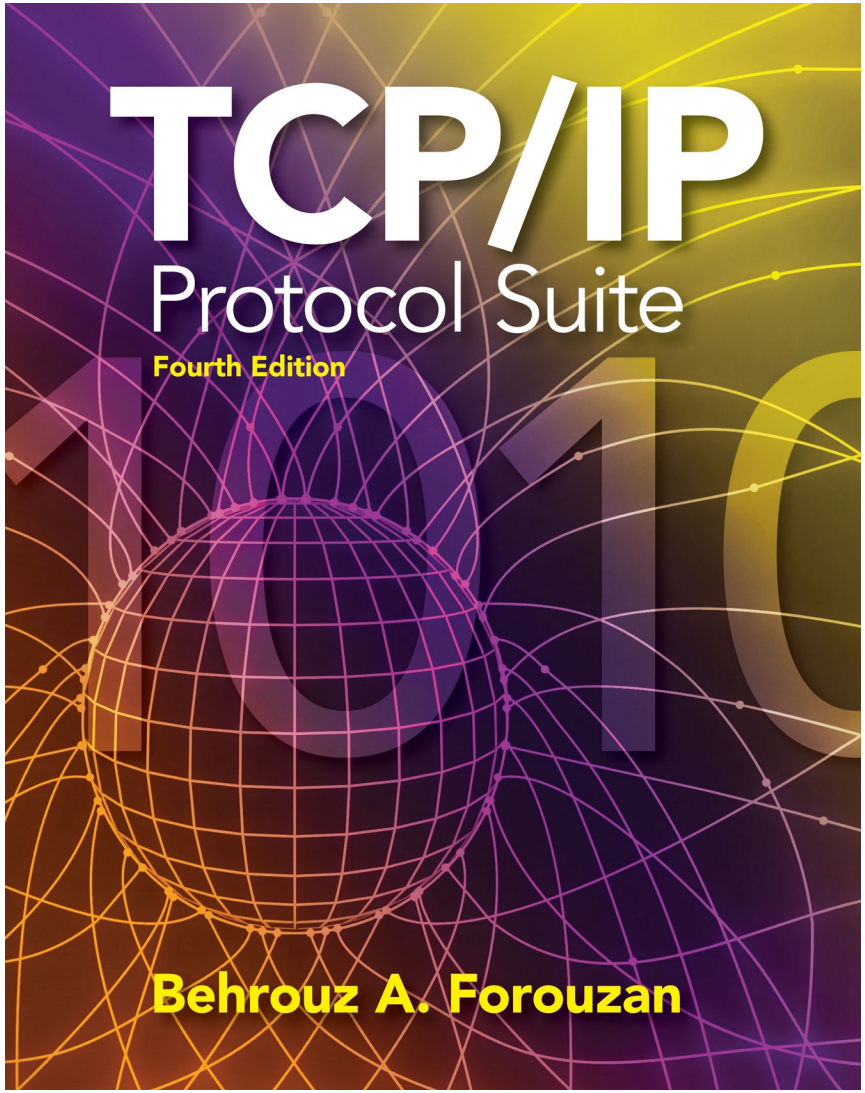
Chapter 24

Network Management: SNMP



OBJECTIVES:

- To discuss SNMP as a framework for managing devices in an internet using the TCP/IP protocol suite.
- To define a manager as a host that runs SNMP client and any agents as a router or host that runs a server program.
- Discuss SMI and MIB, which are used by SNMP.
- To show how SMI names objects, defines the type of data, and encodes data.
- To show how data types are defined using ASN.1.
- To show how SMI uses BER to encode data.
- To show the functionality of SNMP using three methods.

OBJECTIVES:

- To show how SNMP uses two different ports of UDP.
- To show how SNMPv3 has enhanced security features over previous versions.

Chapter Outline

24.1 Concept

24.2 Management Componen

24.3 SMI

24.4 MIB

24.5 SNMP

24.6 UDP Ports

24.7 Security

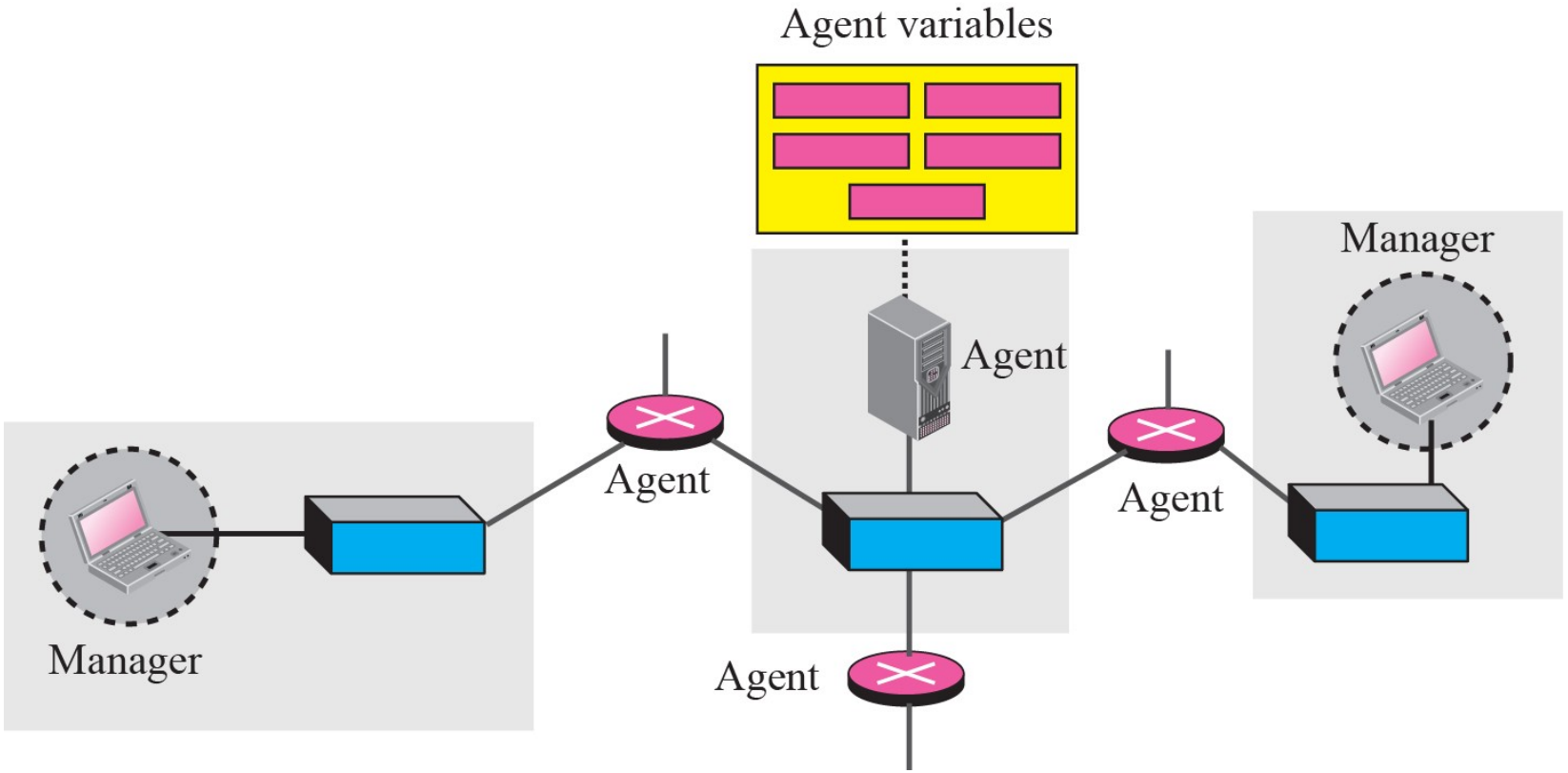
24-1 CONCEPT

SNMP uses the concept of manager and agent. That is, a manager, usually a host, controls and monitors a set of agents, usually routers or servers (see Figure 24.1).

Topics Discussed in the Section

- ✓ **Managers and Agents**

Figure 24.1 *SNMP concept*



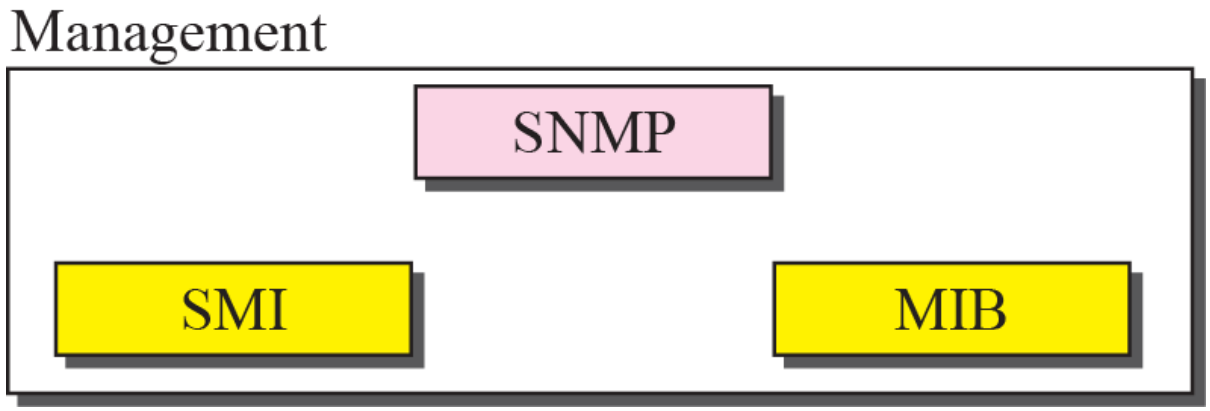
24-2 MANAGEMENT COMPONENTS

To do management tasks, SNMP uses two other protocols: Structure of Management Information (SMI) and Management Information Base (MIB). In other words, management on the Internet is done through the cooperation of three protocols: SNMP, SMI, and MIB, as shown in Figure 24.2.

Topics Discussed in the Section

- ✓ **Role of SNMP**
- ✓ **Role of SMI**
- ✓ **Role of MIB**
- ✓ **An Analogy**
- ✓ **An Overview**

Figure 24.2 *Companion of network management on the Internet*



Note

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

Note

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

Figure 24.3 *Comparing computer programming and network management*

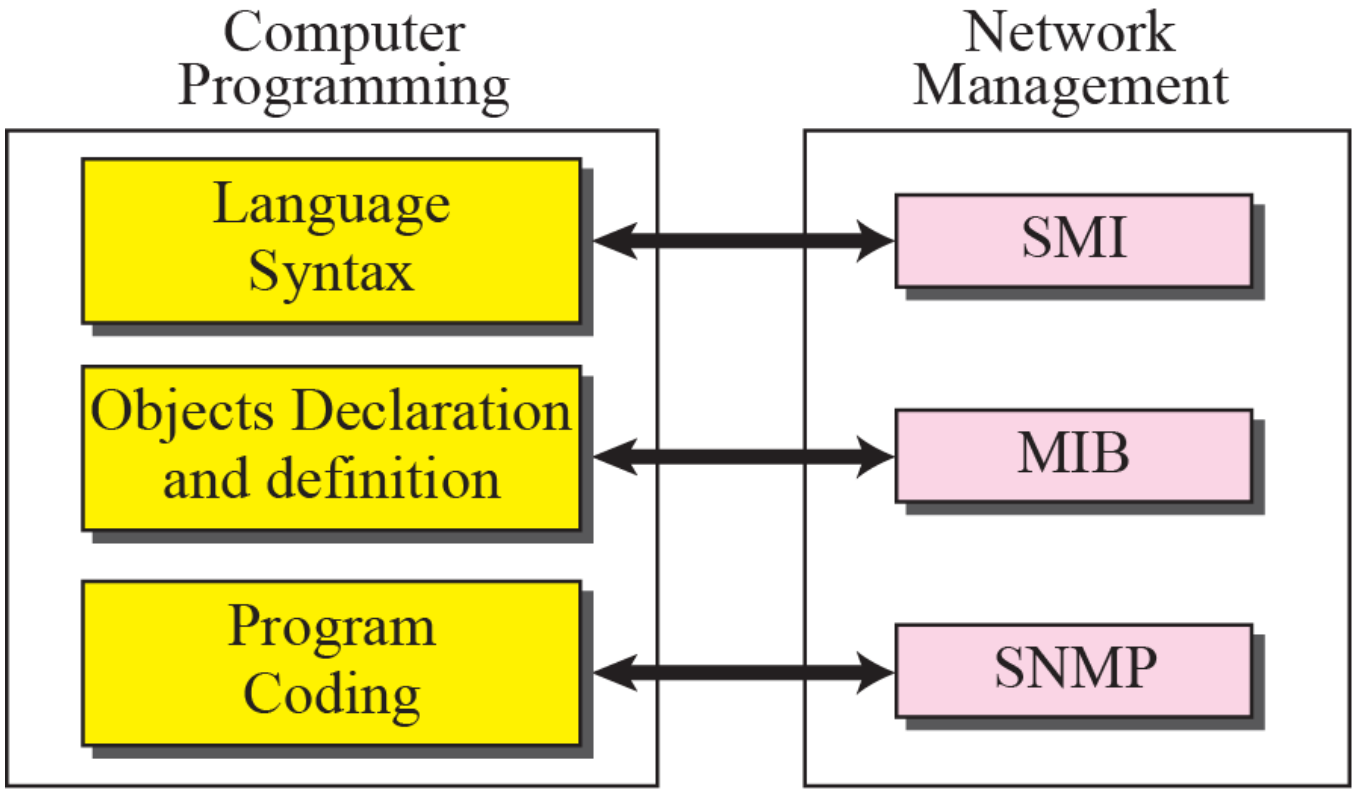
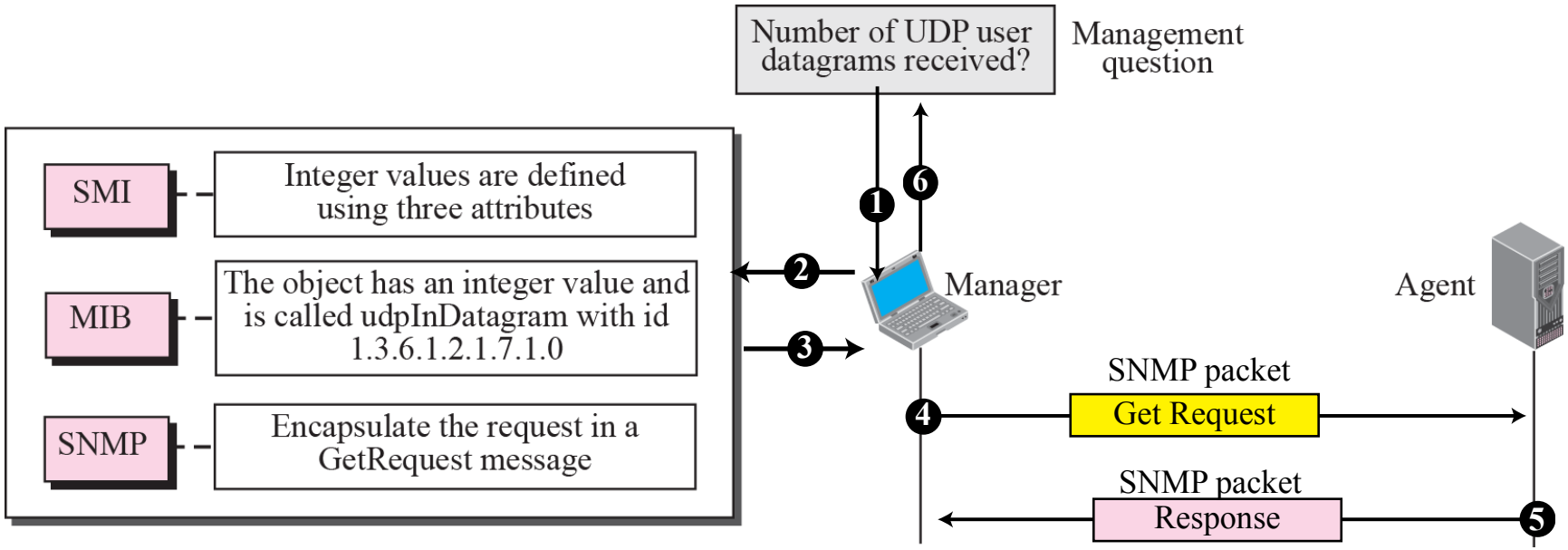


Figure 24.4 *Management overview*



24-3 SMI

The Structure of Management Information is a component for network management. Its functions are:

1. To name objects.

2. To define the type of data that can be stored in an object.

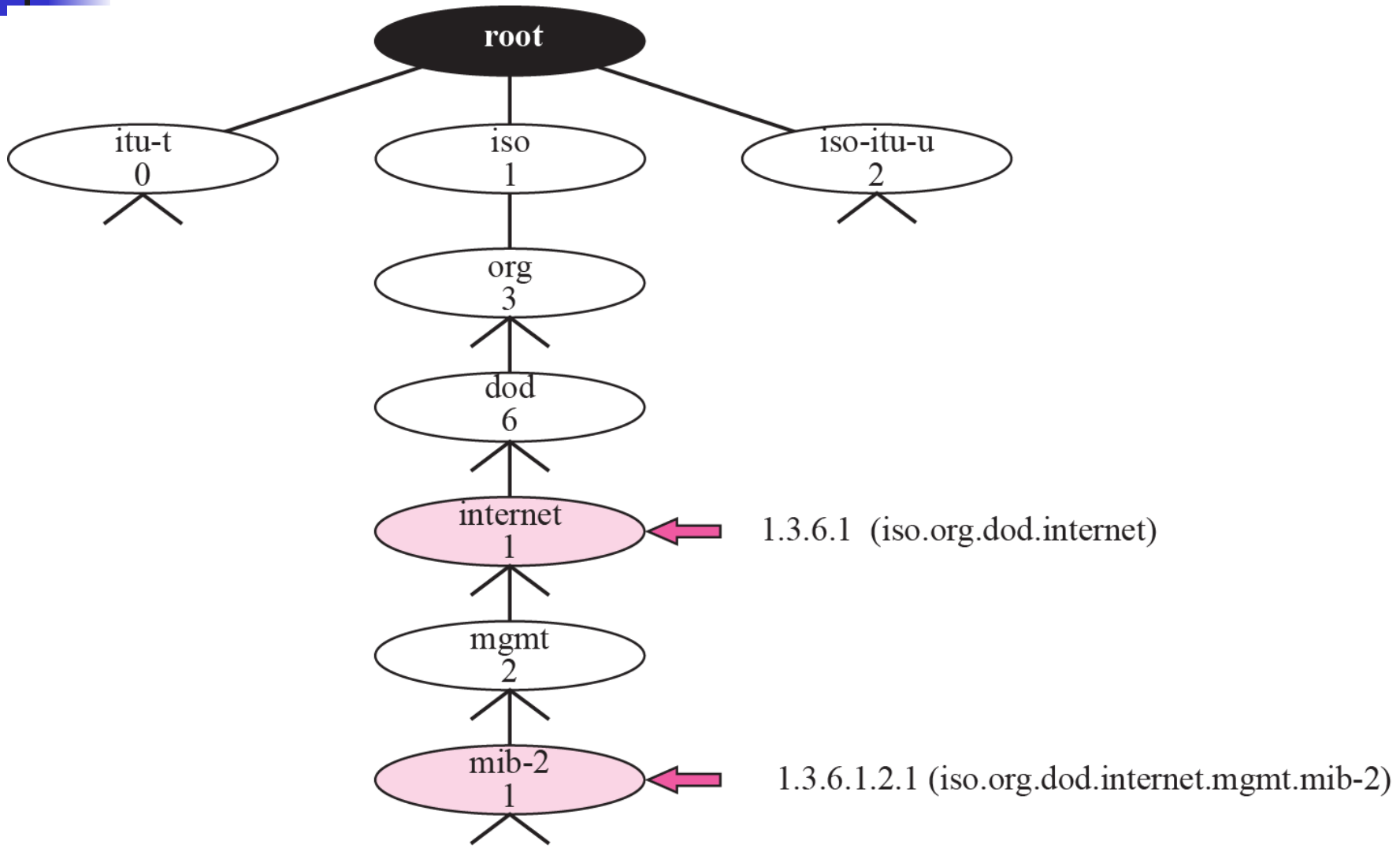
3. To show how to encode data for transmission over the network.

SMI is a guideline for SNMP. It emphasizes three attributes to handle an object: name, data type, and encoding method.

Topics Discussed in the Section

- ✓ **Name**
- ✓ **Type**
- ✓ **Encoding Method**

Figure 24.5 *Object identifier*



Note

All objects managed by SNMP are given an object identifier. The object identifier always starts with 1.3.6.1.2.1.

Table 24.1 *Data Types*

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 24.6 *Conceptual data types*

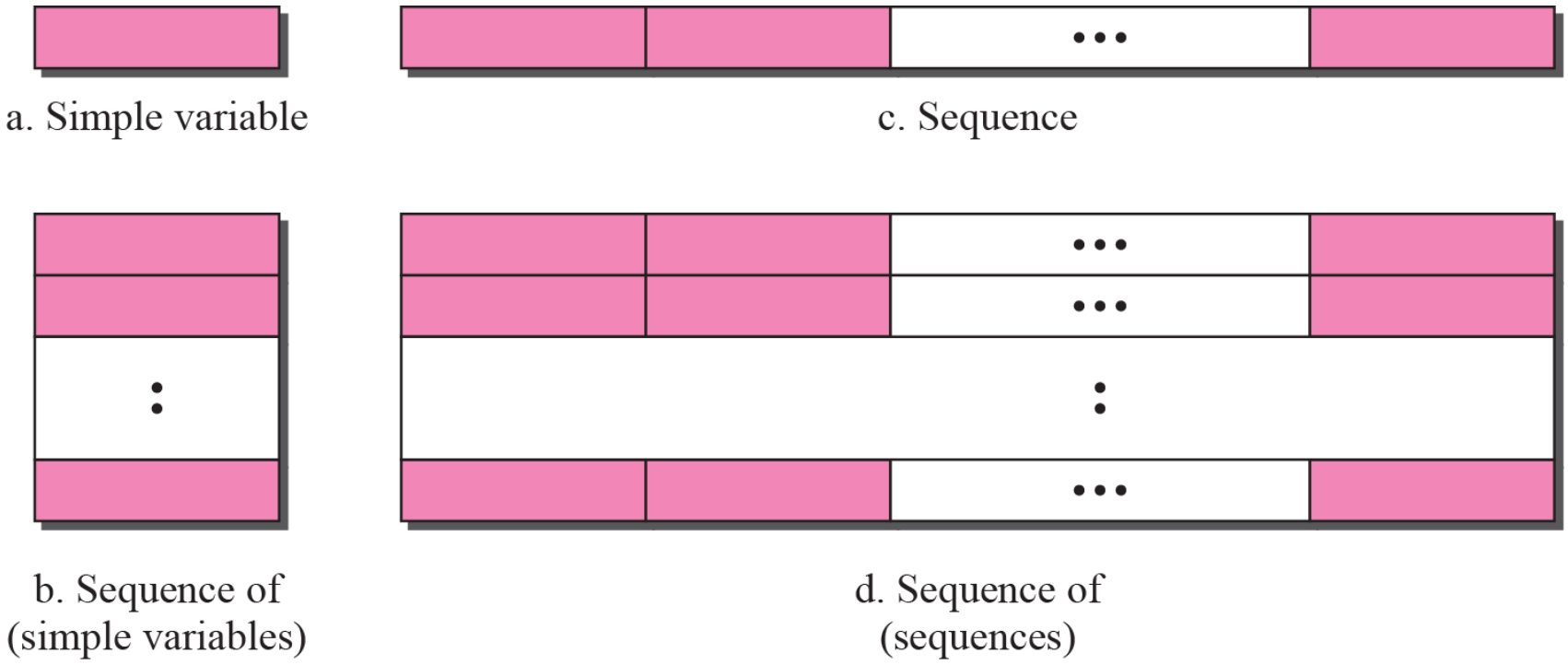


Figure 24.7 *Encoding format*

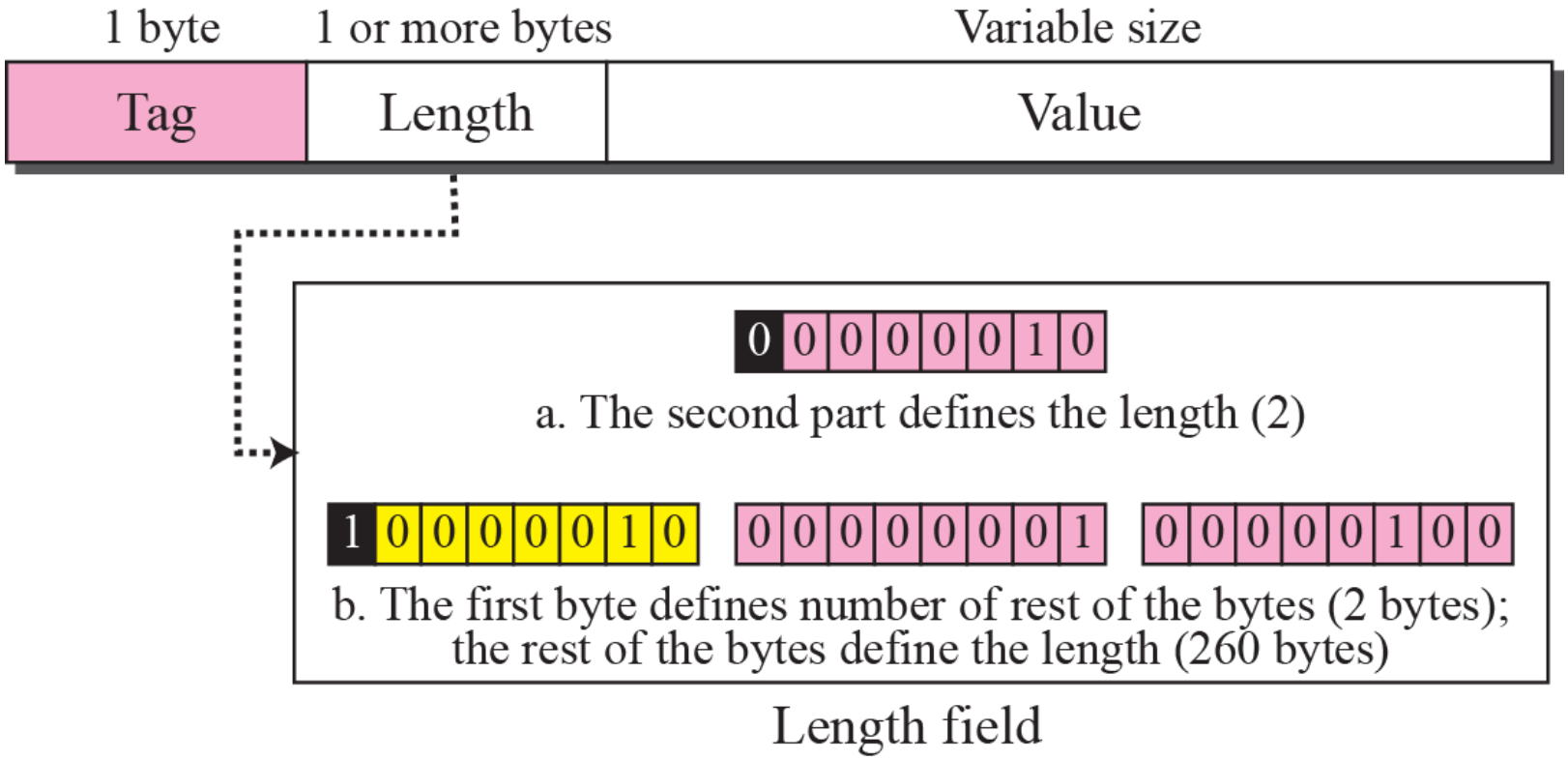


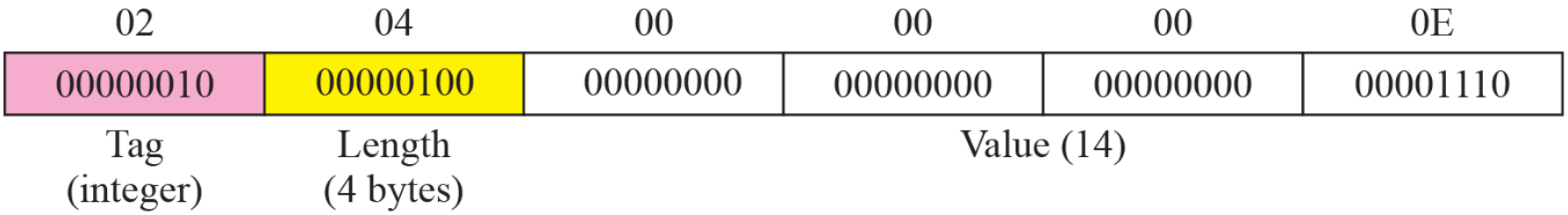
Table 24.2 *Codes for Data Types*

Data Type	*Tag (Binary)*	*Tag (Hex)*
INTEGER	**00000010**	**02**
OCTET STRING	**00000100**	**04**
OBJECT IDENTIFIER	**00000110**	**06**
NULL	**00000101**	**05**
Sequence, sequence of	**00110000**	**30**
IPAddress	**01000000**	**40**
Counter	**01000001**	**41**
Gauge	**01000010**	**42**
TimeTicks	**01000011**	**43**
Opaque	**01000100**	**44**

Example 24.1

Figure 24.8 shows how to define INTEGER 14. Note that we have used both binary representation and hexadecimal representation for the tag. The size of the length field is from Table 24.1.

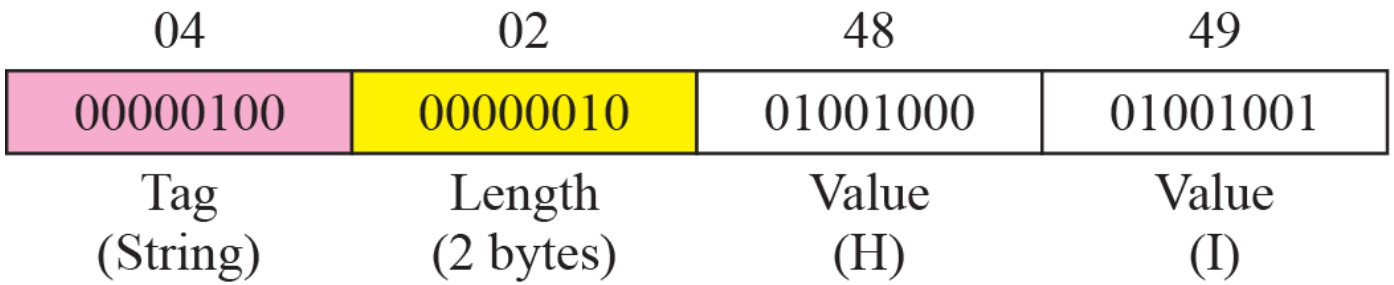
Figure 24.8 *Example 24.1: INTEGER 14*



Example 24.2

Figure 24.9 shows how to define the OCTET STRING “HI.”

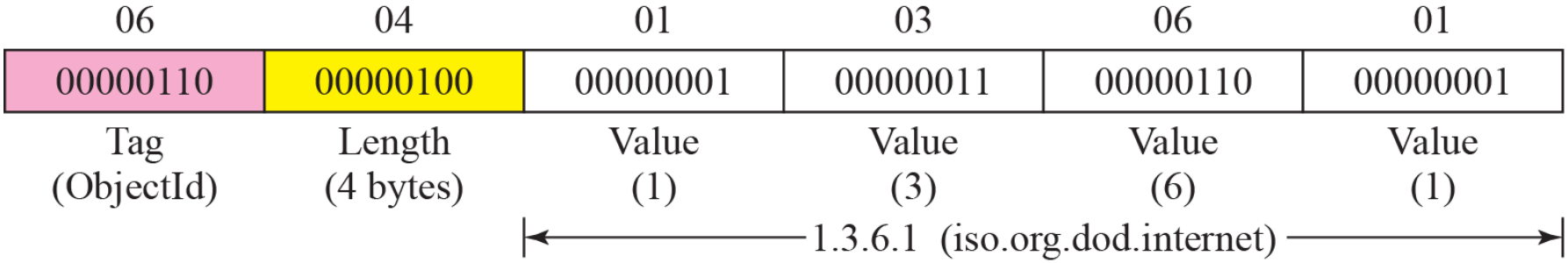
Figure 24.9 *Example 24.2: OCTET STRING "HI"*



Example 24.3

Figure 24.10 shows how to define ObjectIdentifier 1.3.6.1 (iso.org.dod.internet).

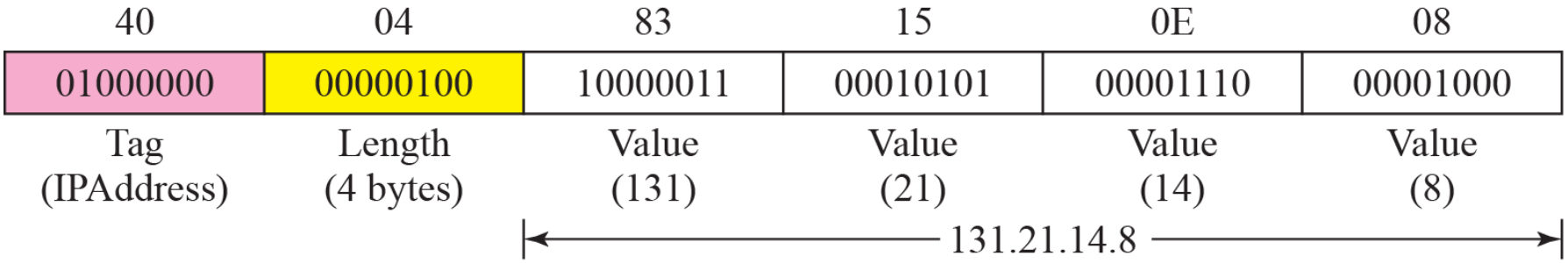
Figure 24.10 *Example 24.3: ObjectIndentifier 1.3.6.1*



Example 24.4

Figure 24.11 shows how to define IPAddress 131.21.14.8.

Figure 24.11 *Example 24.4: IPAddress 131.21.14.8*



24-4 MIB

The Management Information Base, version 2 (MIB2) is the second component used in network management. Each agent has its own MIB2, which is 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, and snmp. These groups are under the mib-2 object in the object identifier tree (see Figure

Topics Discussed in the Section

- ✓ **Accessing MIB Variables**
- ✓ **Lexicographic Ordering**

Figure 24.12 *mib-2*

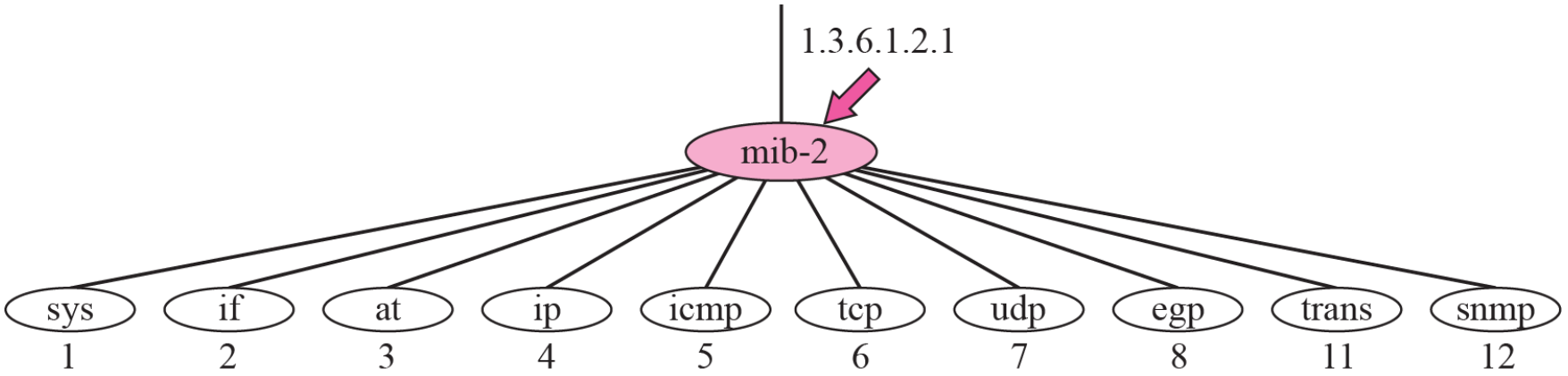


Figure 24.13 *udp group*

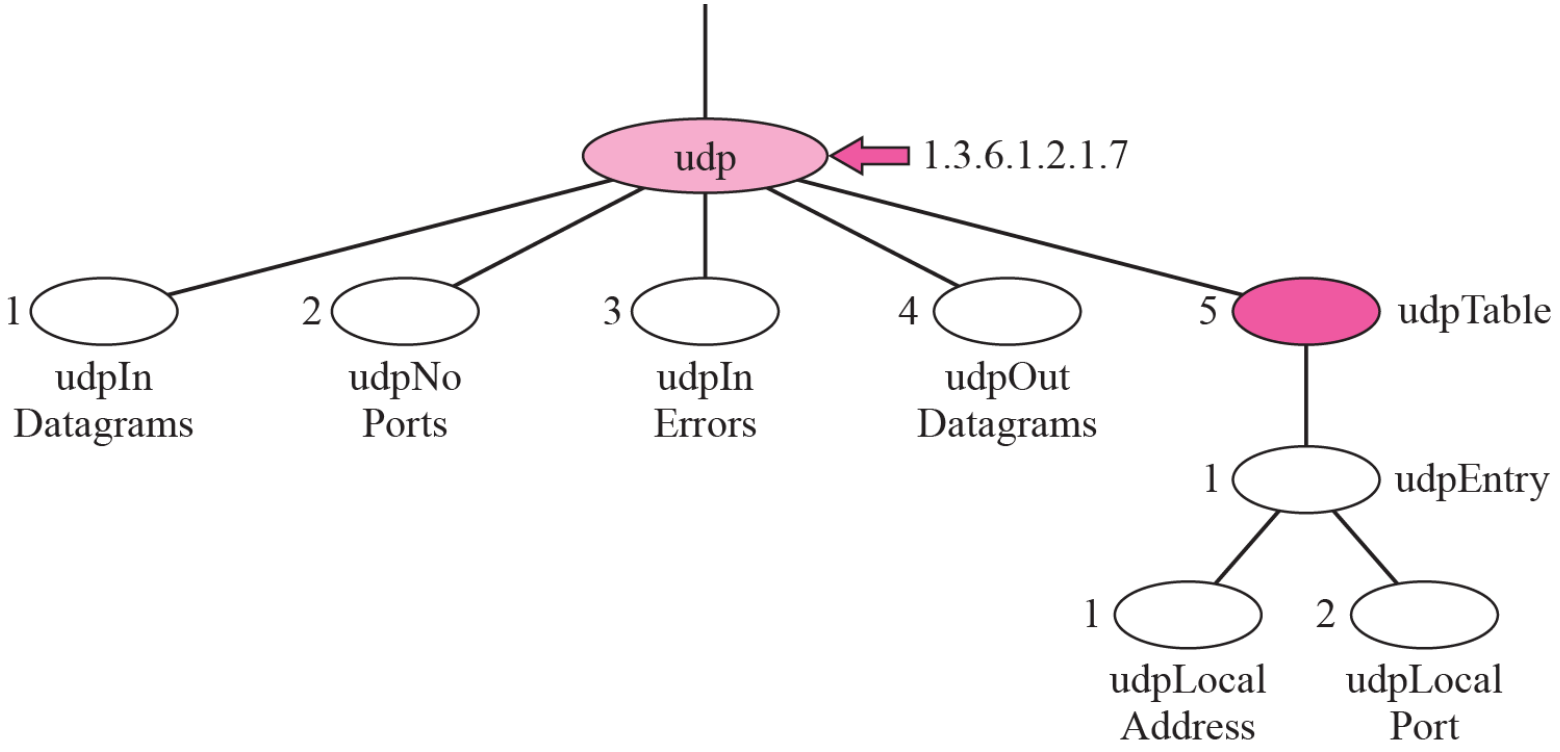


Figure 24.14 *udp variables and tables*

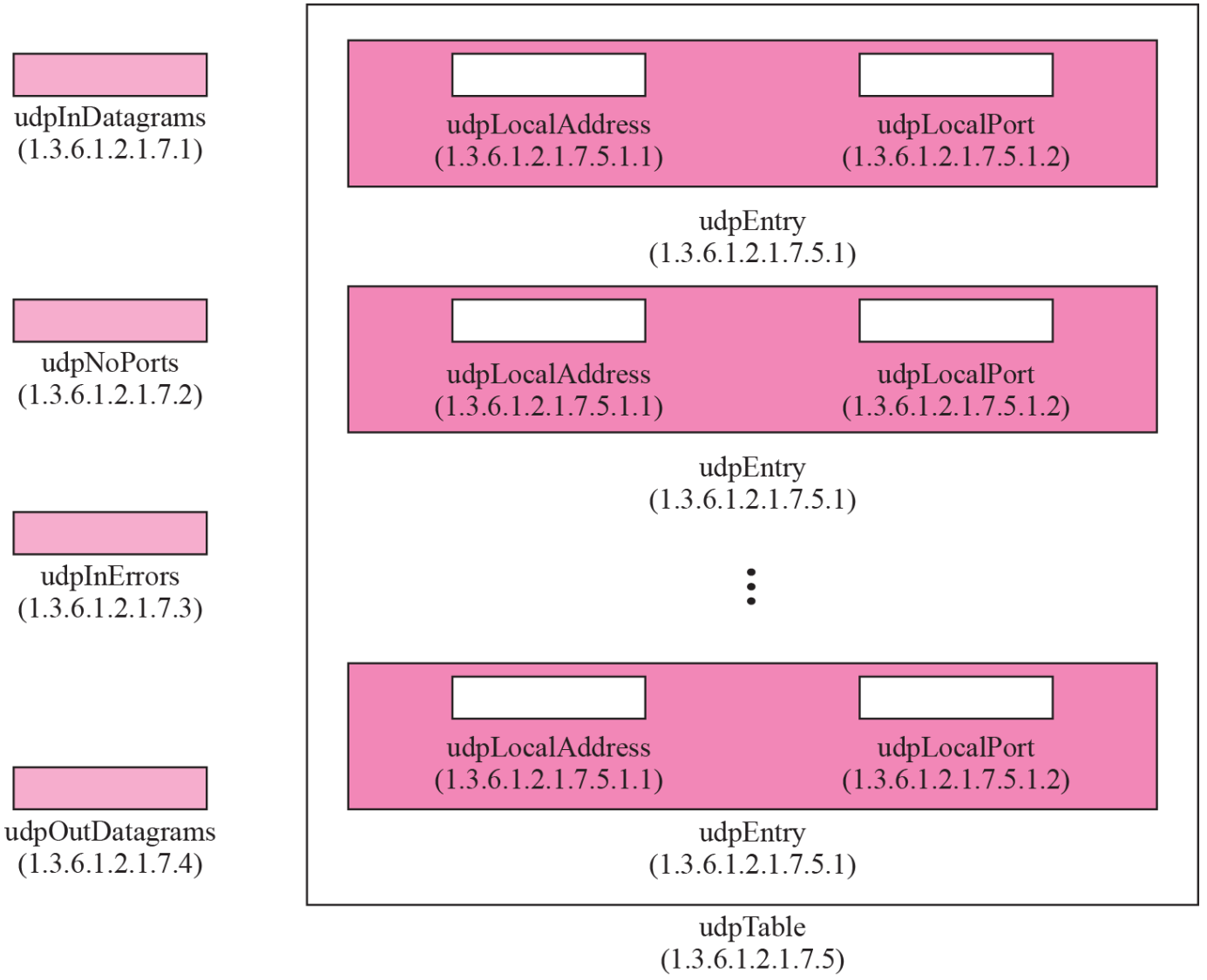


Figure 24.15 *Indexes for udpTable*

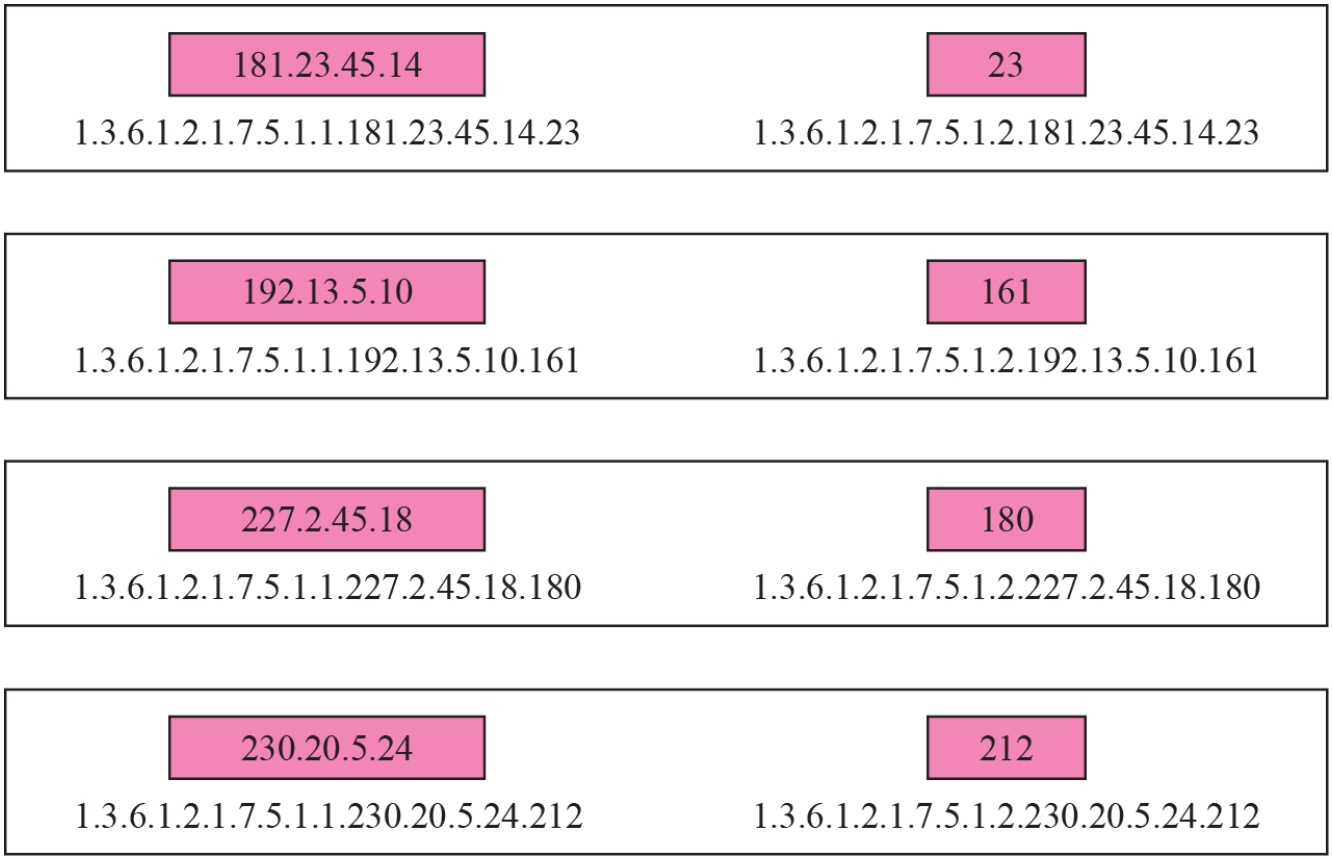
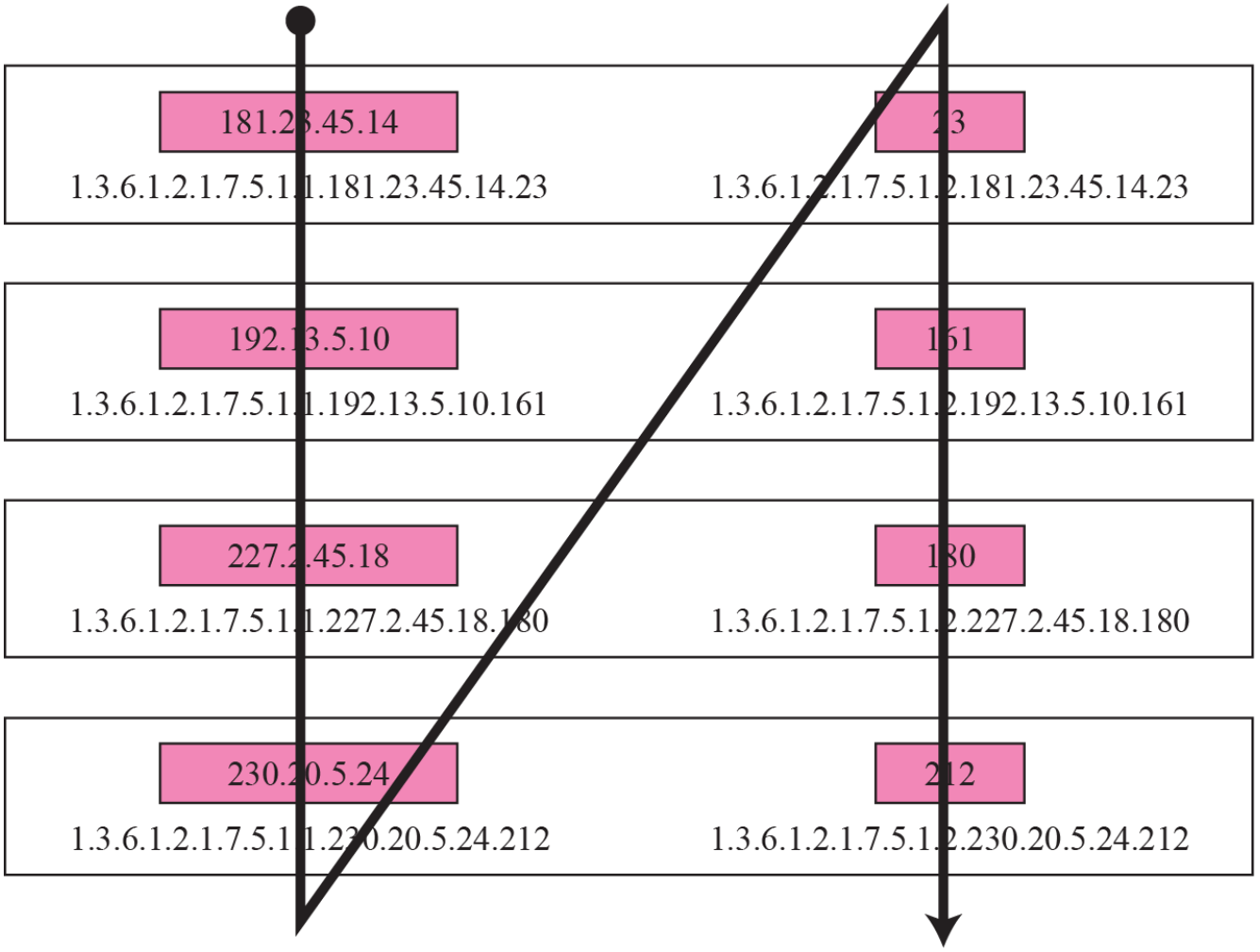


Figure 24.16 *Lexicographic ordering*



24-5 SNMP

SNMP uses both SMI and MIB in Internet network management. It 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.**

Topics Discussed in the Section

- ✓ **PDUs**
- ✓ **Format**
- ✓ **Messages**

Figure 24.17 *SNMP PDUs*

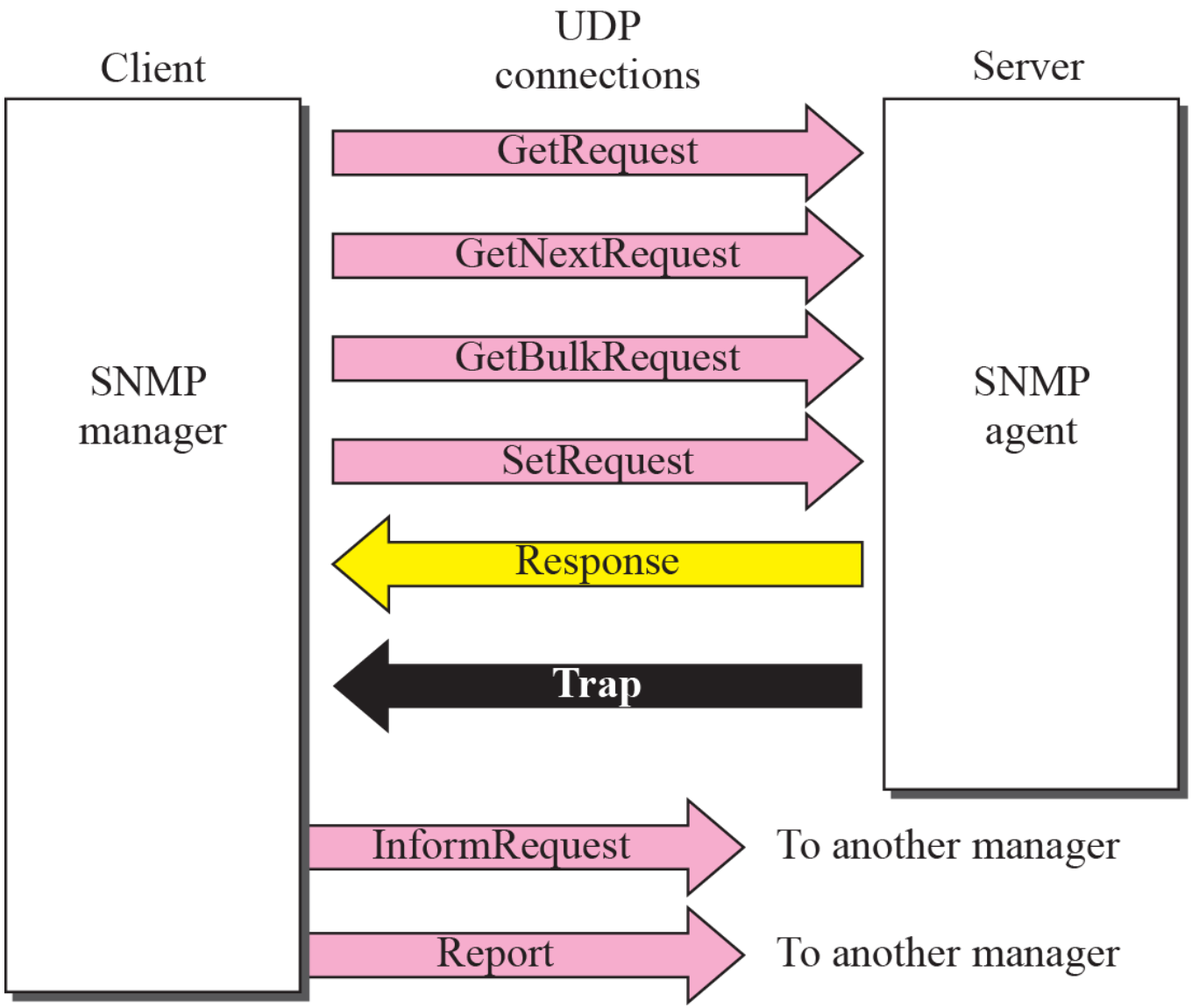
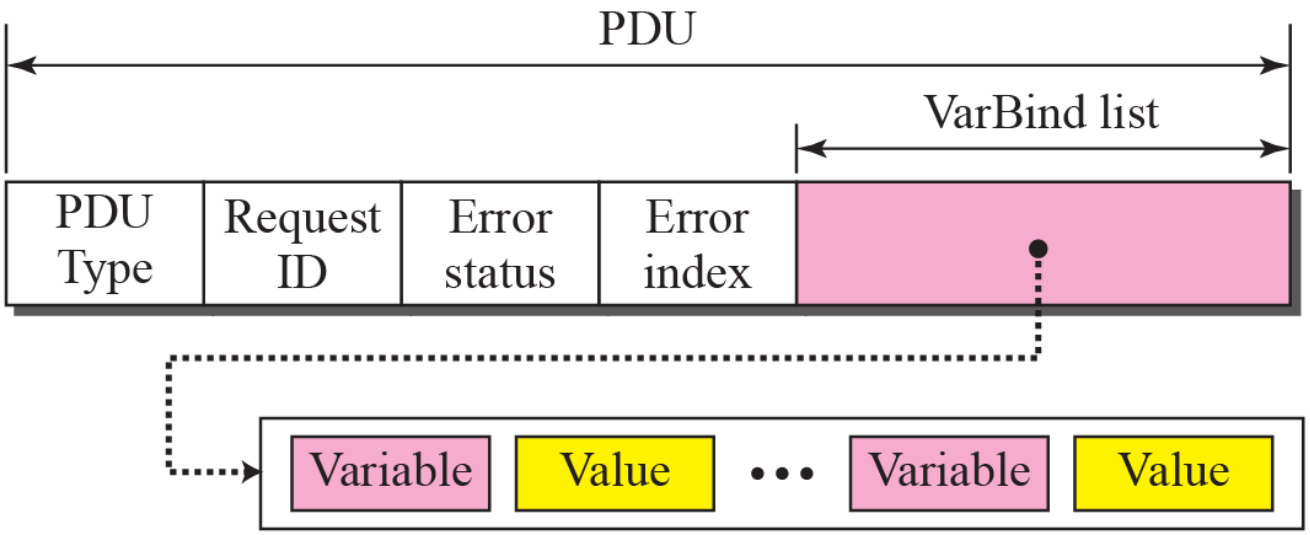


Figure 24.18 *SNMP PDU format*



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.

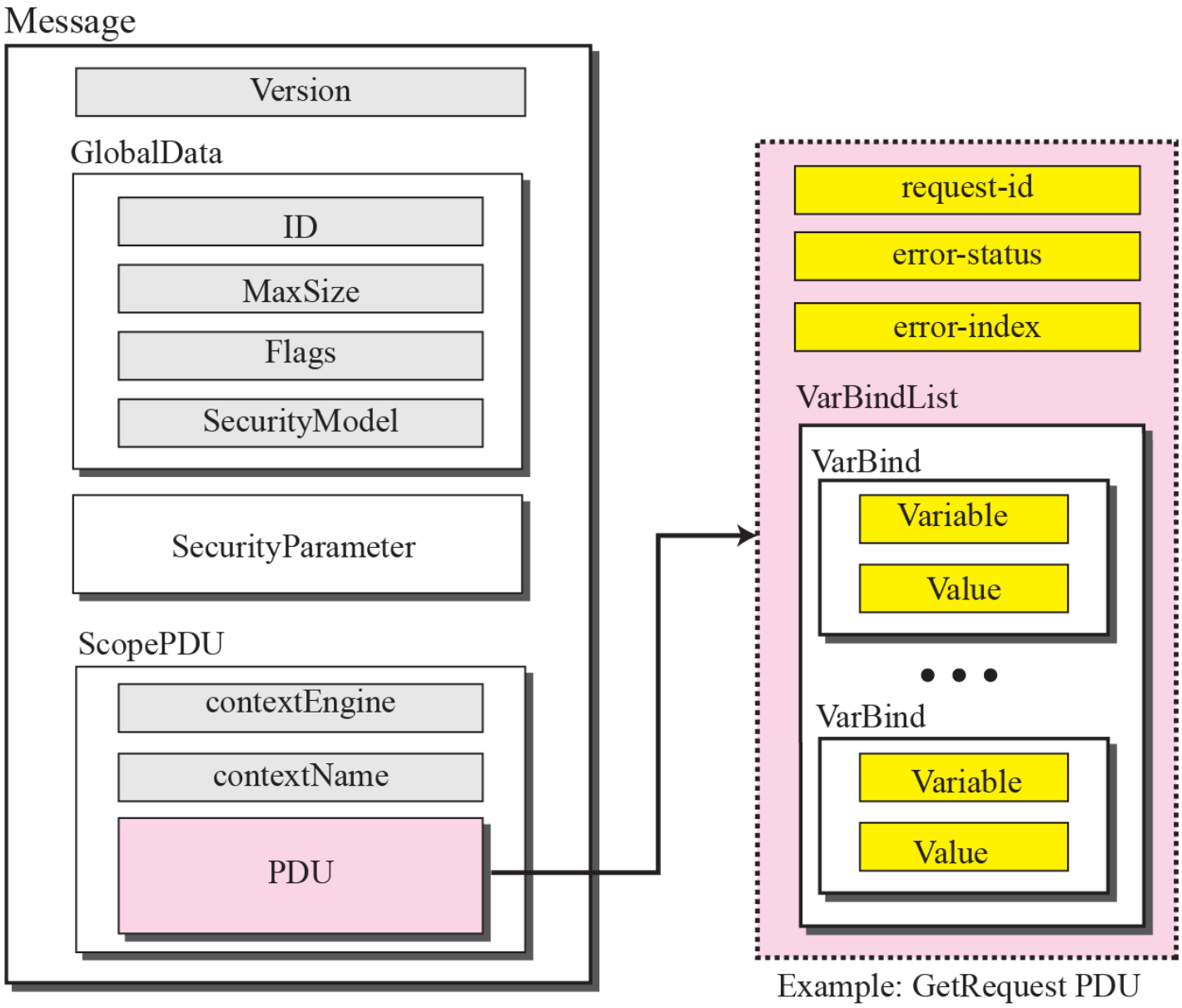
Table 24.3 *PDU Types*

Type	*Tag (Binary)*	*Tag (Hex)*
GetRequest	**10100000**	**A0**
GetNextRequest	**10100001**	**A1**
Response	**10100010**	**A2**
SetRequest	**10100011**	**A3**
GetBulkRequest	**10100101**	**A5**
InformRequest	**10100110**	**A6**
Trap (SNMPv2)	**10100111**	**A7**
Report	**10101000**	**A8**

Table 24.4 *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

Figure 24.19 *SNMP message*



Example 24.4

In this example, a manager station (SNMP client) uses a message with GetRequest PDU to retrieve the number of UDP datagrams that a router has received (Figure 24.20). There is only one VarBind sequence. The corresponding MIB variable related to this information is udpInDatagrams with the object identifier 1.3.6.1.2.1.7.1.0. The manager wants to retrieve a value (not to store a value), so the value defines a null entity. The bytes to be sent are shown in hexadecimal representation.

Figure 24.20 *Example 24.5*

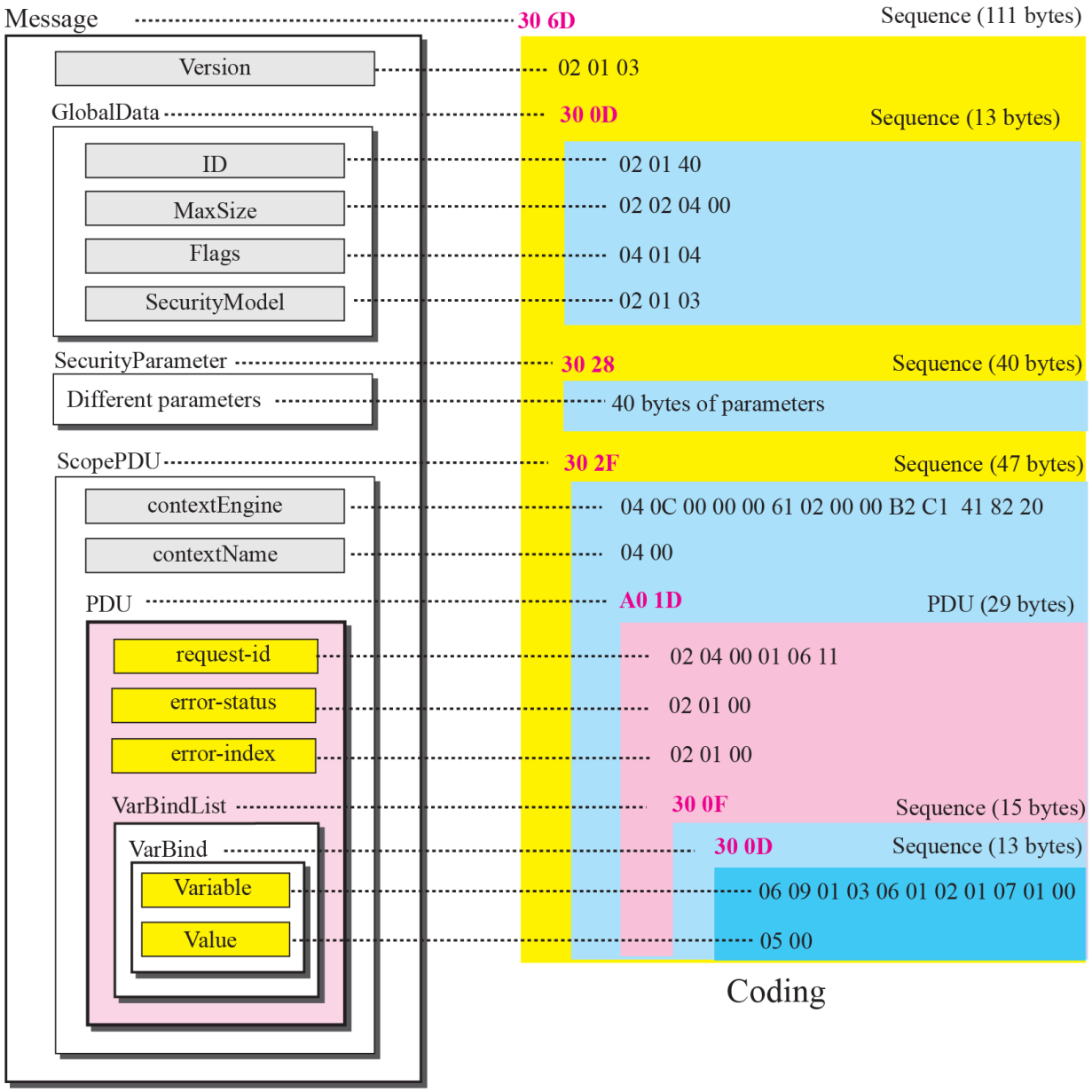


Figure 24.21 *Actual message sent for Example 24.5*

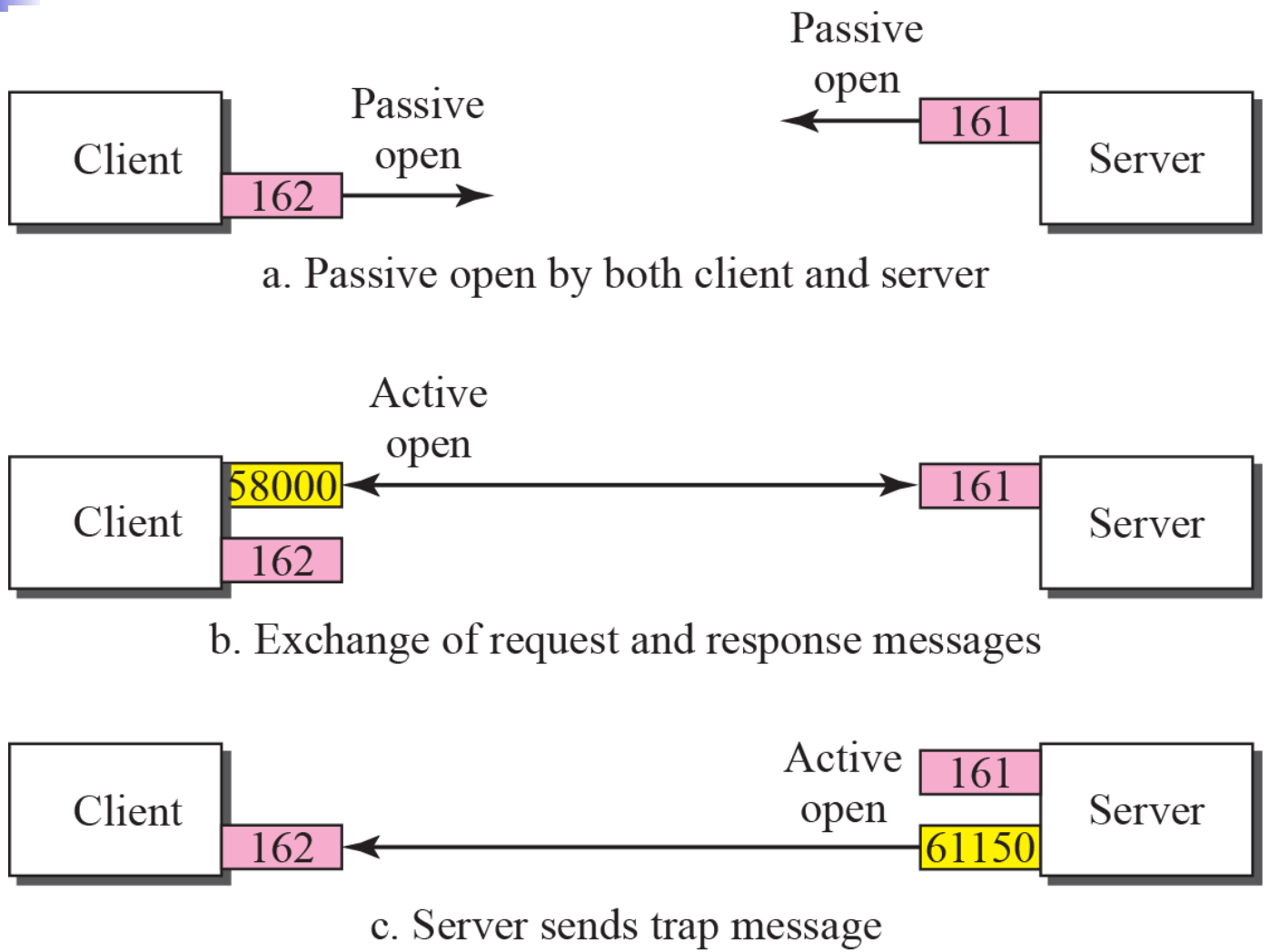
Message

30	**6D**	**02**	**01**	03	**30**	**0D**	02	01	04	02	02	04	00	04	01
04	02	01	03	**30**	**28**	--	--	--	--	--	--	--	--	--	--
--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--
--	--	--	--	--	--	--	--	--	--	--	--	--	--	**30**	**2F**
04	0C	00	00	00	61	02	00	00	B2	C1	41	82	20	04	00
A0	**1D**	**02**	**04**	00	01	06	11	02	01	00	02	01	00	**30**	**0F**
30	**0D**	**06**	**09**	01	03	06	01	02	01	07	01	00	05	00	

24-6 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 24.2 *Port numbers for SNMP*



24-7 SECURITY

SNMPv3 has added two new features to the previous version: security and remote administration. SNMPv3 allows a manager to choose one or more levels of security when accessing an agent. Different aspects of security can be configured by the manager to allow message authentication, confidentiality, and integrity.

SNMPv3 also allows remote configuration of security aspects without requiring the administrator to actually be at the place where the device is