What is network management?

- autonomous systems (aka "network"): 100s or 1000s of interacting hardware/software components
- other complex systems requiring monitoring, control:
  - jet airplane
  - nuclear power plant
  - others?

"Network management includes the deployment, integration and coordination of the hardware, software, and human elements to monitor, test, poll, configure, analyze, evaluate, and control the network and element resources to meet the real-time, operational performance, and Quality of Service requirements at a reasonable cost."

21.1 CONCEPT

SNMP defines a manager, usually a host, that controls and monitors a set of agents, usually routers.

The topics discussed in this section include:

Managers and Agents

Figure 21.1 *SNMP concept*

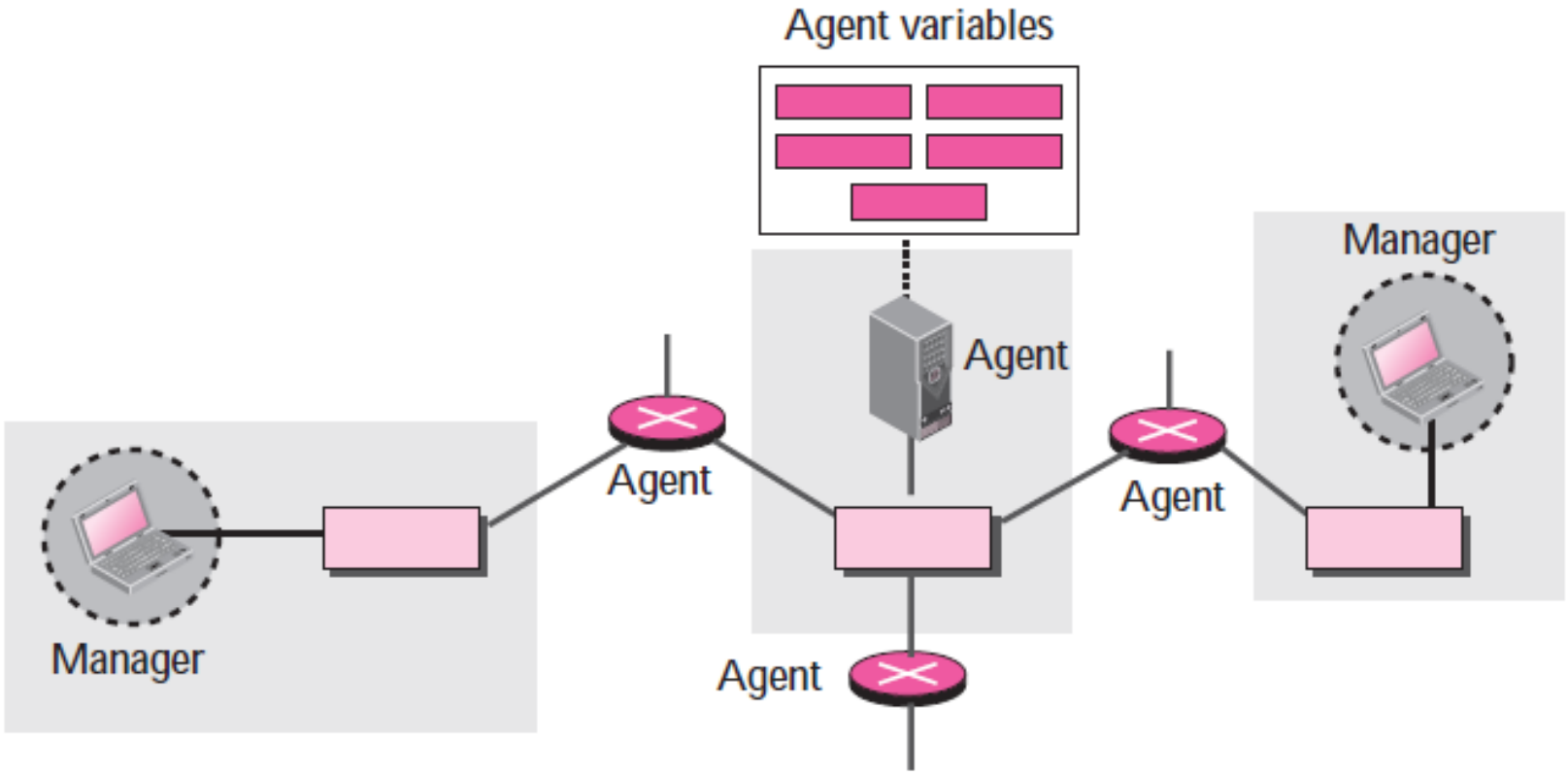
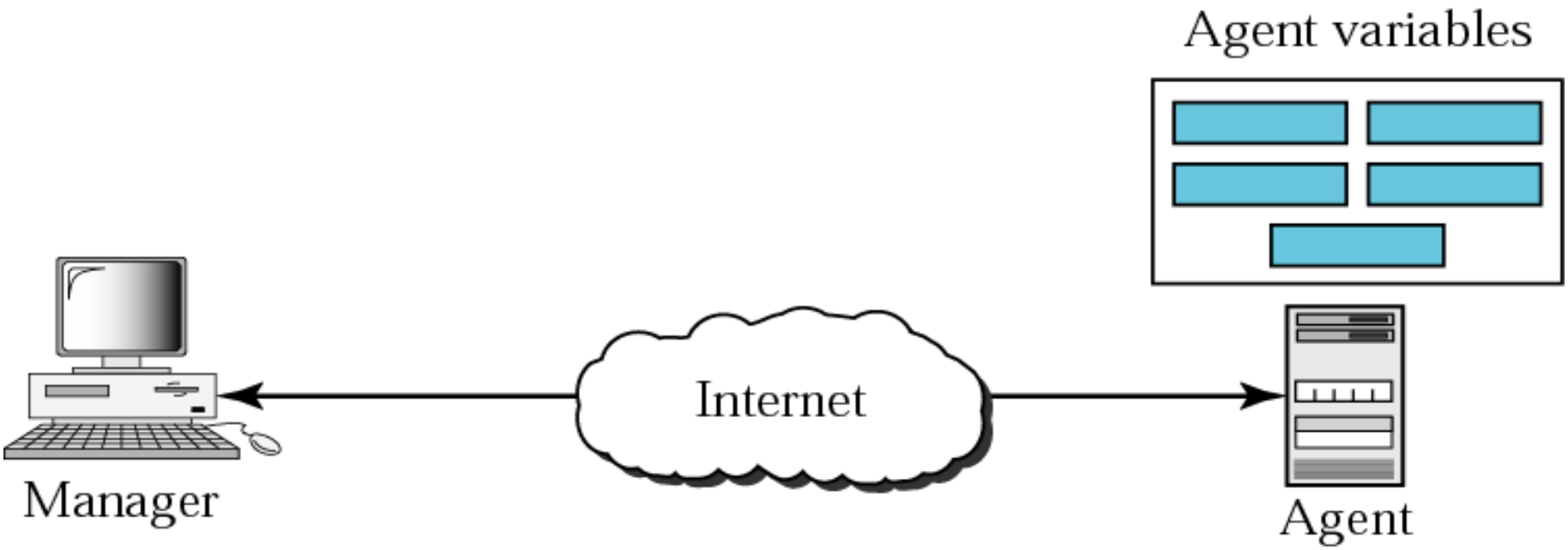
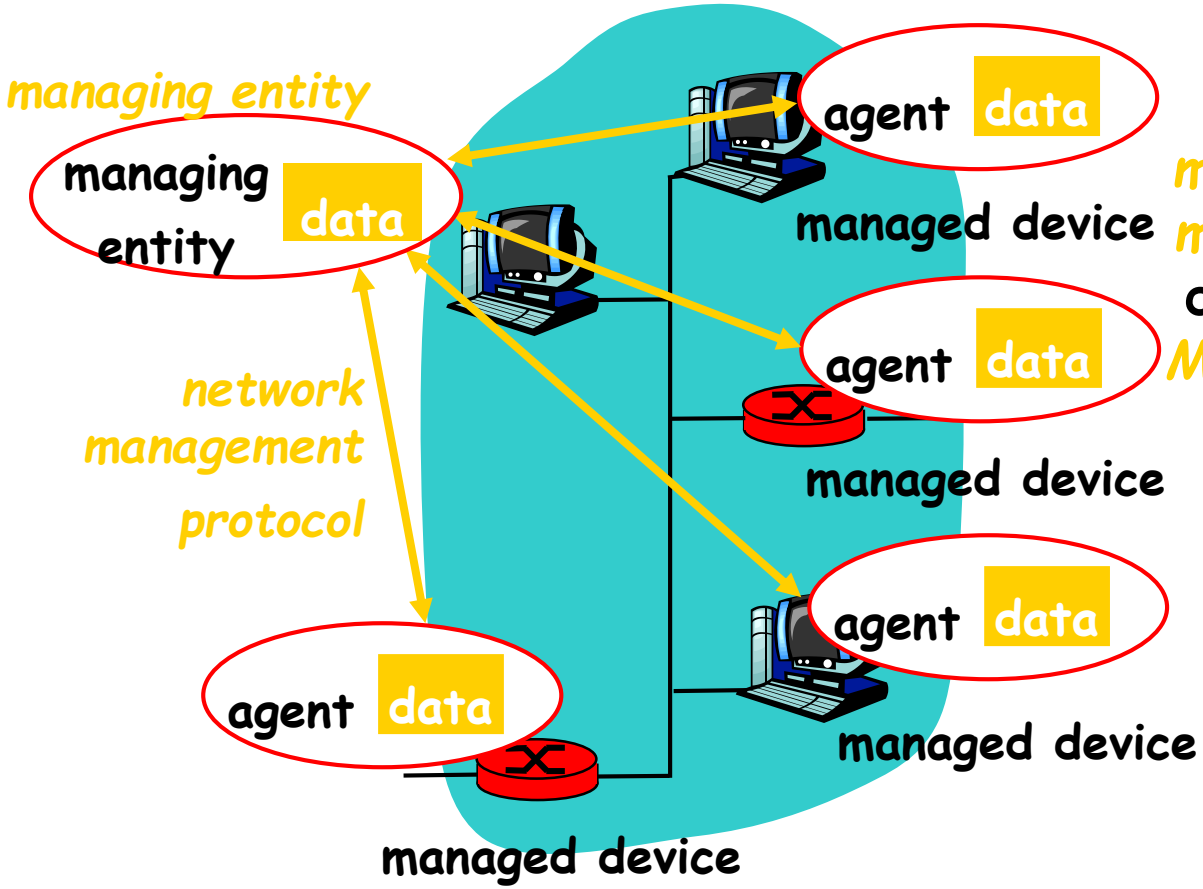


Figure 21.1 *SNMP concept*



Infrastructure for network management

definitions:



managed devices contain *managed objects* whose data is gathered into a *Management Information Base (MIB)*

Network Management standards

OSI CMIP

- Common Management Information Protocol
- designed 1980's: *the* unifying net management standard
- too slowly standardized

SNMP: Simple Network Management Protocol

- Internet roots (SGMP)
- started simple
- deployed, adopted rapidly
- growth: size, complexity
- currently: SNMP V3
- *de facto* network management standard

1. A manager **checks an agent by requesting information** that reflects the behavior of the agent.
2. A manager **forces an agent to perform a task** by resetting values in the agent database.
3. An agent **contributes to the management process** by warning the manager of an unusual situation.

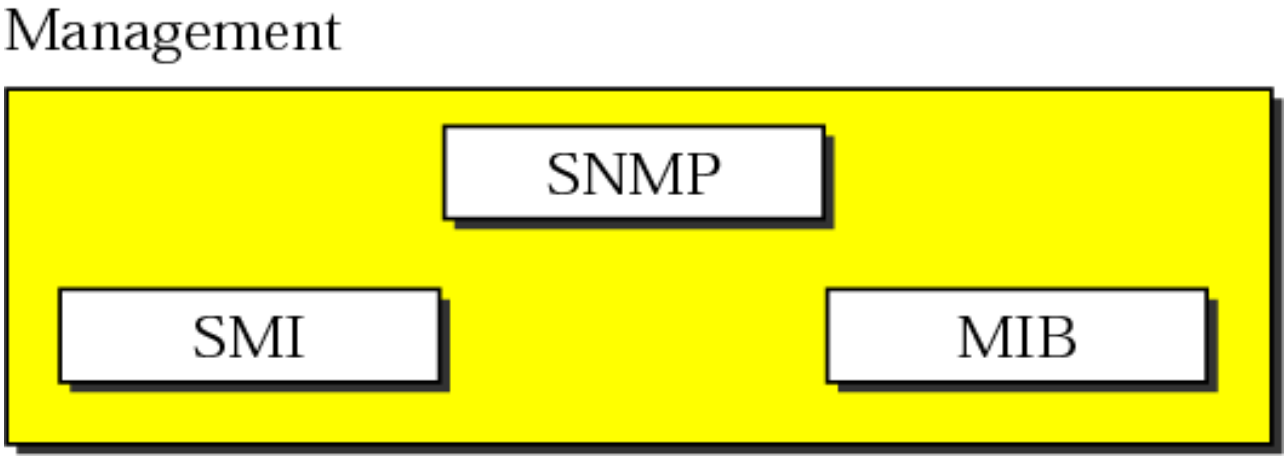
21.2 MANAGEMENT COMPONENTS

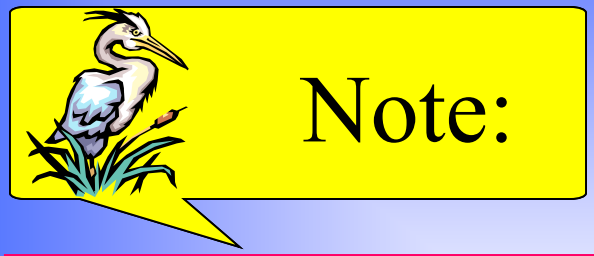
SNMP requires the use of two other protocols: Structure of Management Information (SMI) and Management Information Base (MIB). Network management on the Internet is done through the cooperation of SNMP, SMI, and MIB.

The topics discussed in this section include:

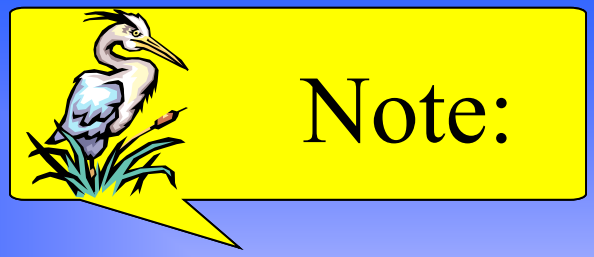
Role of SNMP
Role of SMI
Role of MIB
An Analogy
An Overview

Figure 21.2 *Components of network management on the Internet*



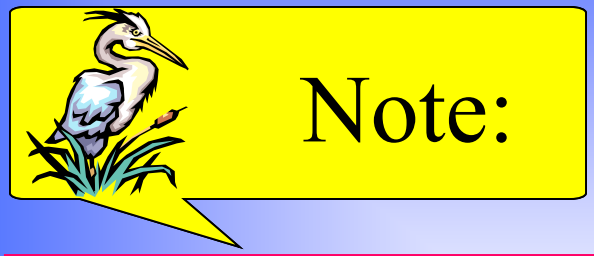


SNMP defines the format of packets exchanged between a manager and an agent. It reads and changes the status (values) of objects (variables) in SNMP packets.



Note:

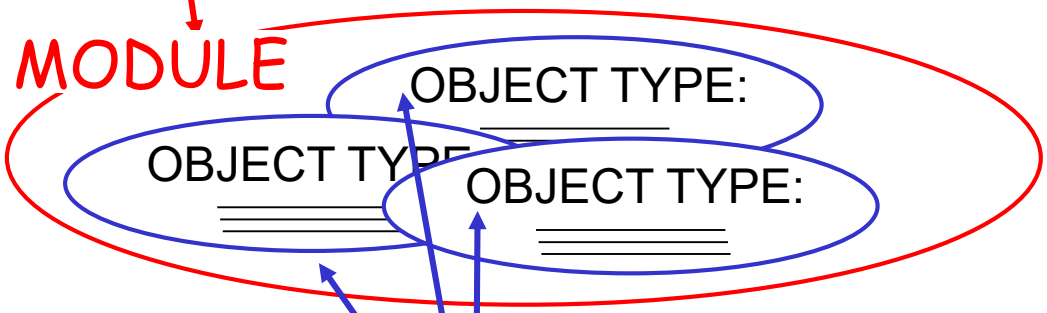
SMI defines the general rules for naming objects, defining object types (including range and length), and showing how to encode objects and values. SMI defines neither the number of objects an entity should manage, nor names the objects to be managed nor defines the association between the objects and their values.



MIB creates a collection of named objects, their types, and their relationships to each other in an entity to be managed.

SNMP MIB

MIB module specified via SMI
MODULE-IDENTITY
(100 standardized MIBs, more vendor-specific)



objects specified via SMI
OBJECT-TYPE construct

Note:

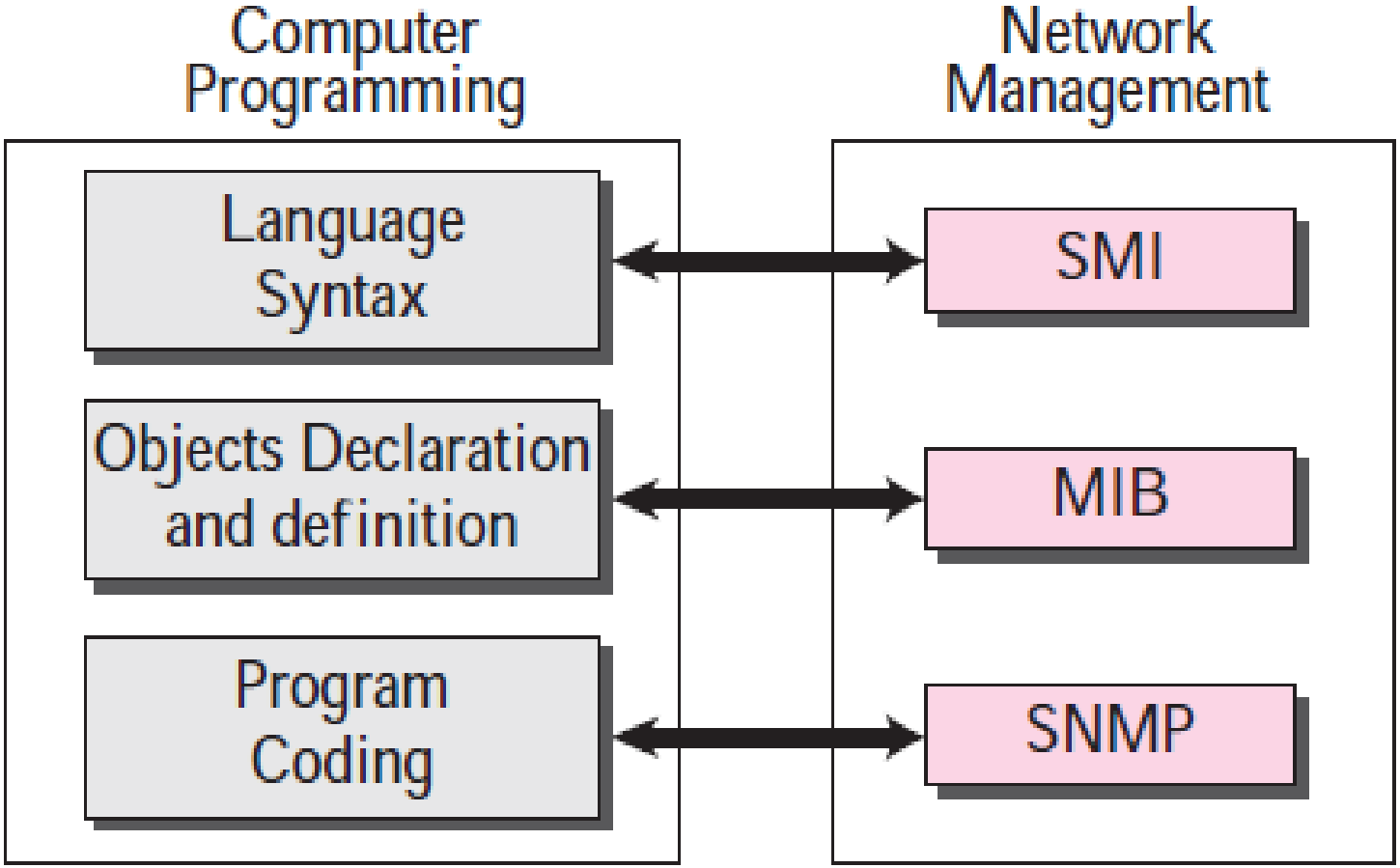
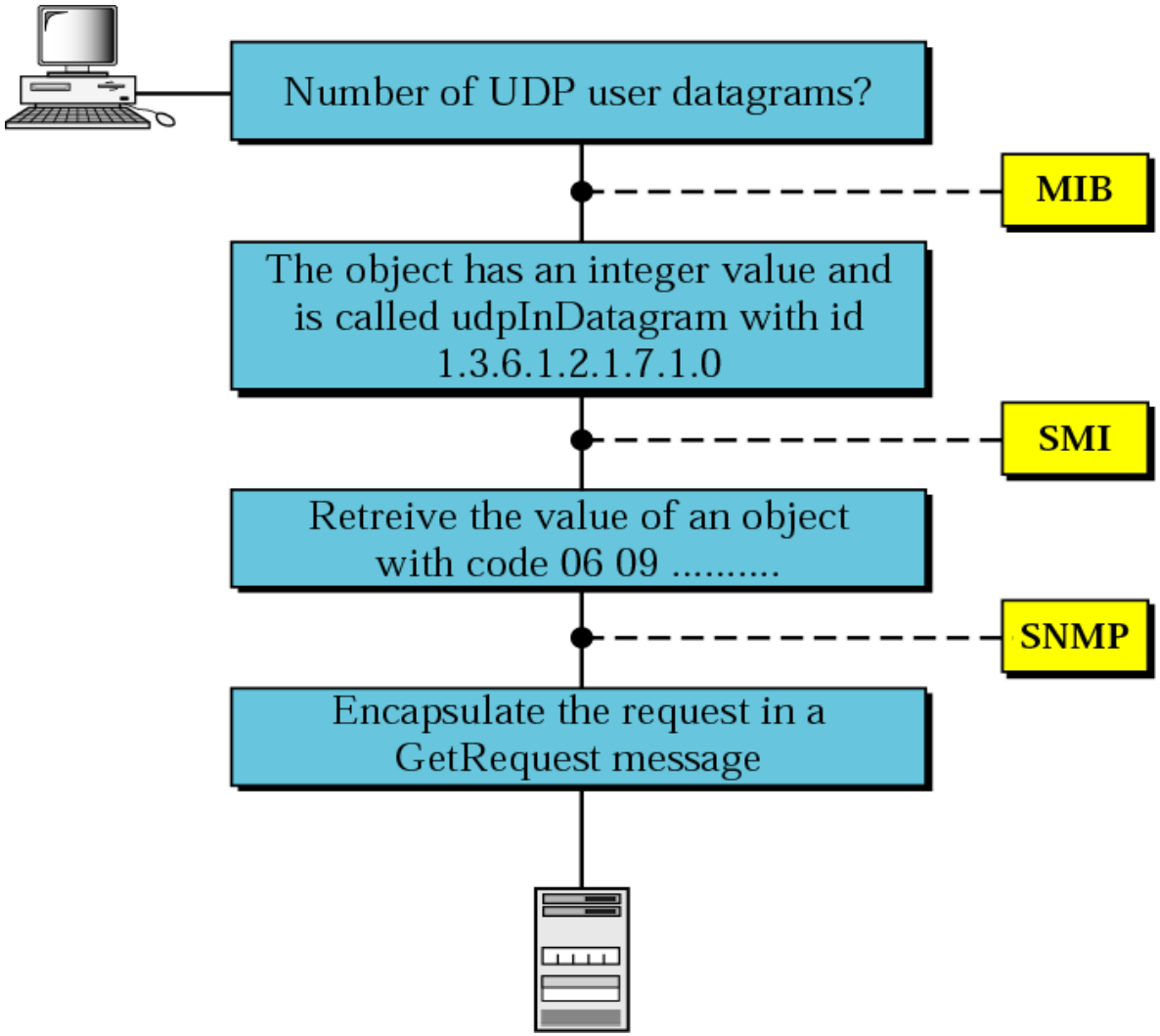

Computer Programming
Network Management
Language Syntax
Objects Declaration and definition
Program Coding
SMI
MIB
SNMP

Figure 21.3 *Management overview*



21.3 SMI

SMI is a component used in network management. It names objects, defines the type of data that can be stored in an object, and shows how data can be encoded for transmission over the network

The topics discussed in this section include:

Name
Type
Encoding Method

Figure 21.4 *Object attributes*

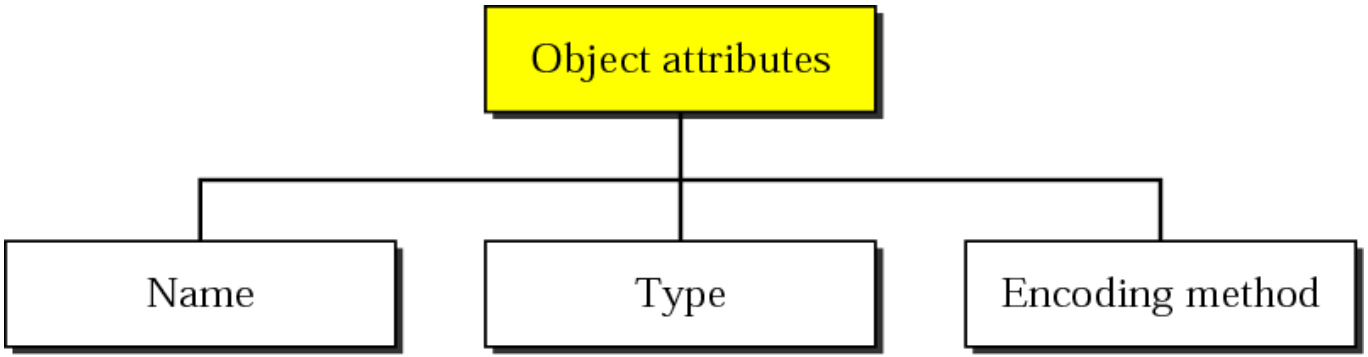
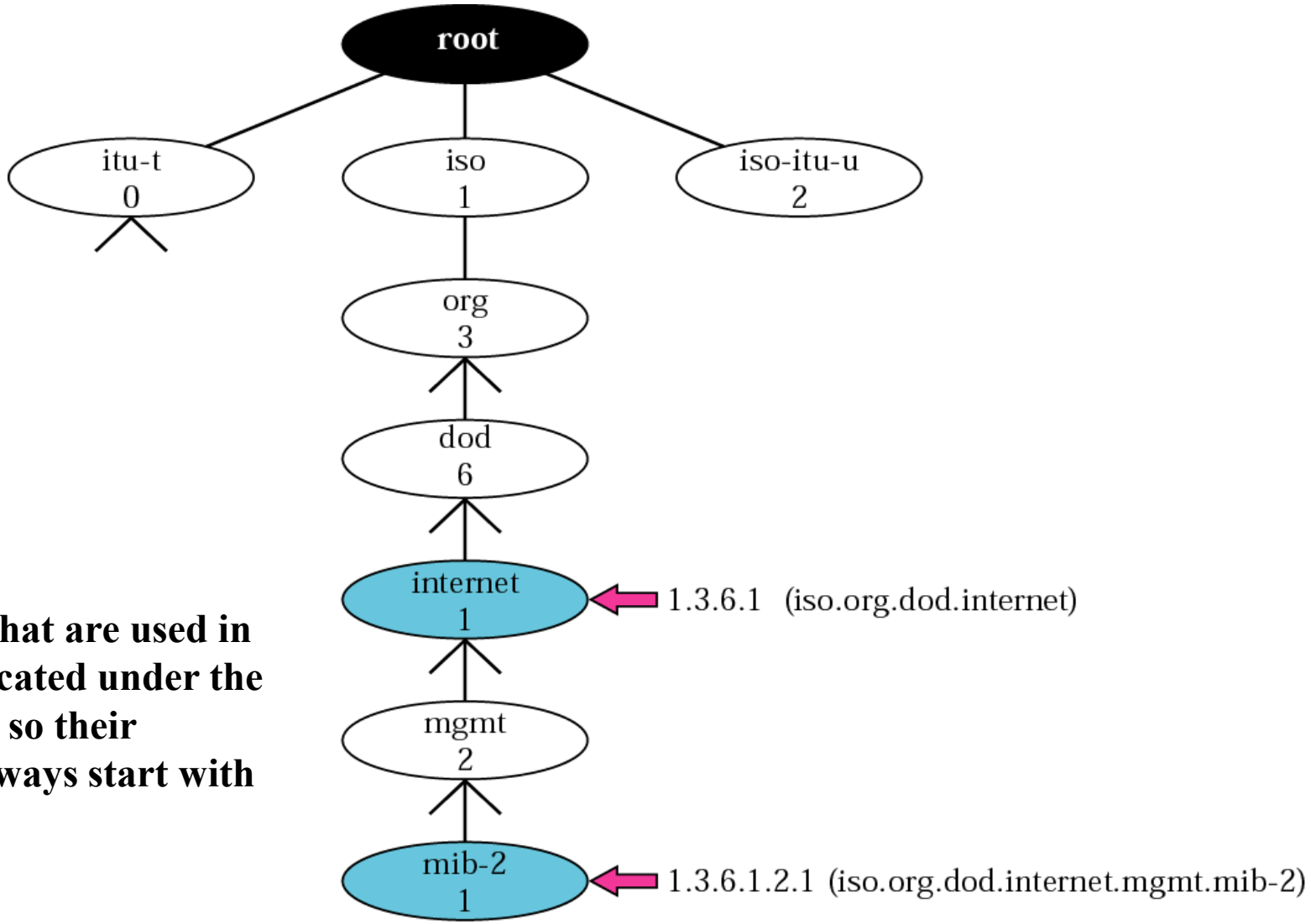
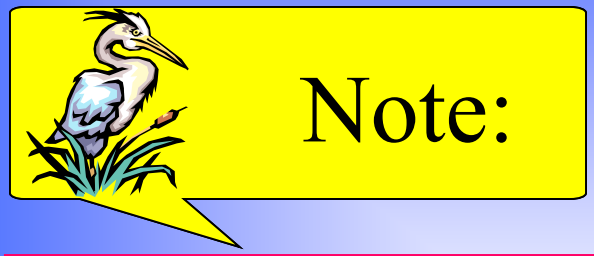


Figure 21.5 *Object identifier*



The objects that are used in SNMP are located under the *mib-2* object, so their identifiers always start with 1.3.6.1.2.1



All objects managed by SNMP are given an object identifier.

The object identifier always starts with 1.3.6.1.2.1.

Figure 21.6 *Data type*

To define the data type, SMI uses fundamental **Abstract Syntax Notation 1 (ASN.1)** definitions and adds some new definitions.

In other words, SMI is both a subset and a superset of ASN.1.

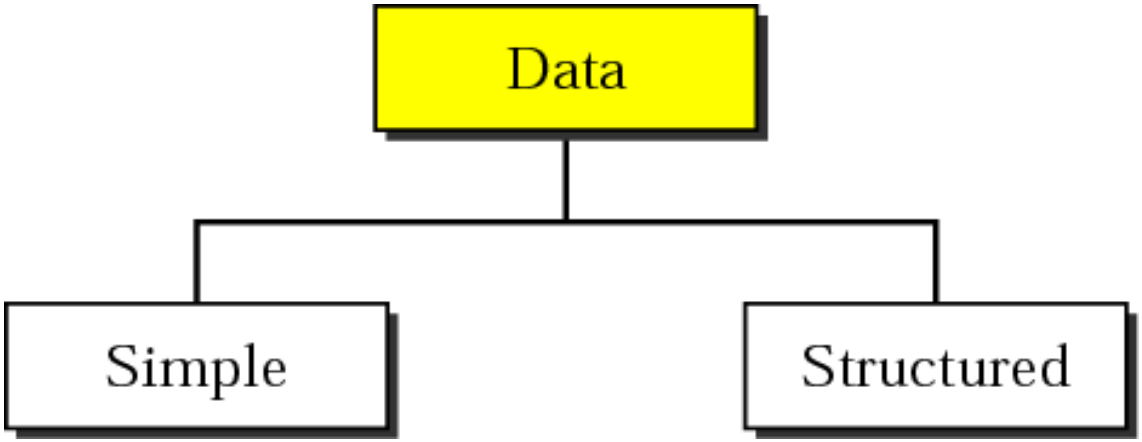


Table 21.1 Data types (The first five are from ASN.1; the next seven are defined by SMI.)

Type	*Size*	*Description*
INTEGER	4 bytes	An integer with a value between -2^{31} and $2^{31}-1$
Integer32	4 bytes	Same as INTEGER
Unsigned32	4 bytes	Unsigned with a value between 0 and $2^{32}-1$
OCTET STRING	Variable	Byte-string up to 65,535 bytes long
OBJECT IDENTIFIER	Variable	An object identifier
IPAddress	4 bytes	An IP address made of four integers
Counter32	4 bytes	An integer whose value can be incremented from zero to 2^{32}; when it reaches its maximum value it wraps back to zero
Counter64	8 bytes	64-bit counter
Gauge32	4 bytes	Same as Counter32, but when it reaches its maximum value, it does not wrap; it remains there until it is reset
TimeTicks	4 bytes	A counting value that records time in 1/100ths of a second
BITS		A string of bits
Opaque	Variable	Uninterpreted string

Figure 21.7 *Conceptual data types*

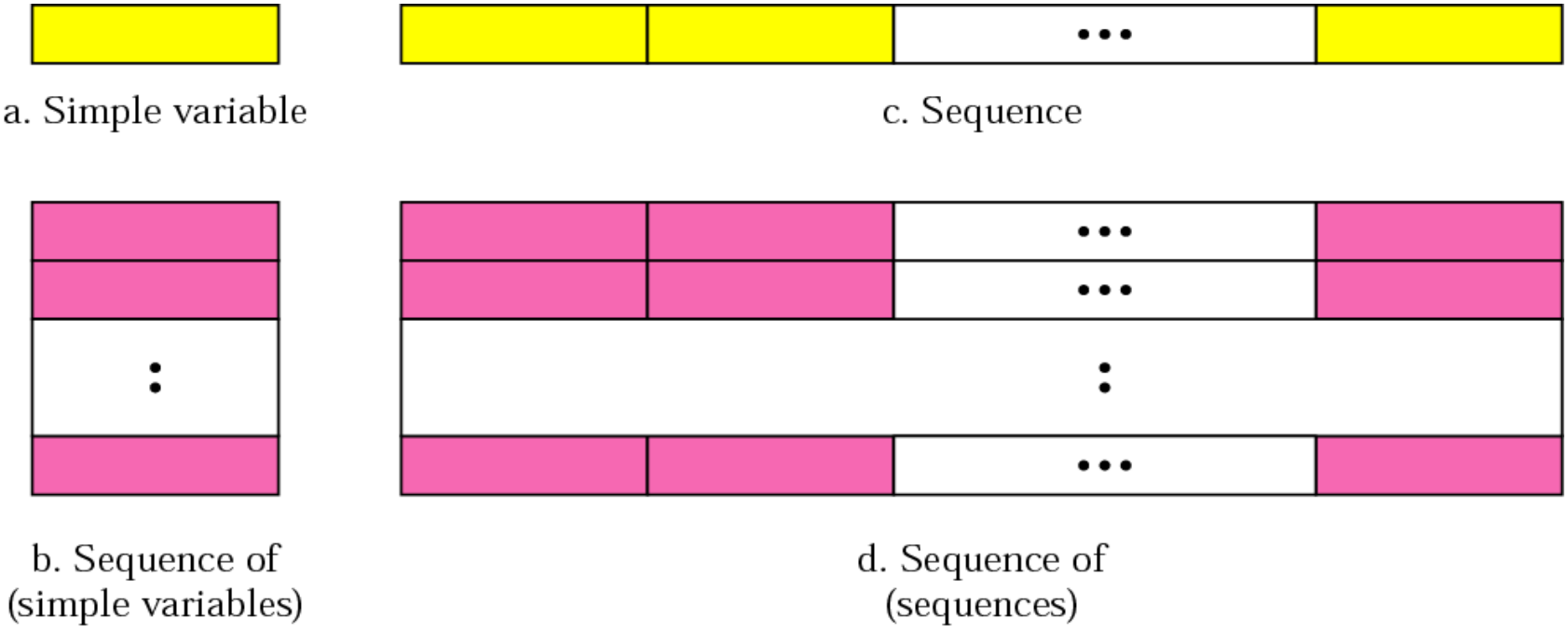
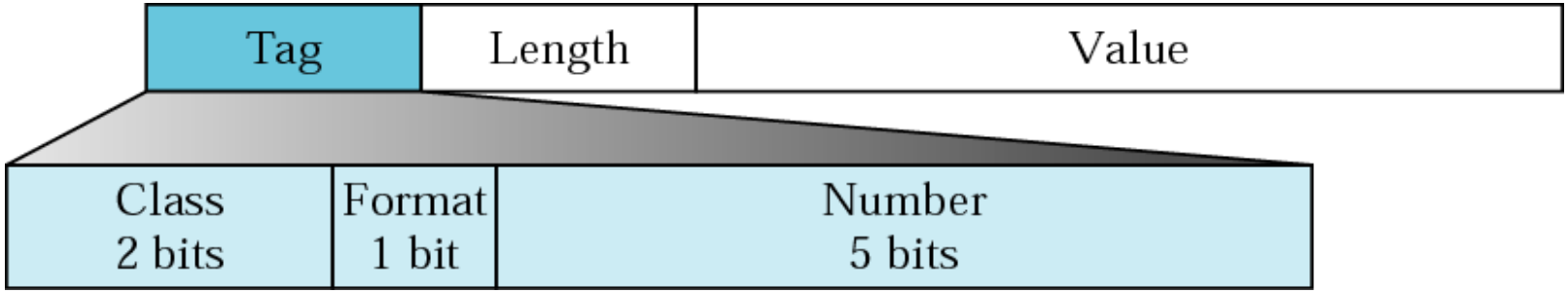


Figure 21.8 *Encoding format*



21.4 MIB

MIB is a component used in network management. Each agent has its own MIB, a collection of all the objects that the manager can manage.

The objects in MIB2 are categorized under 10 different groups:
system,
interface,
address translation,
ip,
icmp,
tcp,
udp,
egp,
transmission,
snmp.

Note:-These groups are under the mib-2 object in the object identifier tree

Figure 21.14 *mib-2*

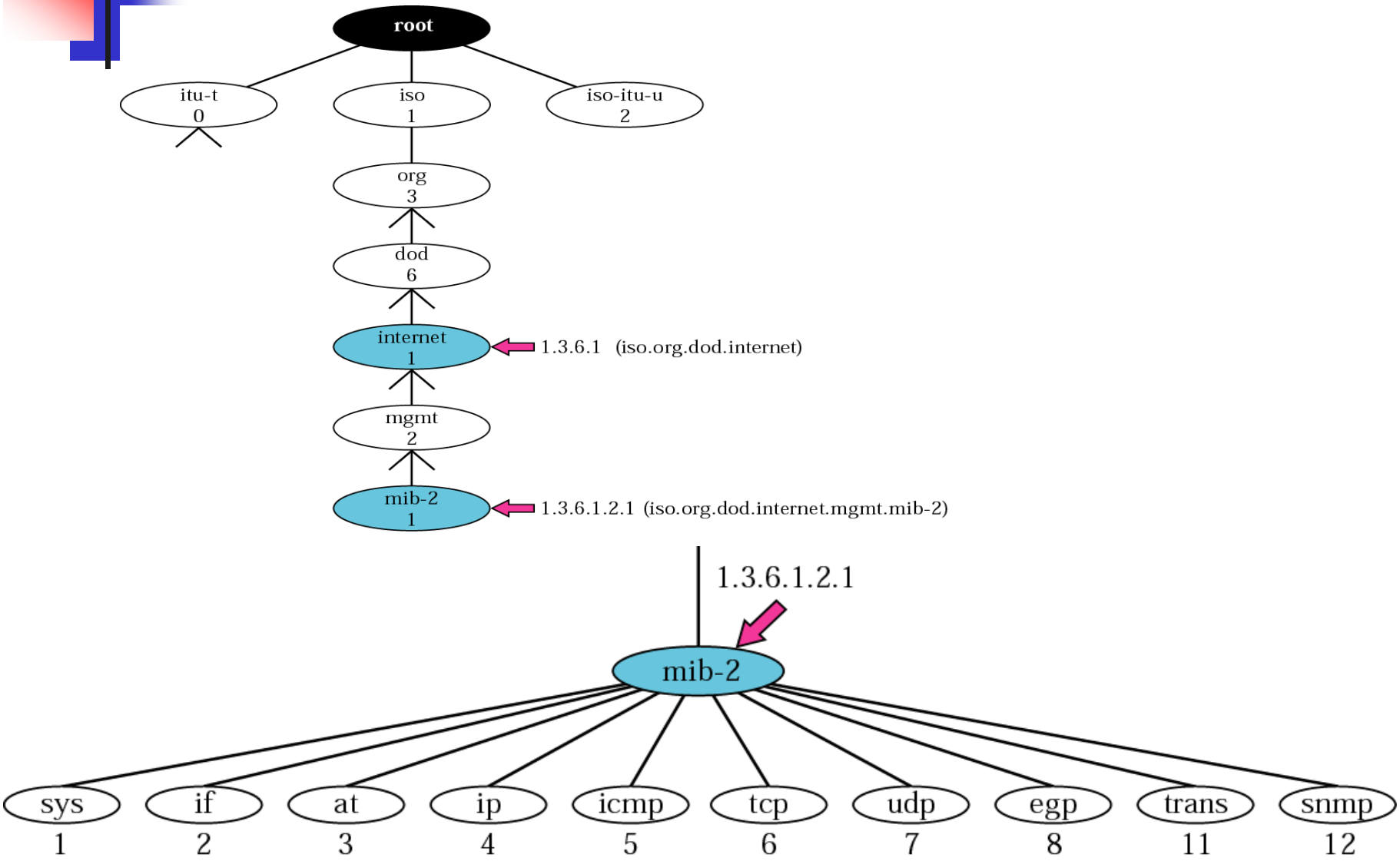


Figure 21.14 *mib-2*

sys This object (*system*) defines general information about the node (system), such as the name, location, and lifetime.

if This object (*interface*) defines information about all of the interfaces of the node including interface number, physical address, and IP address.

at This object (*address translation*) defines the information about the ARP table.

ip This object defines information related to IP, such as the routing table and the IP address.

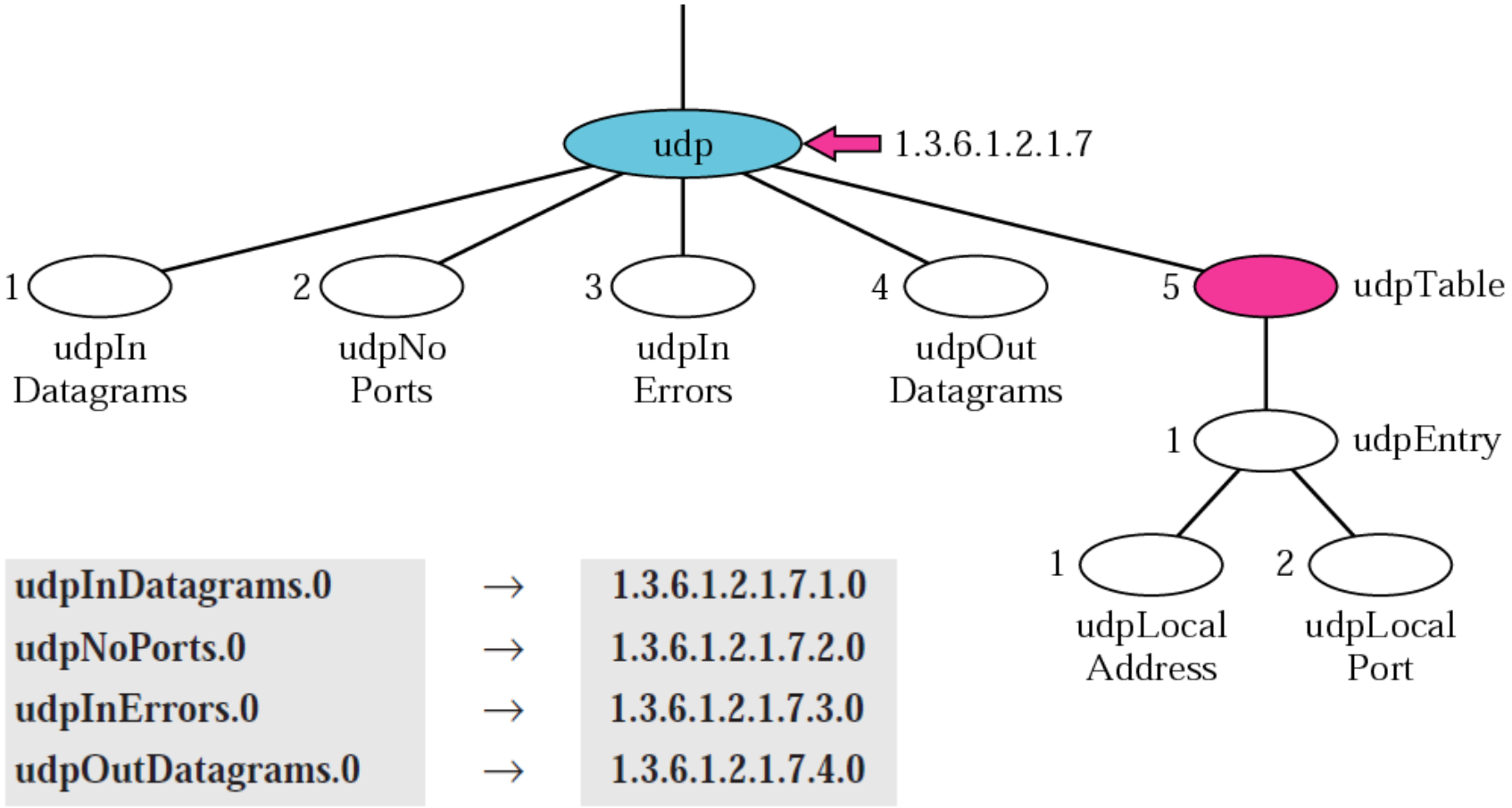
icmp This object defines information related to ICMP, such as the number of packets sent and received and total errors created.

tcp This object defines general information related to TCP, such as the connection table, time-out value, number of ports, and number of packets sent and received.

udp This object defines general information related to UDP, such as the number of ports and number of packets sent and received.

snmp This object defines general information related to SNMP itself.

Figure 21.15 Accessing MIB Variables use *udp group*



udpInDatagrams.0	→	1.3.6.1.2.1.7.1.0
udpNoPorts.0	→	1.3.6.1.2.1.7.2.0
udpInErrors.0	→	1.3.6.1.2.1.7.3.0
udpOutDatagrams.0	→	1.3.6.1.2.1.7.4.0

Figure 21.16 *udp variables and tables*

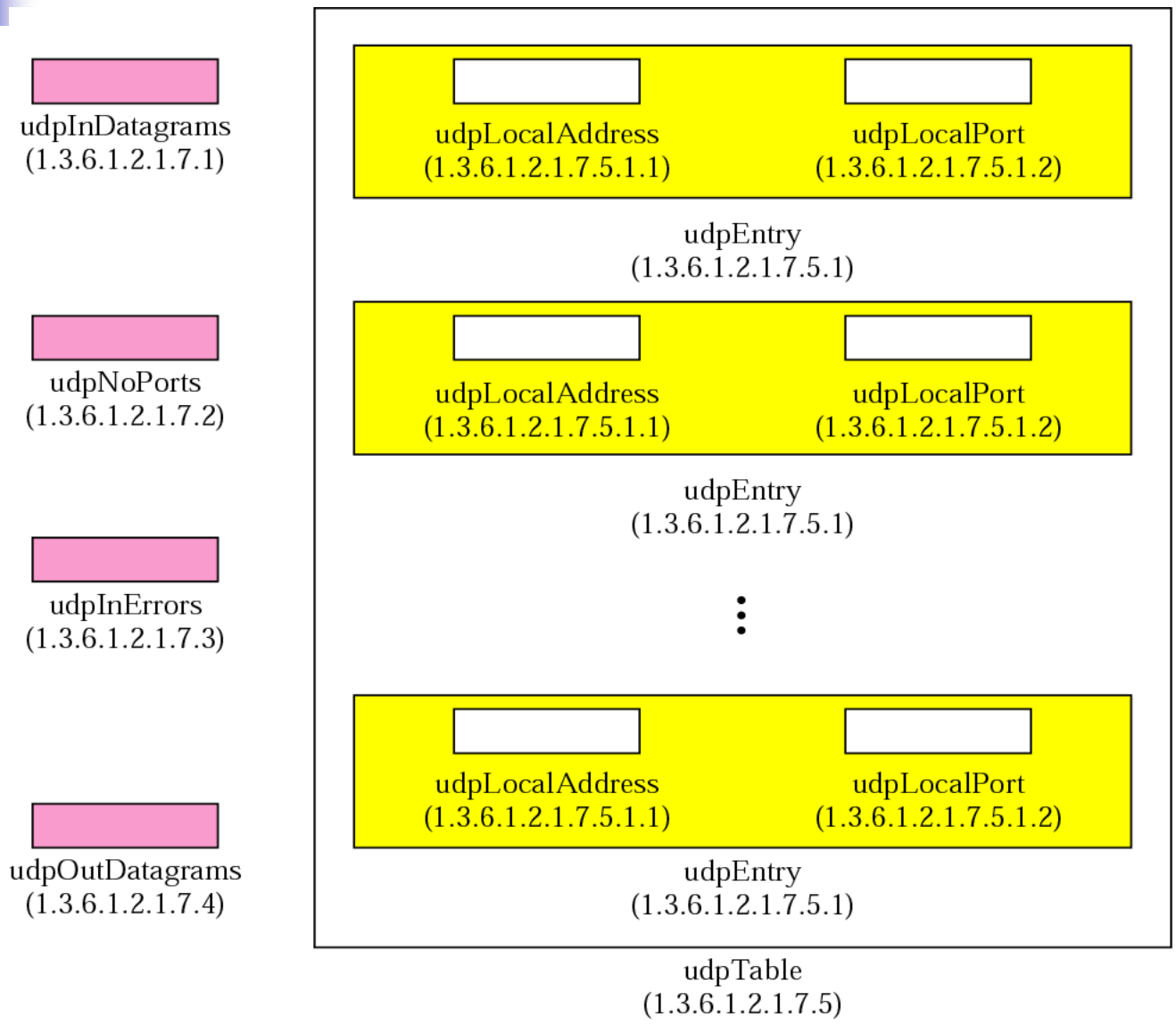


Figure 21.17 *Indexes for udpTable*

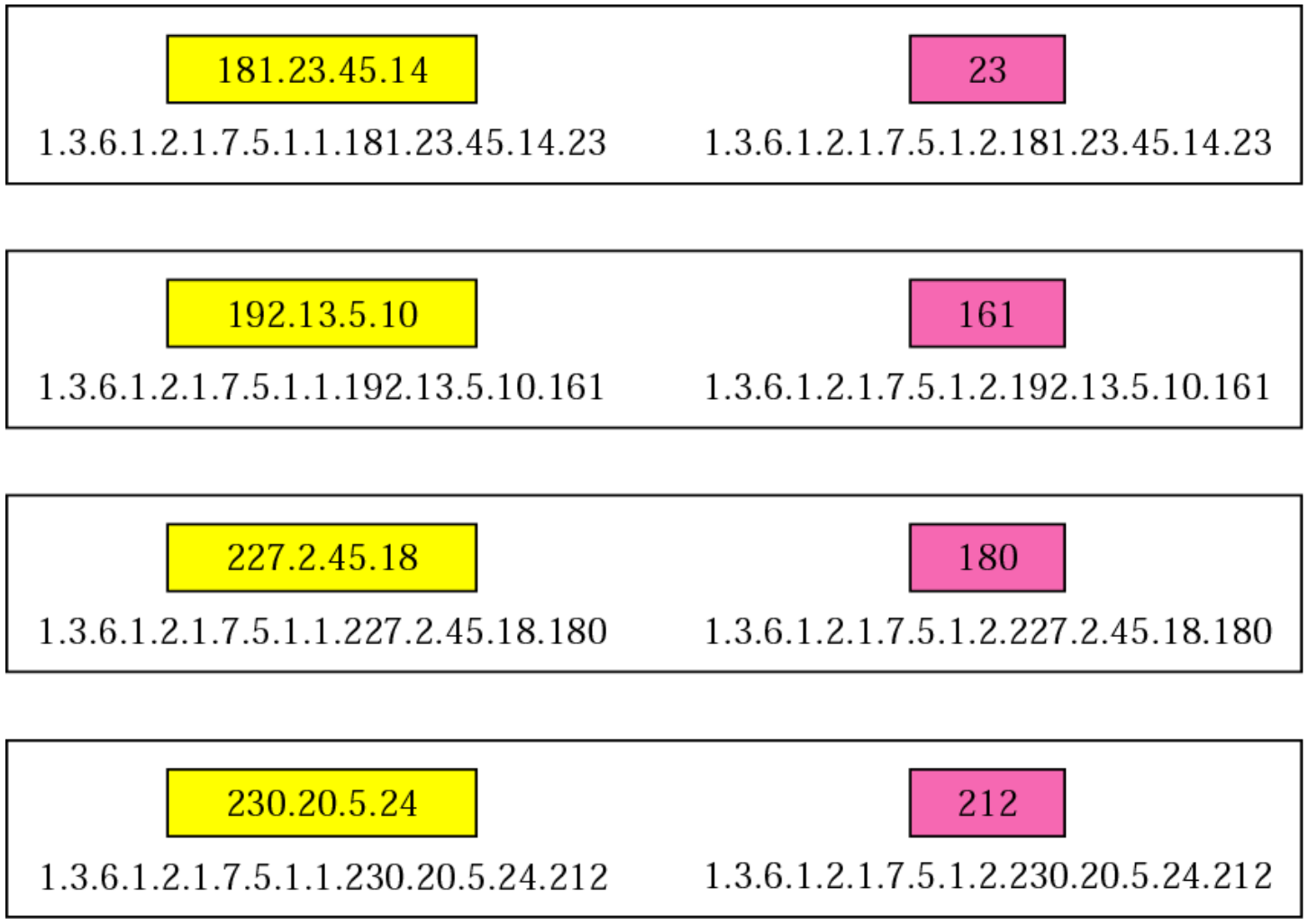
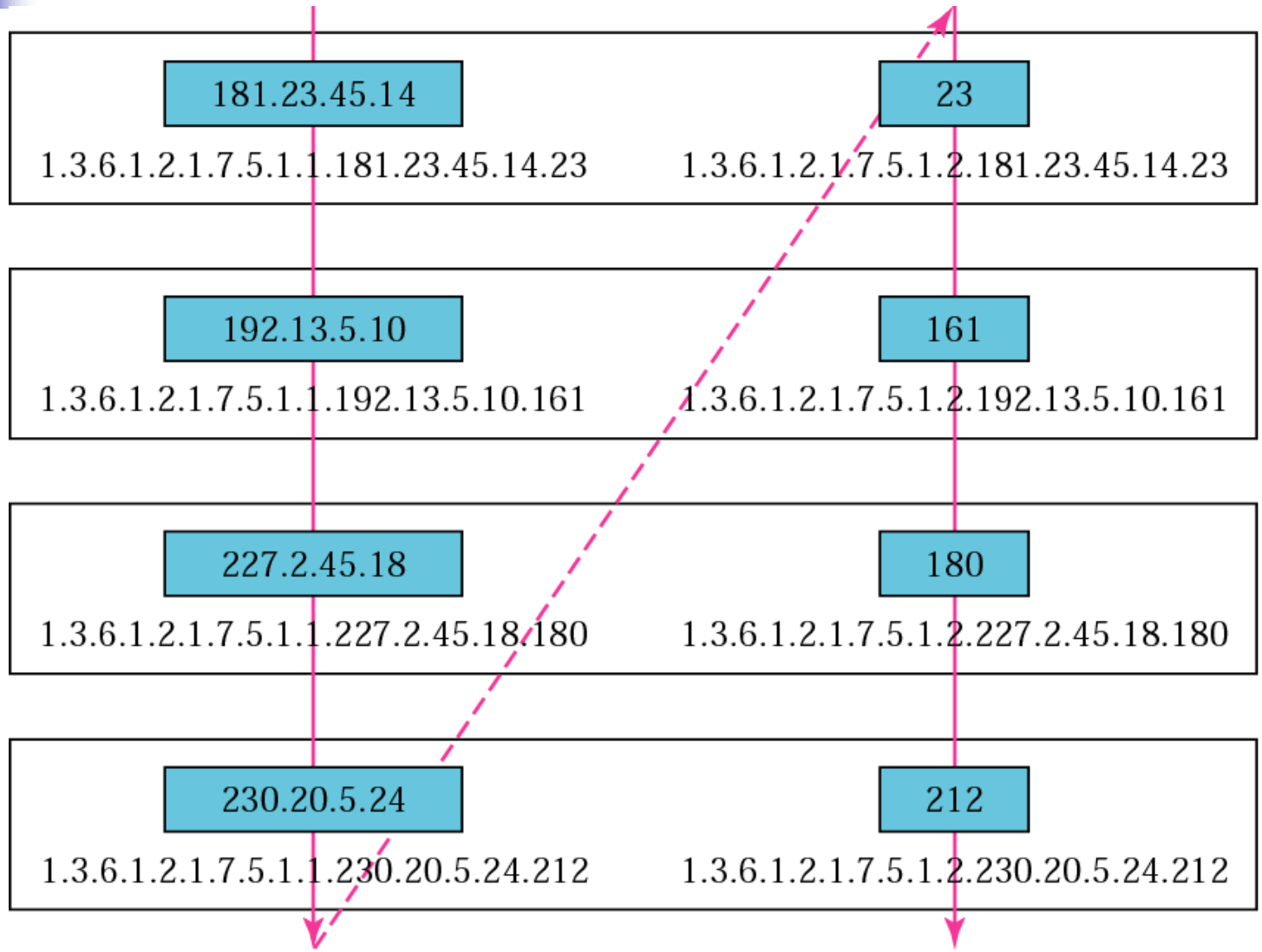


Figure 21.18 *Lexicographic ordering*



21.5 SNMP

SNMP is an application program that allows

1) *a manager to retrieve the value of an object defined in an agent;*
2) *a manager to store a value in an object defined in an agent;*
3) *an agent to send an alarm message about an abnormal situation to the manager*

The topics discussed in this section include:

PDUs
Format

Figure 21.19 *SNMP PDUs*

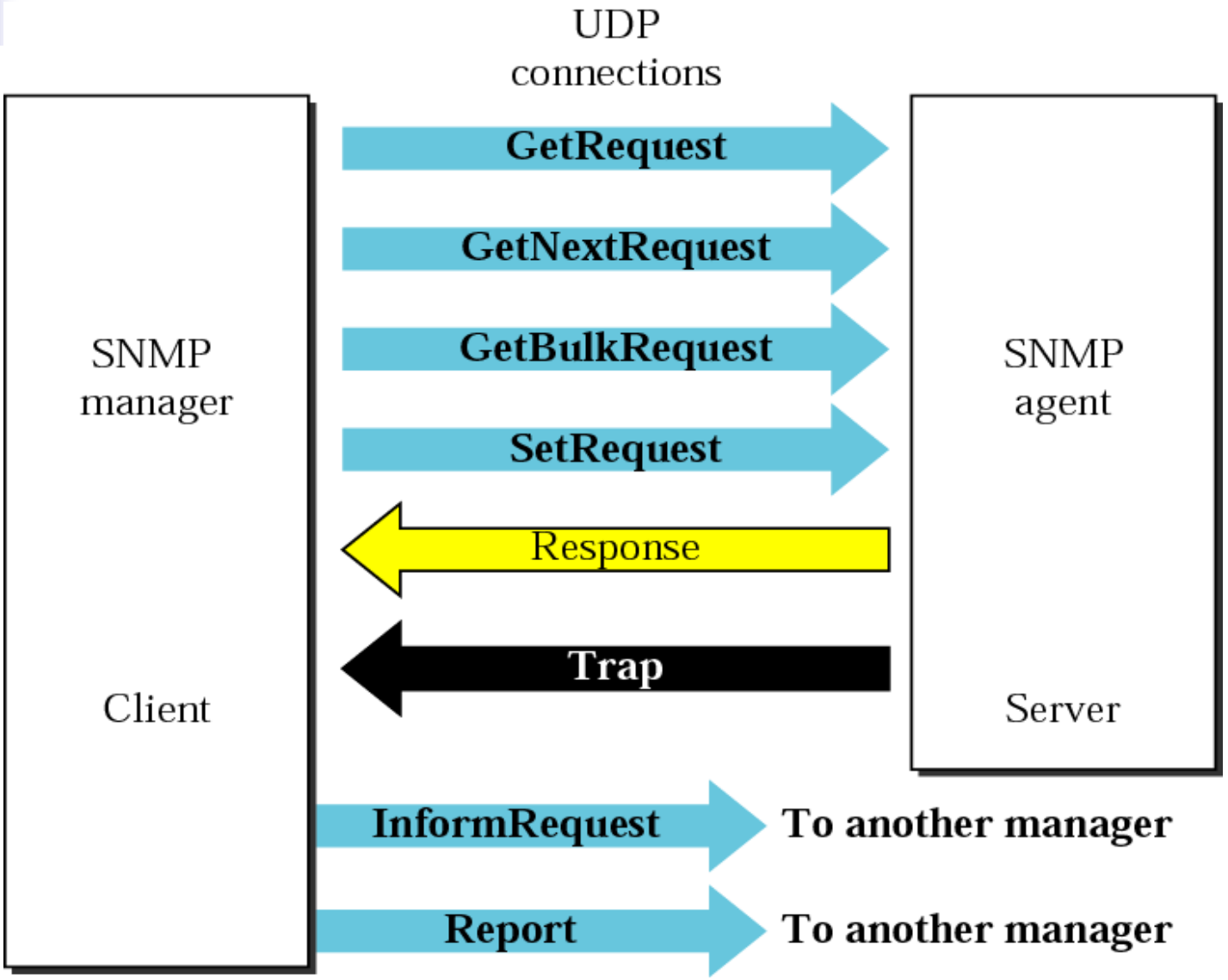
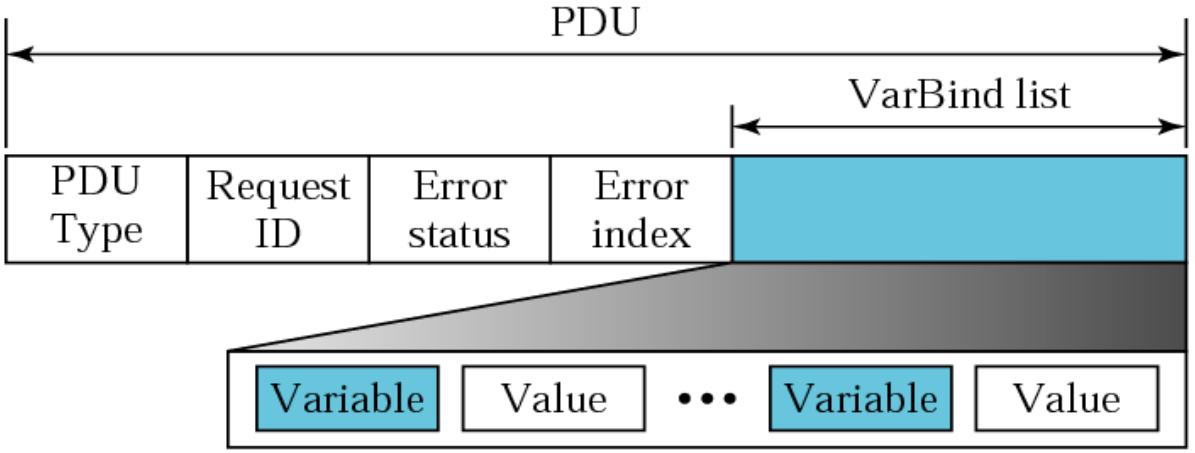


Figure 21.20 *SNMP PDU format*



Differences:

1. Error status and error index values are zeros for all request messages except GetBulkRequest.
2. Error status field is replaced by non-repeater field and error index field is replaced by max-repetitions field in GetBulkRequest.

Table 21.3 *Types of errors*

Status	*Name*	*Meaning*
0	noError	No error
1	tooBig	Response too big to fit in one message
2	noSuchName	Variable does not exist
3	badValue	The value to be stored is invalid
4	readOnly	The value cannot be modified
5	genErr	Other errors

21.6 MESSAGES

A message in SNMP is made of four elements: version, header, security parameters, and data (which includes the encoded PDU).

Figure 21.21 *SNMP message*

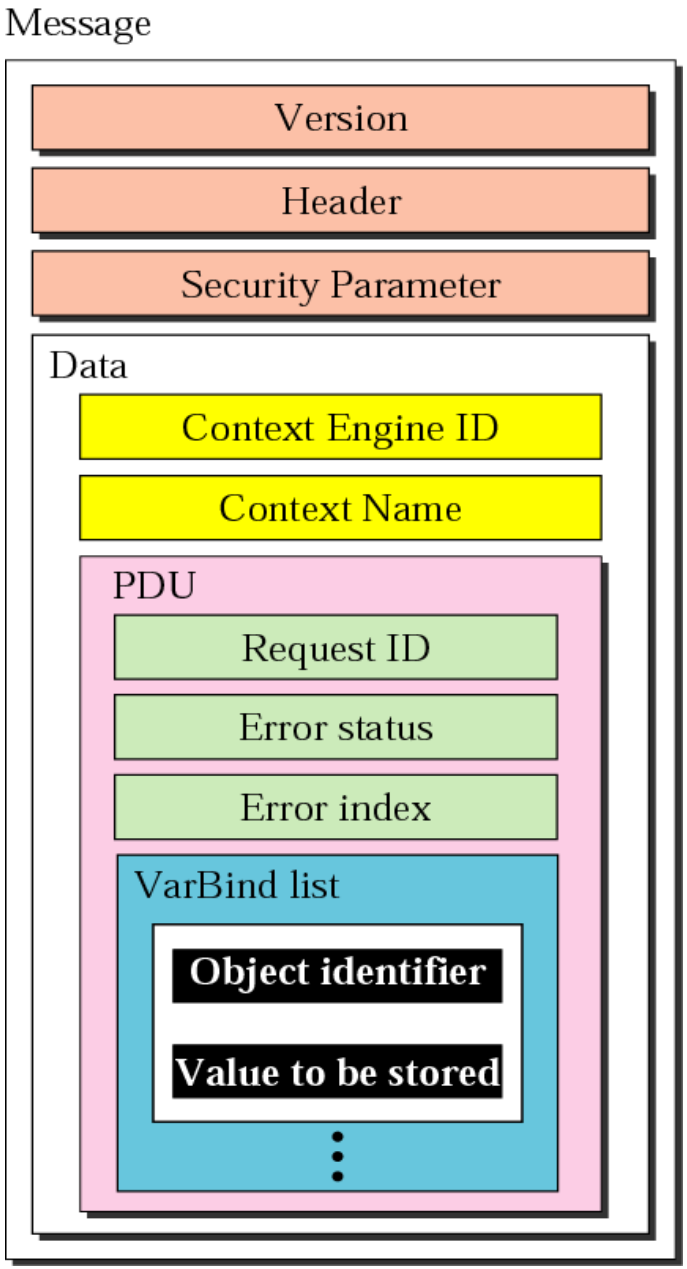
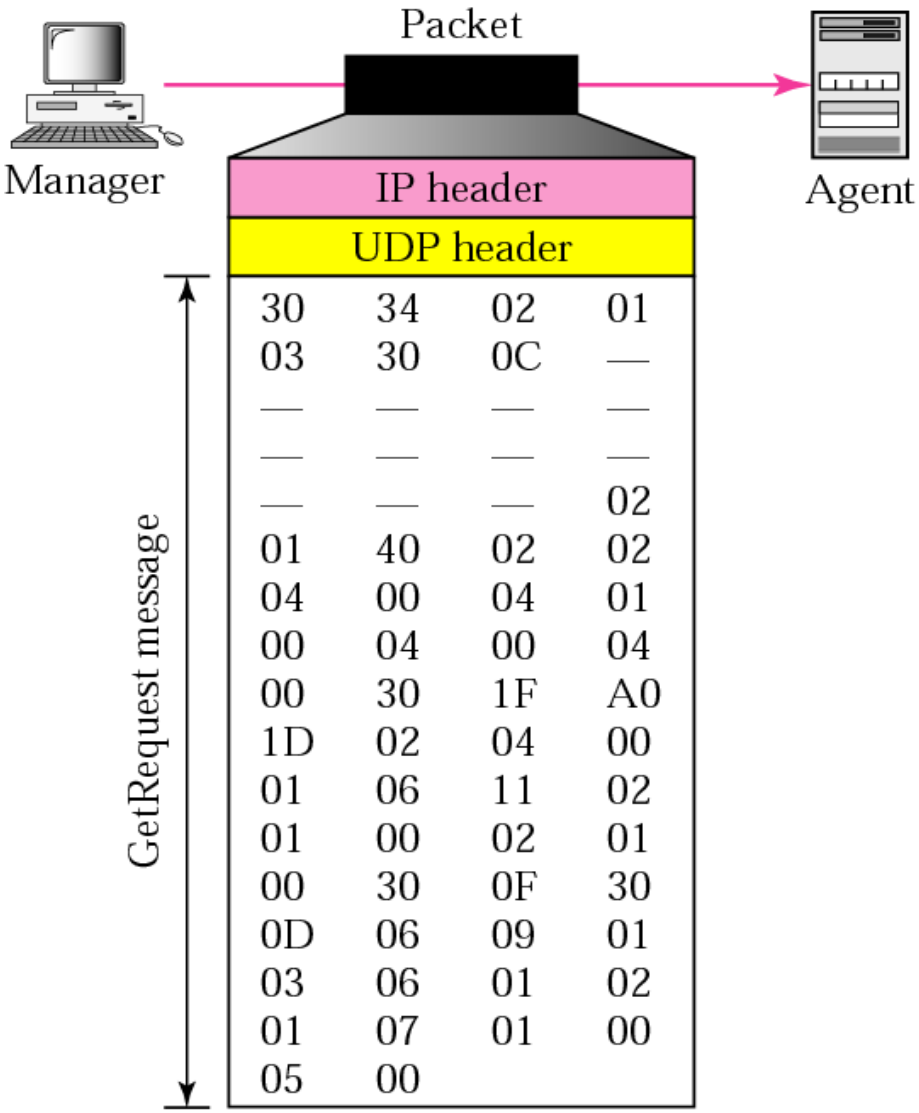


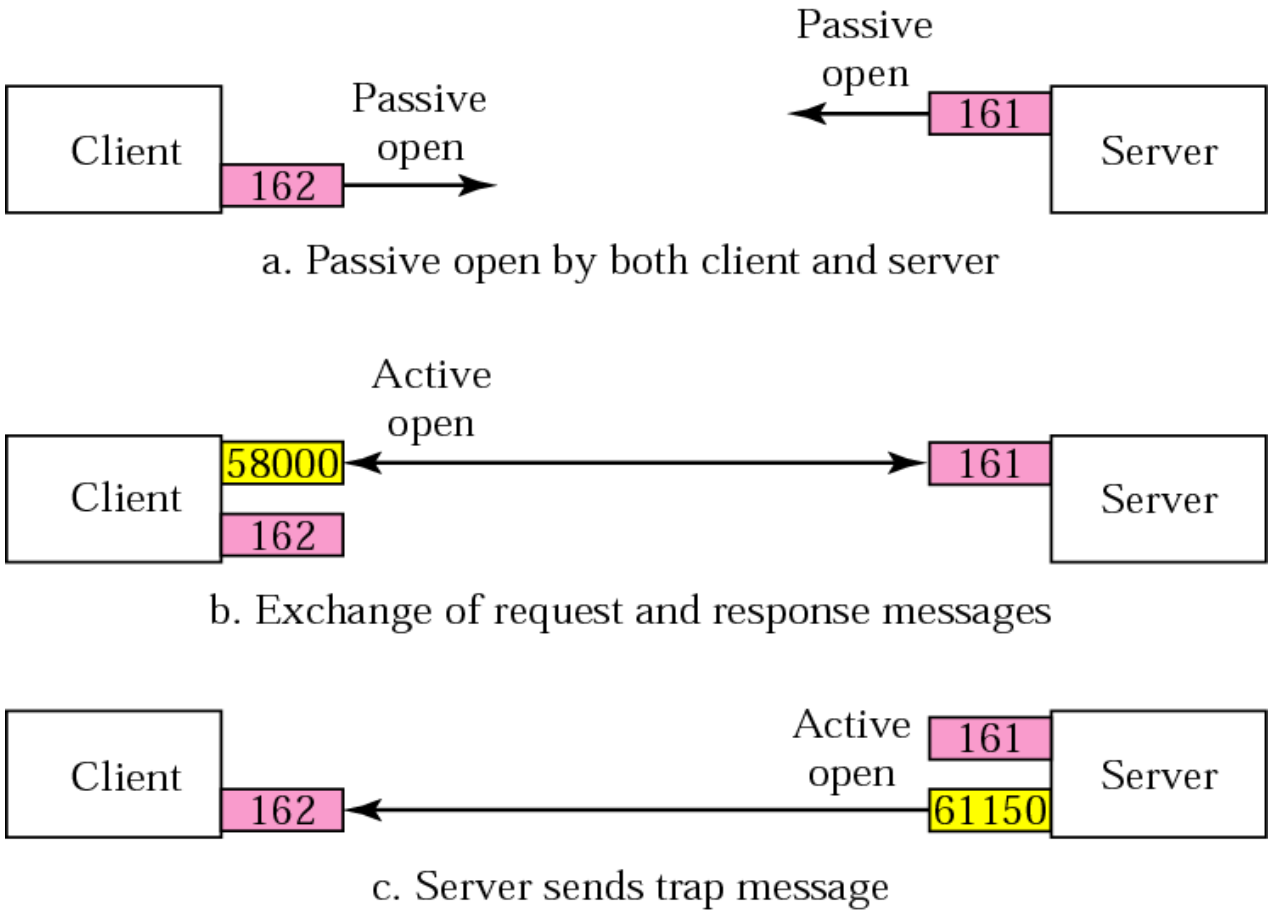
Figure 21.23 *GetRequest message*



21.7 UDP PORTS

SNMP uses the services of UDP on two well-known ports, 161 and 162. The well-known port 161 is used by the server (agent), and the well-known port 162 is used by the client (manager).

Figure 21.24 *Port numbers for SNMP*



21.8 SECURITY

The main difference between SNMPv3 and SNMPv2 is the enhanced security. SNMPv3 provides two types of security: general and specific. SNMPv3 provides message authentication, privacy, and manager authorization.