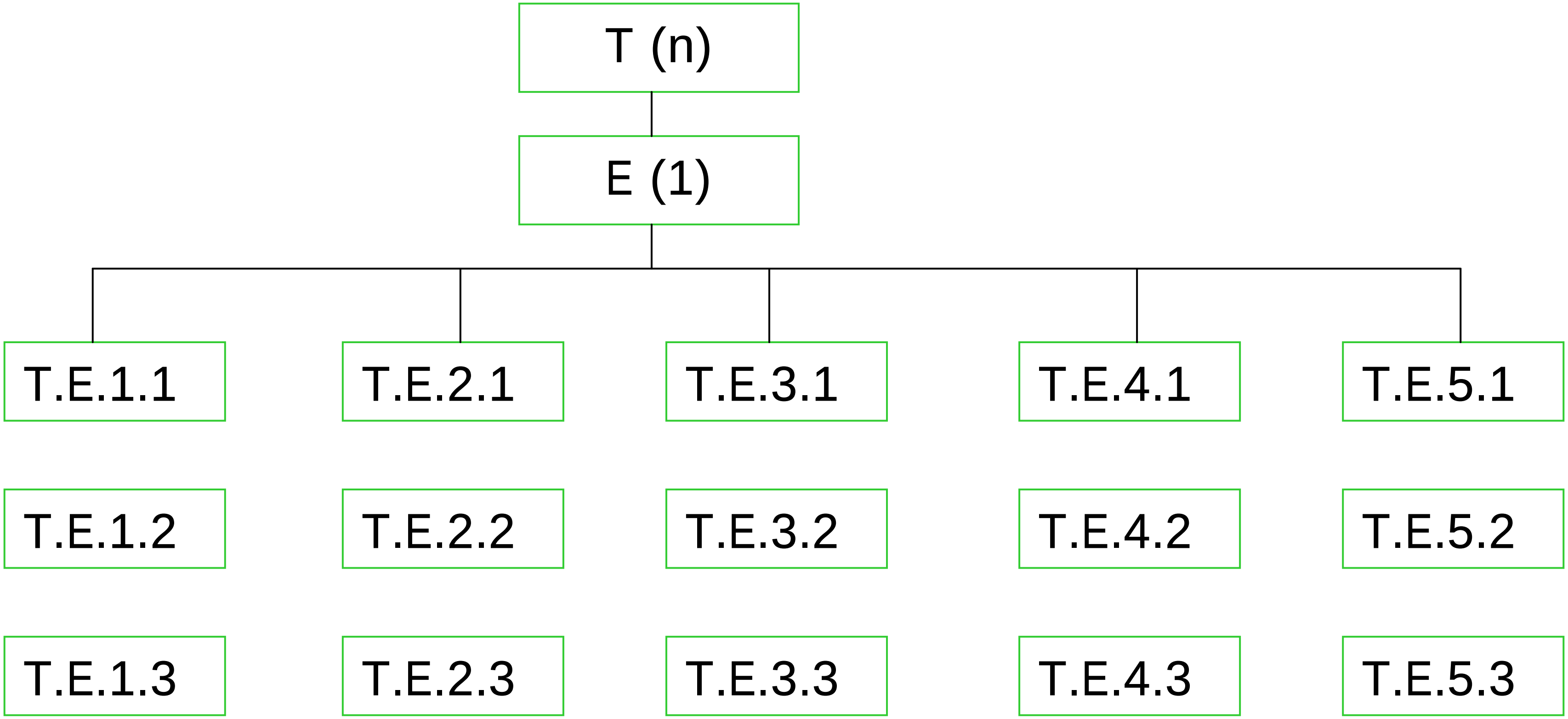
```
ifEntry OBJECT-TYPE
    SYNTAX      IfEntry
    ACCESS      not-accessible
    STATUS      mandatory
    DESCRIPTION     " ... "
    INDEX   {ifIndex}
    ::= {ifTable 1}
```

The Structure of managed objects:

- IfEntry data structure

```
IfEntry ::= SEQUENCE {
    ...
    ...
    }
```

- Structure/order of table entries



T (n)

E (1)

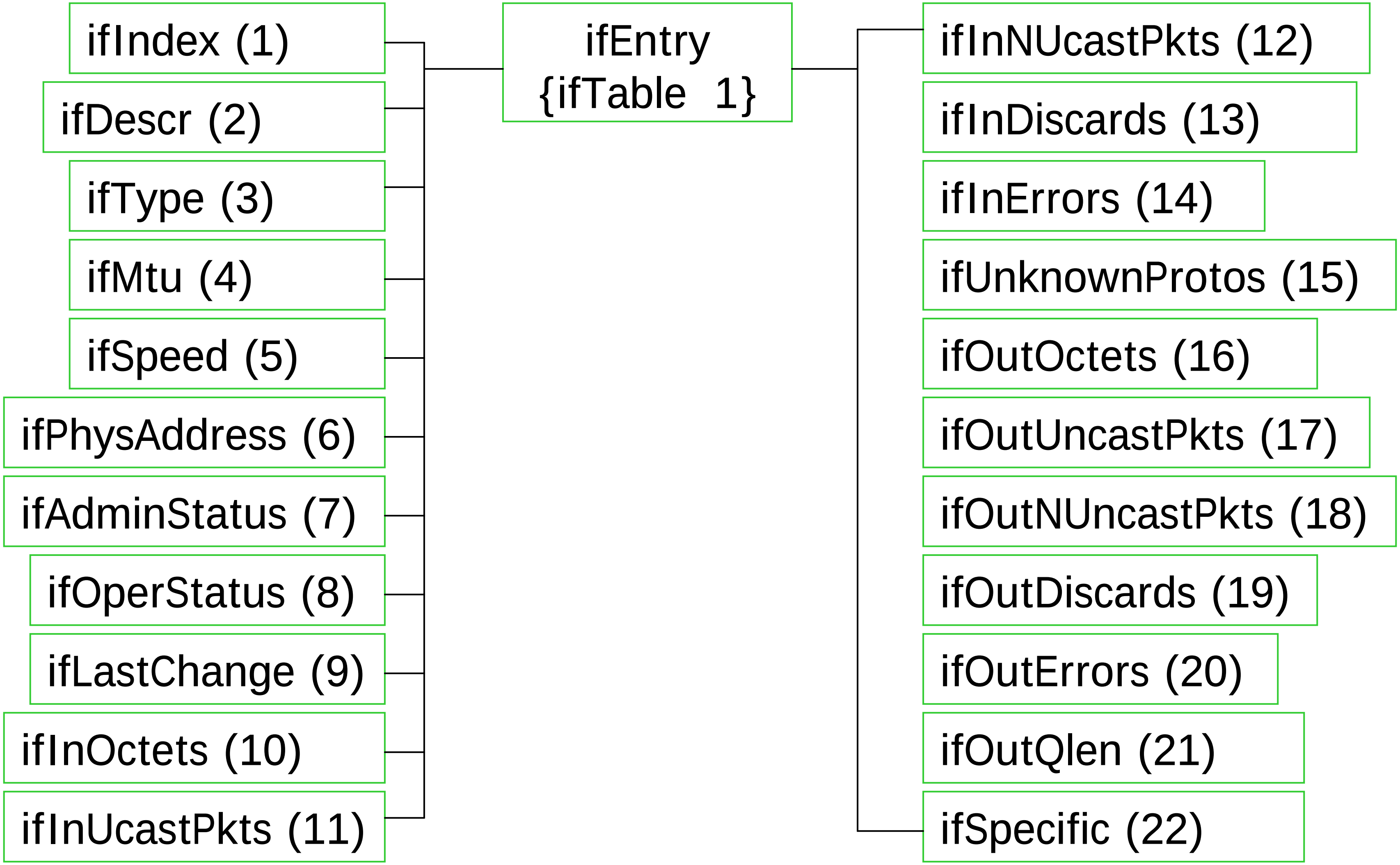
T.E.1.1	T.E.2.1	T.E.3.1	T.E.4.1	T.E.5.1
T.E.1.2	T.E.2.2	T.E.3.2	T.E.4.2	T.E.5.2
T.E.1.3	T.E.2.3	T.E.3.3	T.E.4.3	T.E.5.3

e.g.

- Write out the object identifier for the incoming octet counter of the third interface of a given switch

(refer to the ifEntry group in next slide)

- The {ifEntry} group



ifEntry {ifTable 1}

ifIndex (1)

ifDescr (2)

ifType (3)

ifMtu (4)

ifSpeed (5)

ifPhysAddress (6)

ifAdminStatus (7)

ifOperStatus (8)

ifLastChange (9)

ifInOctets (10)

ifInUcastPkts (11)

ifInNUcastPkts (12)

ifInDiscards (13)

ifInErrors (14)

ifUnknownProtos (15)

ifOutOctets (16)

ifOutUncastPkts (17)

ifOutNUncastPkts (18)

ifOutDiscards (19)

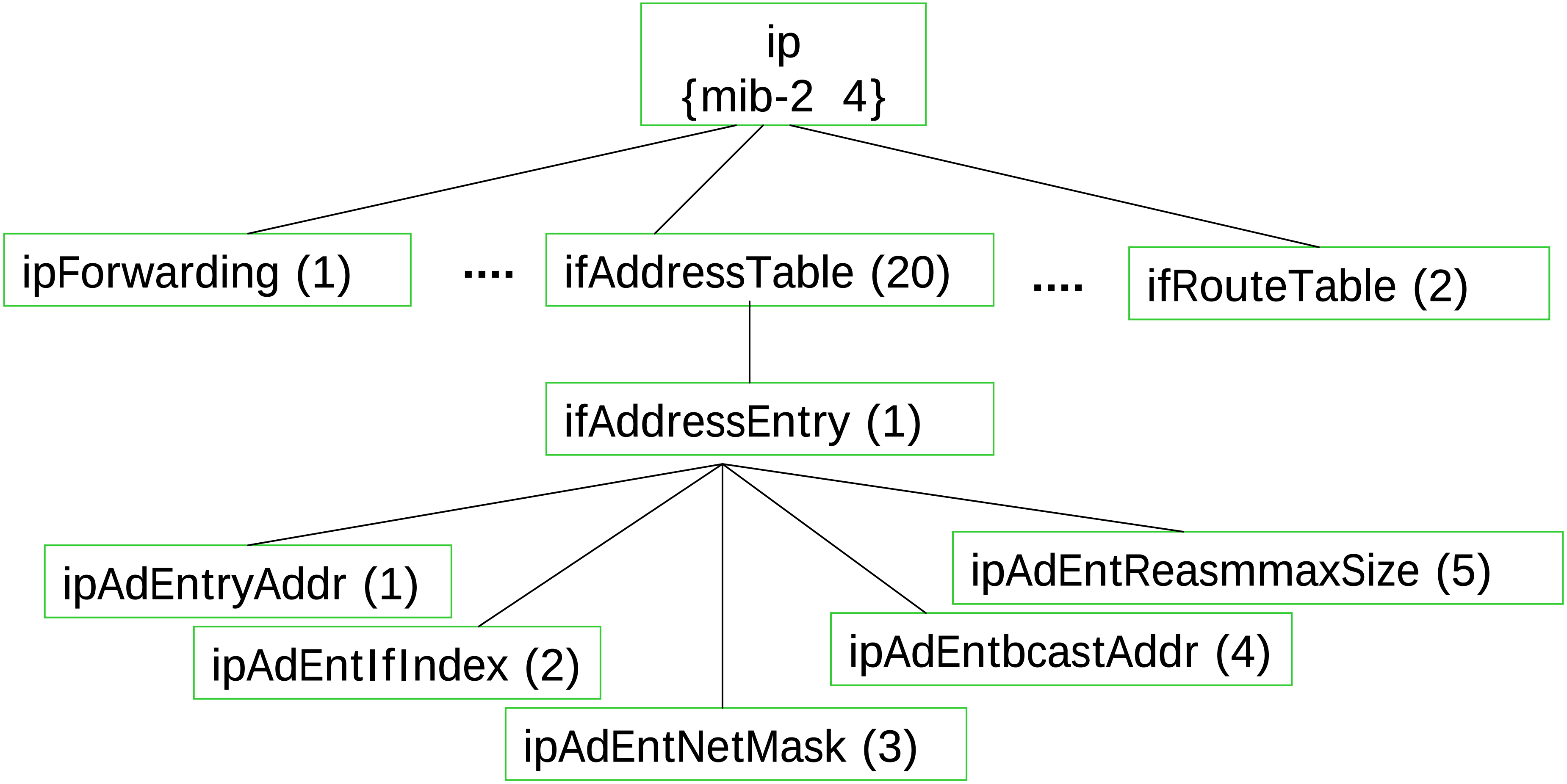
ifOutErrors (20)

ifOutQlen (21)

ifSpecific (22)

The ip group

To students: make an educated guess as to the semantics and syntax of the objects in the ip group shown here



The ip group - Exercise:

Given

- a router with three interface: ser0, eth0 and eth1
- It is used to route traffic between subnets 212.22.90.252, 10.2.21.0, 192.168.5.0
- IP address assignments:
  - ser0: 212.22.90.1
  - eth0: 10.2.21.1, 10.2.30.4
  - eth1: 192.168.5.10, 192.168.20.3

Show the probable ifAddressTable content for this router

Administrative Model

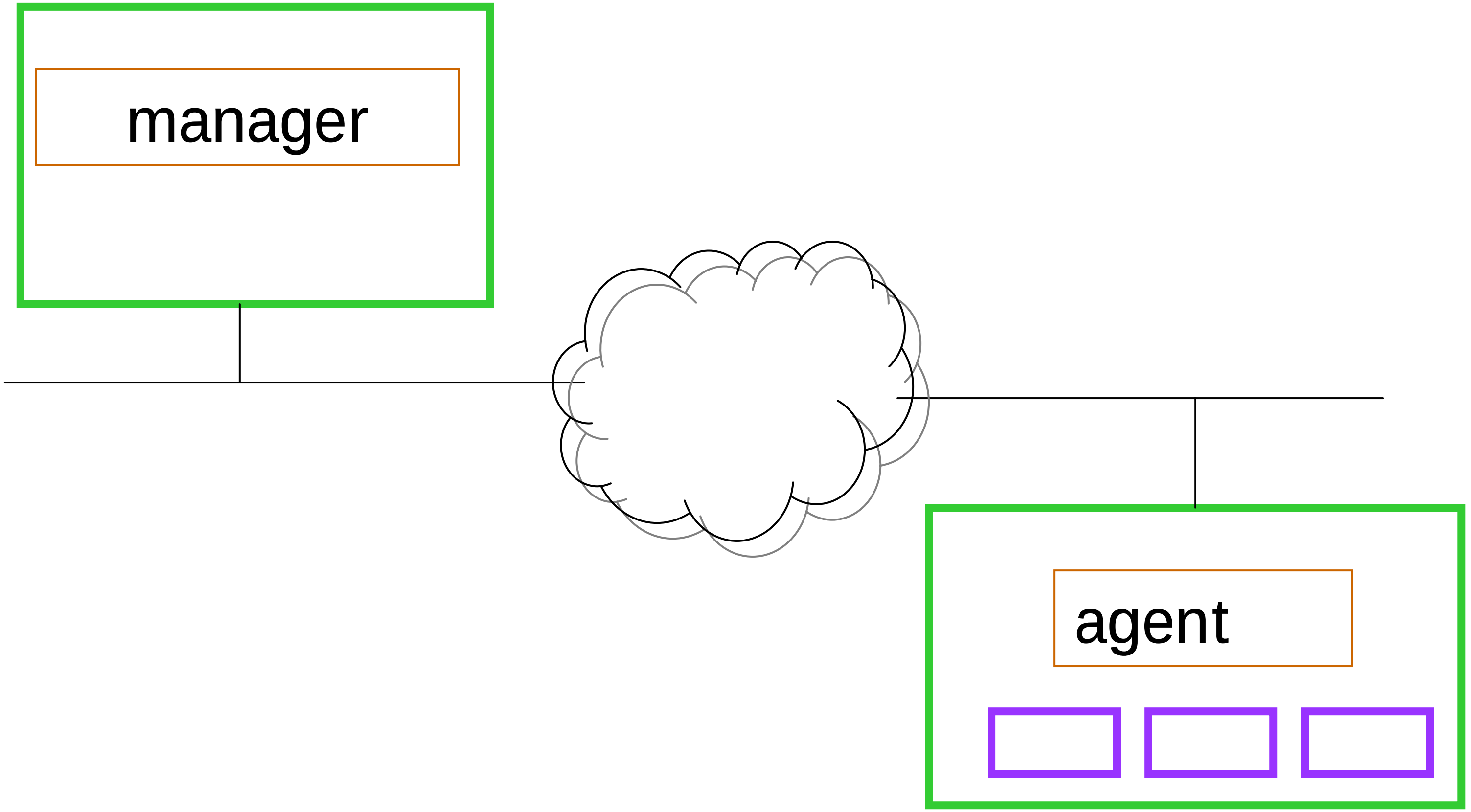
- Administrative Model :

SNMP access policy:

- Application entities
  - Manager
  - Agent

  - The pairing of two is an snmp community
  - Multiple pairs may belong to the same community

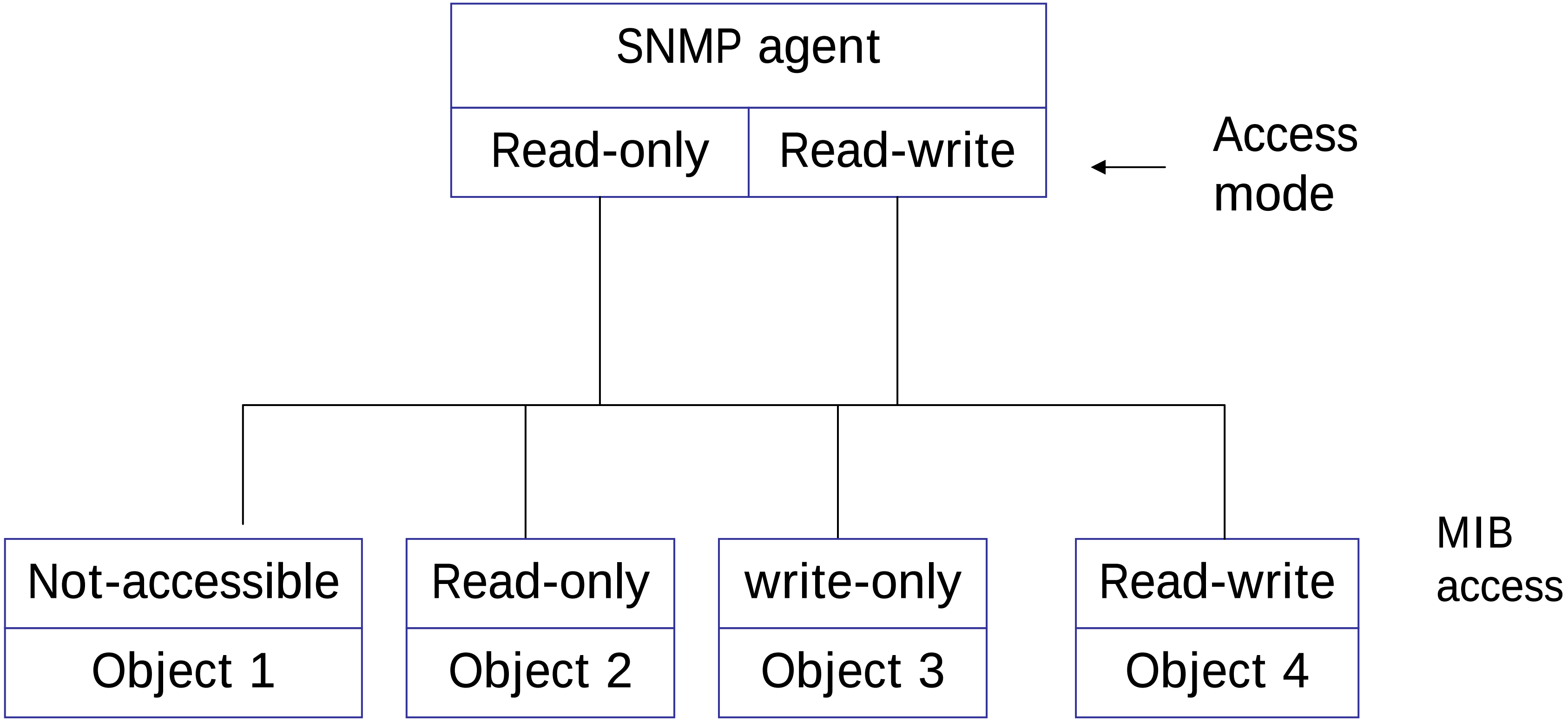
- Recall SNMP operation:



- Protocol messages - Five in number
- Manager initiated
  - Get-request:
  - Get-next-request:
  - Set-request:
- Agent initiated
  - Get-response:
  - Trap:

Administrative Model : Community Profile

- A network element: managed object
- A management agent may be permitted to view only a subset of the network element’s managed objects, i.e.
  - → the community MIB view
- Each community name is also assigned an snmp
  - → access mode: READ-ONLY or READ-WRITE
- A pairing of snmp MIB view and snmp access mode is a
  - → community profile



SNMP agent

Read-only

Read-write

Access mode

Not-accessible

Object 1

Read-only

Object 2

write-only

Object 3

Read-write

Object 4

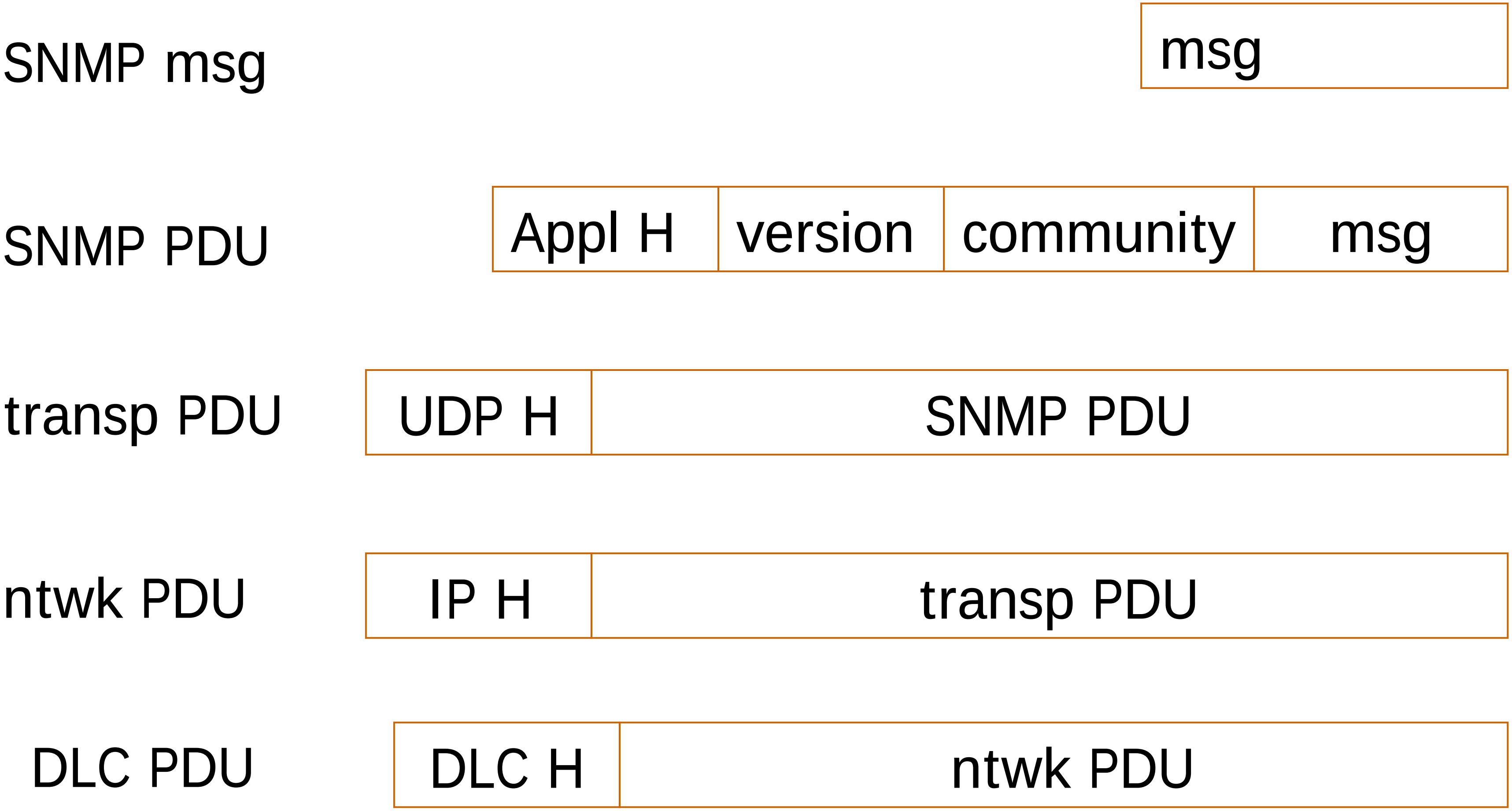
MIB access

SNMP operation: Encapsulation

- Protocol messages - Five in number

- Manager initiated
  - Get-request:
  - Get-next-request:
  - Set-request:
- Agent initiated
  - Get-response:
  - Trap:

snmp Protocol PDU encapsulation (port 12)



SNMP msg: msg

SNMP PDU: Appl H | version | community | msg

transp PDU: UDP H | SNMP PDU

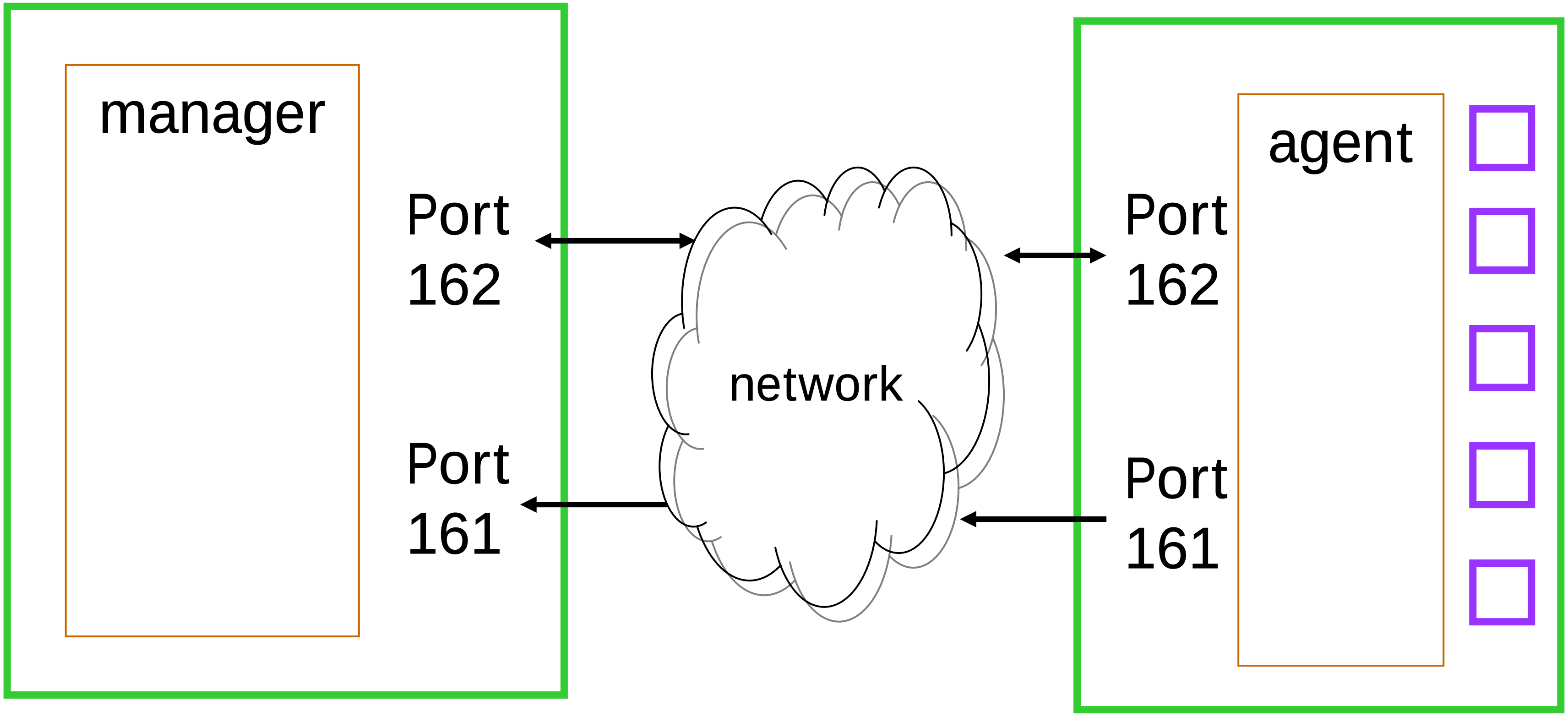
ntwk PDU: IP H | transp PDU

DLC PDU: DLC H | ntwk PDU

snmp Protocol UDP ports

- For most messages, SNMP by default receives on UDP port 161
- Trap messages are received on port 162
- SNMPv1 max msg length is 484 bytes

snmp Protocol UDP ports



- SNMP operation:

Get and Set Type PDUs

PDU type	requestID	Error status	Error index	VarBind 1 name	VarBind 1 value	…	VarBind n name	VarBind n value

Trap PDUs

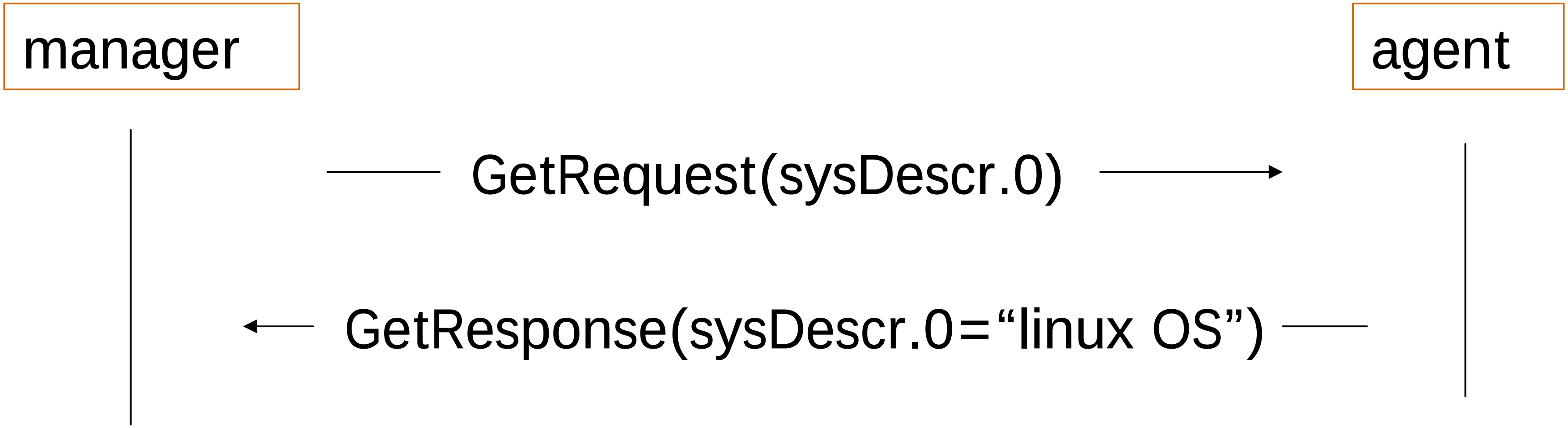
PDU type	enterprise	Agent address	Generic trap type	specific trap type	timestamp

VarBind 1 name	VarBind 1 value	…	VarBind n name	VarBind n value

get-request operation

E.g

- get the system’s description
- Get systems location



manager

agent

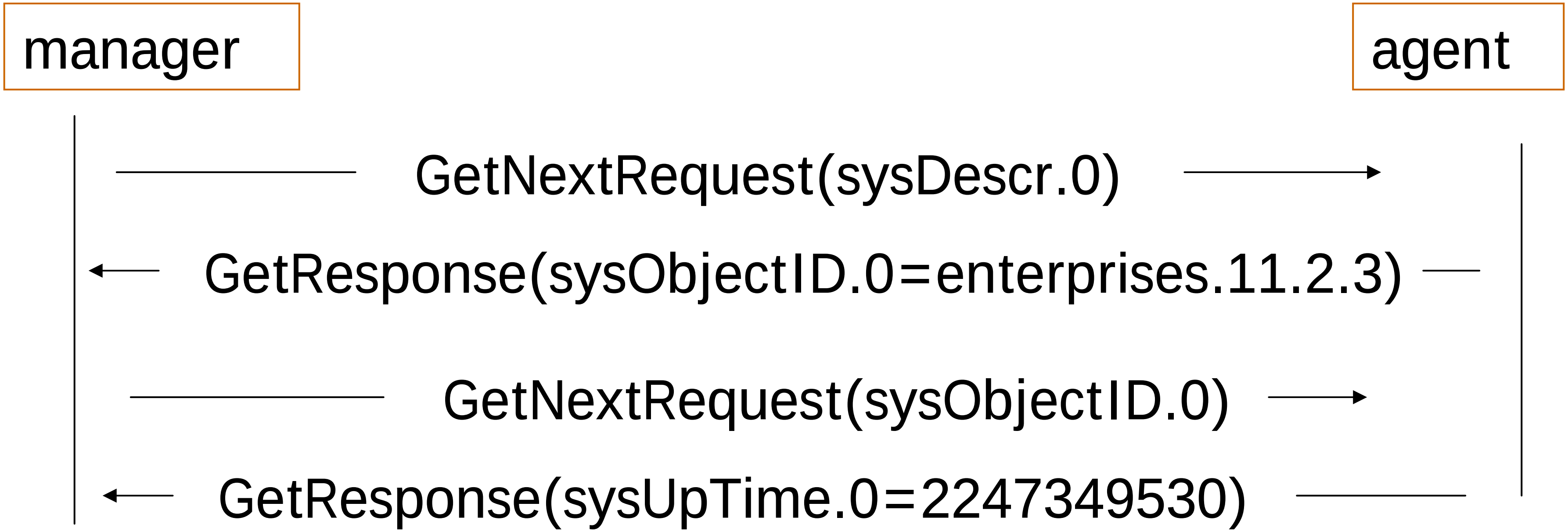
GetRequest(sysDescr.0)

GetResponse(sysDescr.0=“linux OS”)

- get-next-request operation

  E.g

  - get the element following system's description



manager

agent

GetNextRequest(sysDescr.0)

GetResponse(sysObjectID.0=enterprises.11.2.3)

GetNextRequest(sysObjectID.0)

GetResponse(sysUpTime.0=2247349530)

- SNMP operation:

- Getting the elements of a structured object
- Generally column order

- E.g
  - interface information

  - IP information

- SNMP operation:

- Getting the elements of a structured object
- With get bulk ver 2

Get bulk pdu

PDU type	requestID	Non rep	Max rep	VarBind 1 name	VarBind 1 value	...	VarBind n name	VarBind n value

- SNMP operation:

- set-request operation
- E.g
  - set systems location

SNMP on servers and workstations

- Standard operating system platforms provide implementations of SNMP agent
- Enables monitoring and configuration from a remote location (NMS)
- Can provide/manage information on hardware and software; configuration and statistical information

➢ We can, for example, request system and interfaces MIBs from a Windows XP and linux systems.

Exercise (to be accomplished on Wednesday afternoon)

- 1. Write a sequence of snmp commands to retrieve information from your switch, e.g.
  - Location
  - Contact information
  - Number of interfaces
  - IP address(es)
  - Number of incoming bytes that have been seen at interface 1 of the switch
- 2. Explain how, using an snmp based application at a remote workstation, one can determine the type of switch whose IP address is given.

Exercise (should be accomplished on Wednesday afternoon)

- 3. Read about the snmp based software tool known as net-snmp. Write brief descriptive notes on the tool.
- 4. Install net-snmp and use it to execute exercises 1 and two above on the switch available to you.

Net-SNMP

The net-snmp toolkit provides a suite of command line applications that can be used to query and act on remote SNMP agents. **Sections:**

- snmptranslate: learning about the MIB tree.
- snmpget: retrieving data from a host.
- snmpgetnext: retrieving unknown indexed data.
- snmpwalk: retrieving lots of data at once!
- snmptable: displaying table.
- snmpset: peforming write operations.
- snmptrap: Sending and receiving traps, and acting upon them.

PRTG Network Monitoring Software