Network Management: SNMP

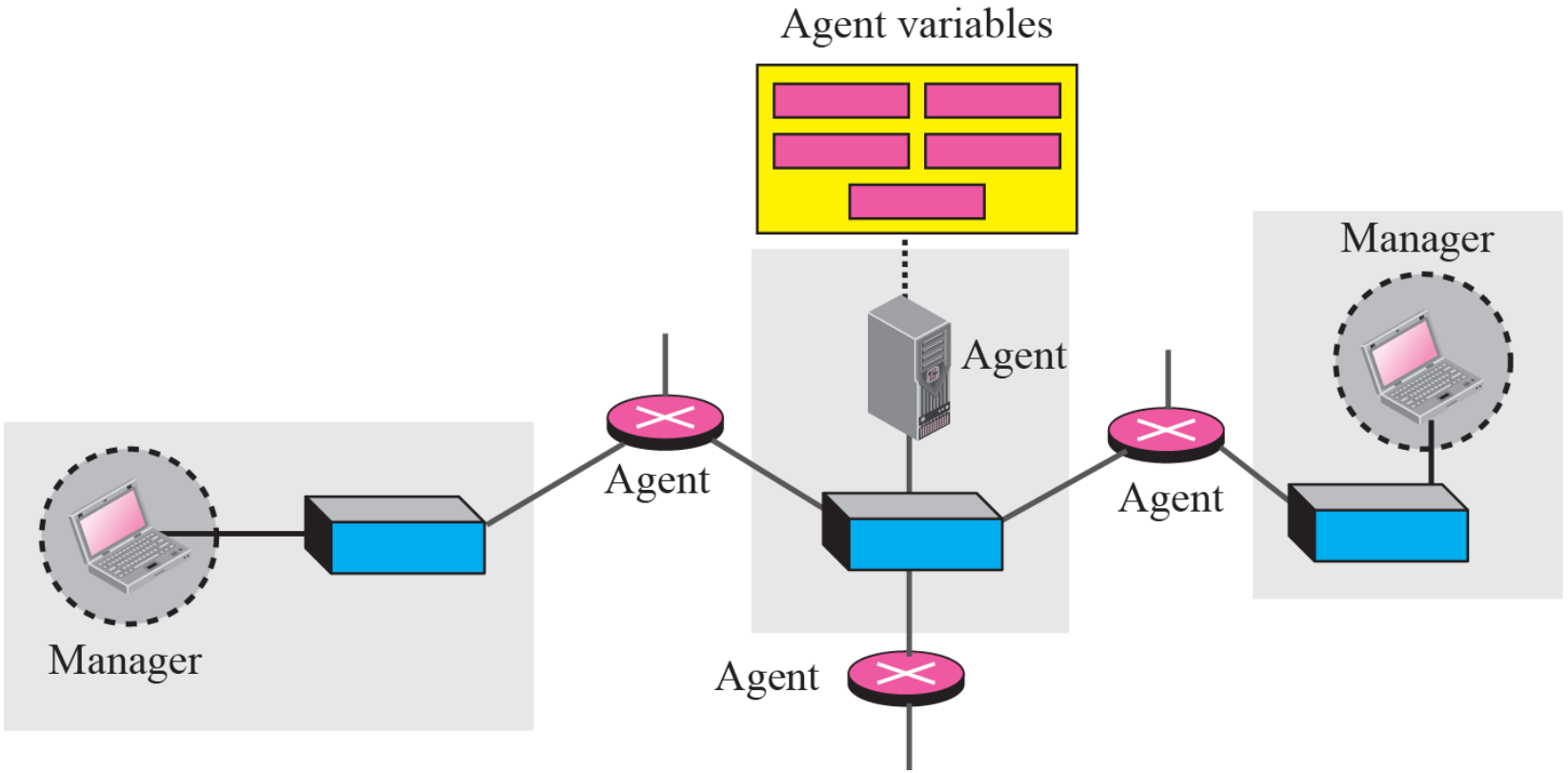
What is SNMP?

- UDP protocol, port 161
- Different versions
  - V1 (1988) – RFC1155, RFC1156, RFC1157
    - Original specification
  - v2 – RFC1901 … RFC1908 + RFC2578
    - Extends v1, new data types, better retrieval methods (GETBULK)
    - Used is version v2c (without security model)
  - v3 – RFC3411 … RFC3418 (w/security)
- Typically we use SNMPv2 (v2c)

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.

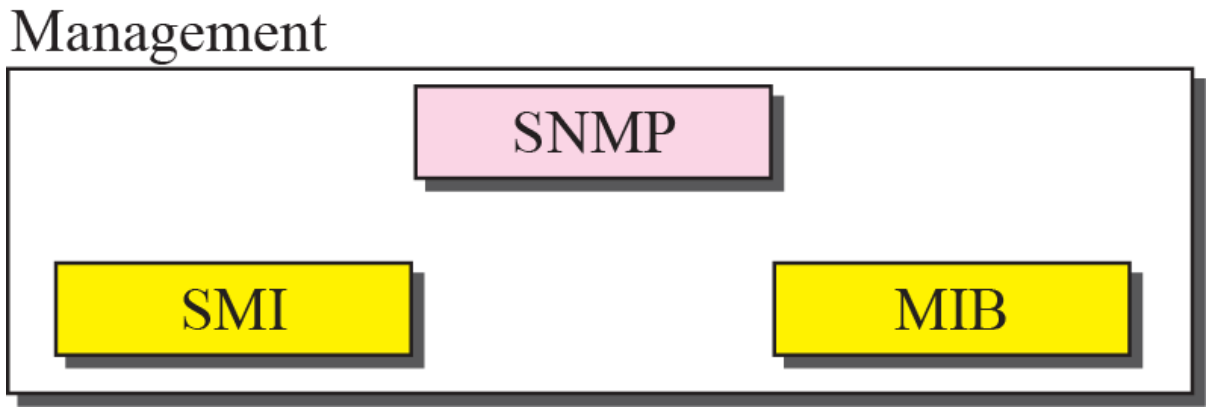
Figure 24.1 *SNMP concept*



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.

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*

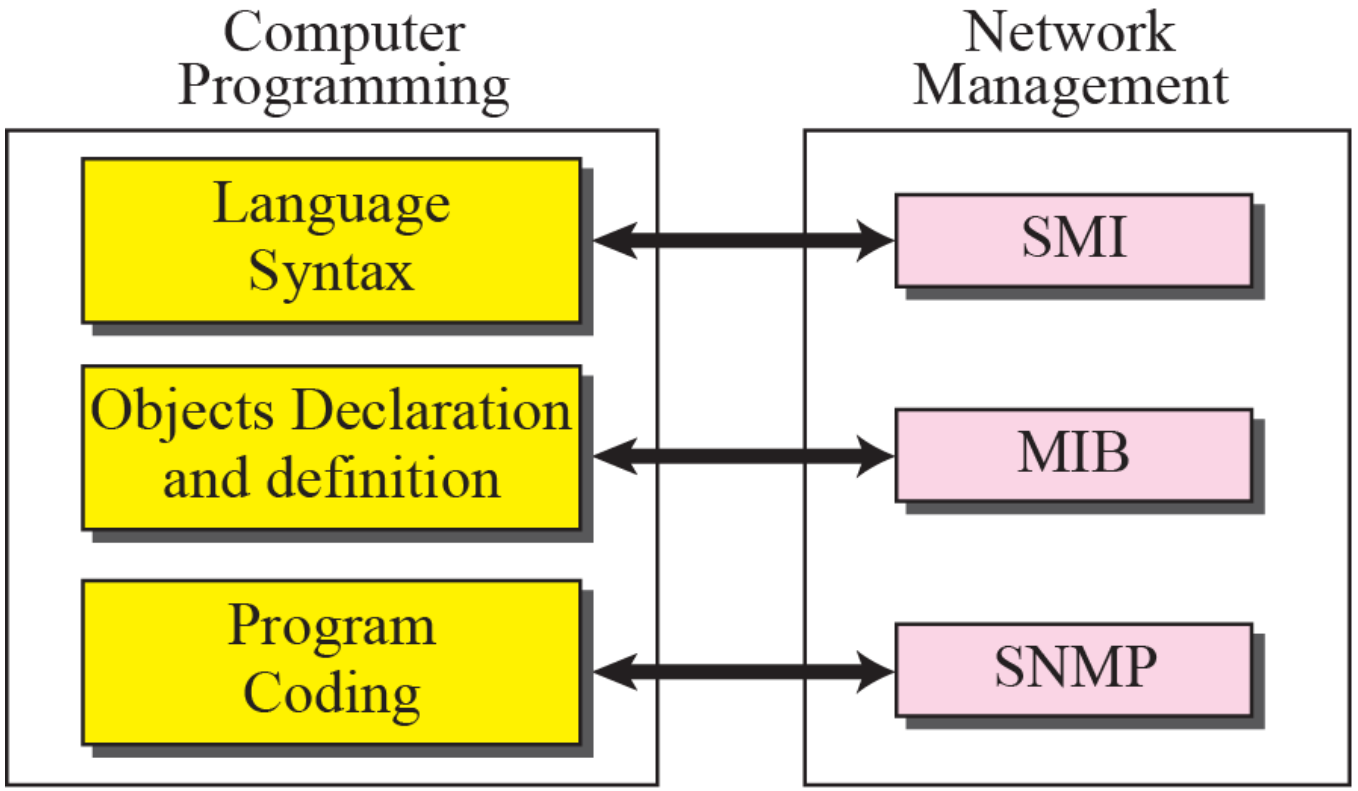
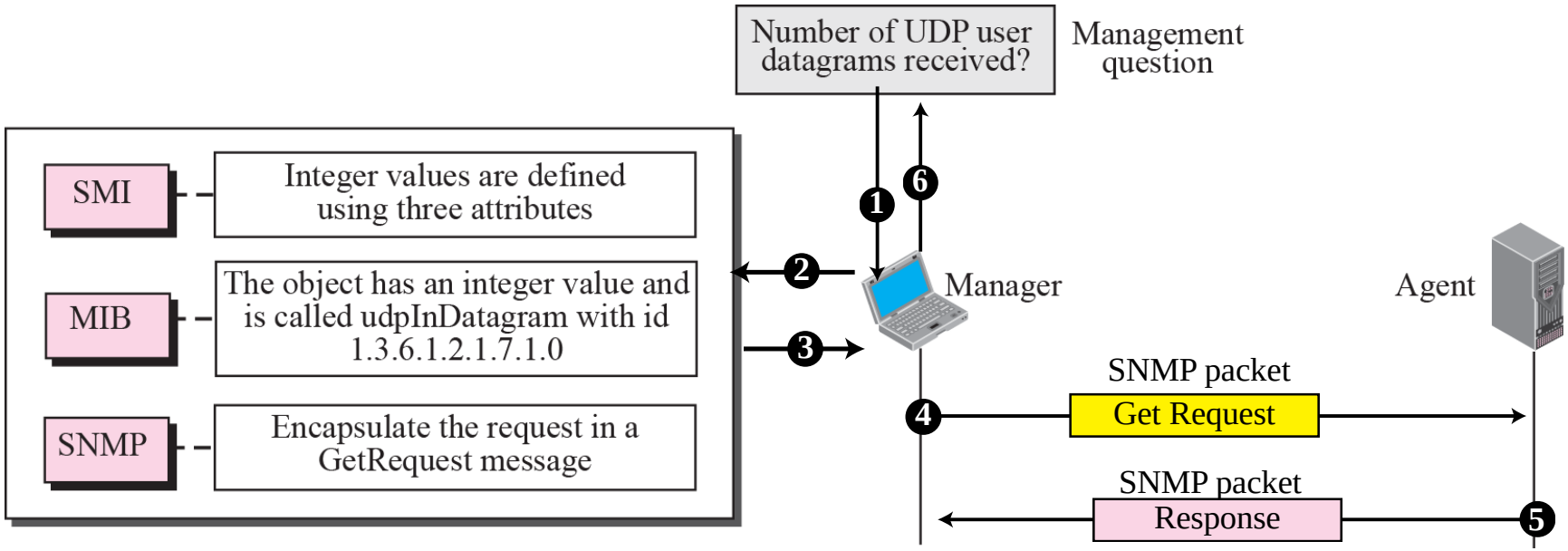


Figure 24.4 *Management overview*



MIBs - SAMPLE

```
sysUpTime OBJECT-TYPE
              SYNTAX  TimeTicks
              ACCESS  read-only
              STATUS  mandatory
              DESCRIPTION
                      "The time (in hundredths of a second) since the
                      network management portion of the system was last
                      re-initialized."
              ::= { system 3 }
```

`sysUpTime OBJECT-TYPE`
This defines the object called `sysUpTime`.

`SYNTAX TimeTicks`
This object is of the type `TimeTicks`. Object types are specified in the SMI we mentioned a moment ago.

`ACCESS read-only`
This object can only be read via SNMP (i.e., `get-request`); it cannot be changed (i.e., `set-request`).

`STATUS mandatory`
`This object must be implemented in any SNMP agent.`

`DESCRIPTION`
`A description of the object`

`::= { system 3 }`
The `sysUpTime` object is the third branch off of the system object group tree.

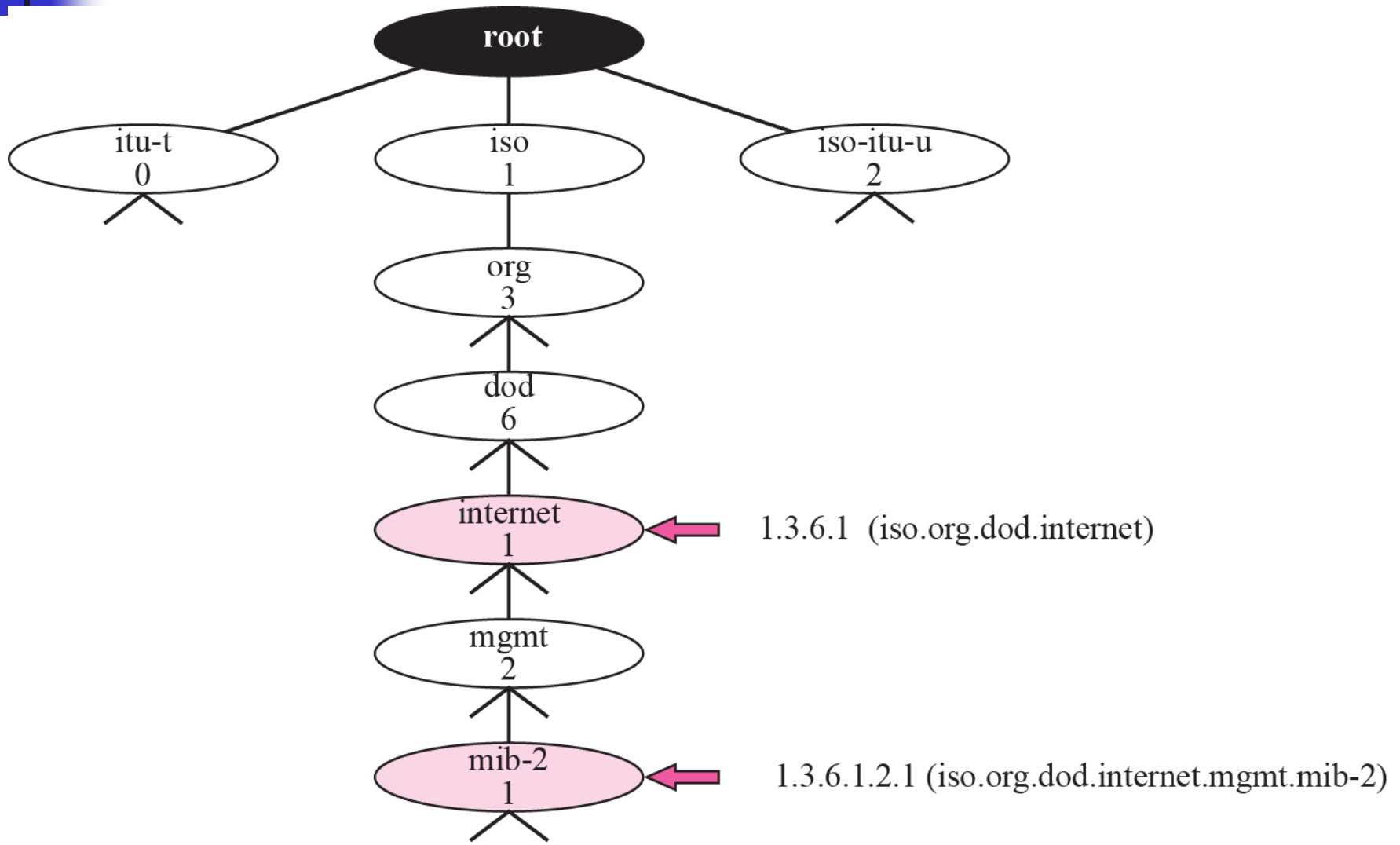
24-3 SMI

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.

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 24.7 *Encoding format*

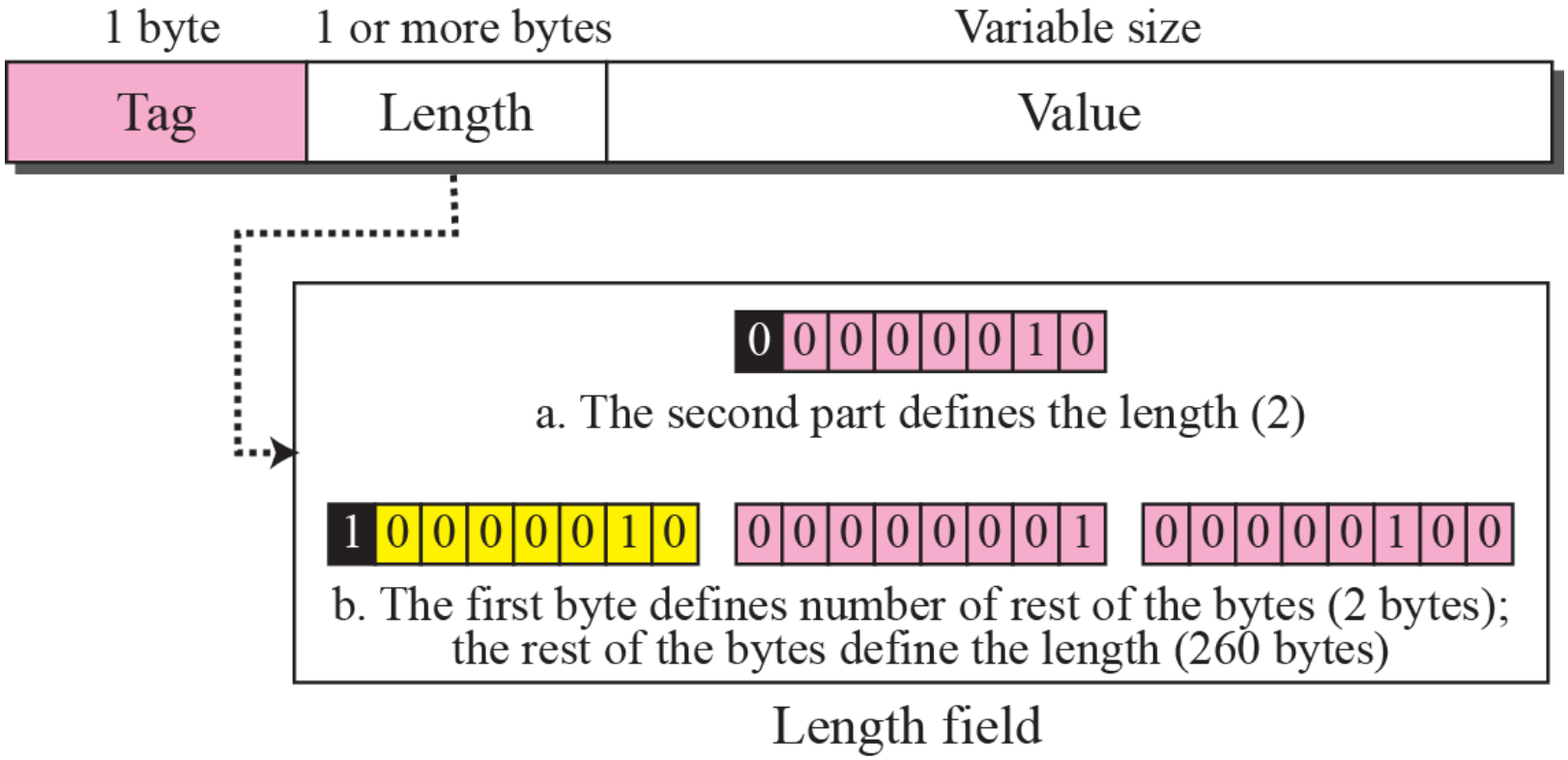


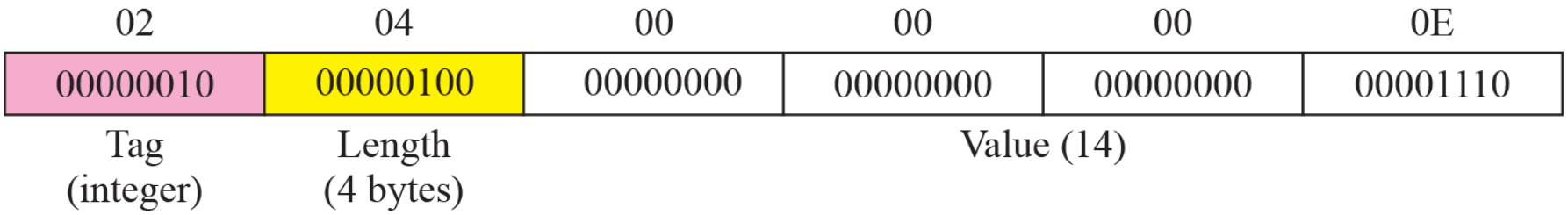
Table 24.2 *Codes for Data Types*

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.

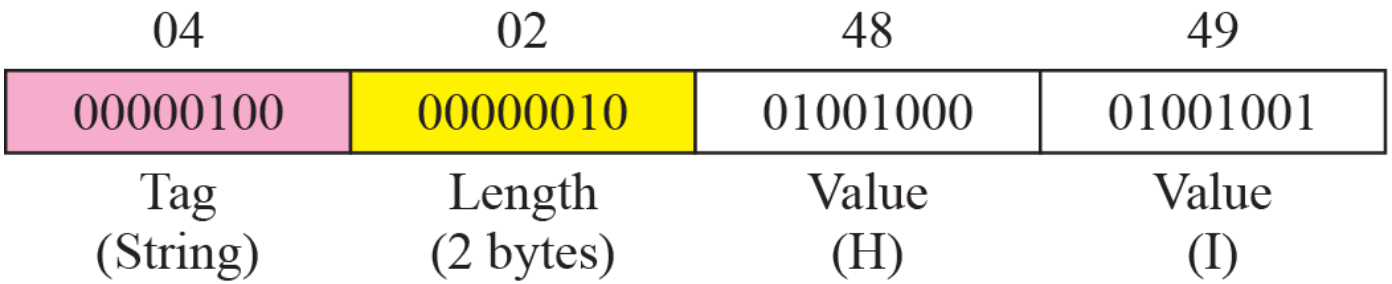
Figure 24.8 *Example 24.1: INTEGER 14*



Example 24.2

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

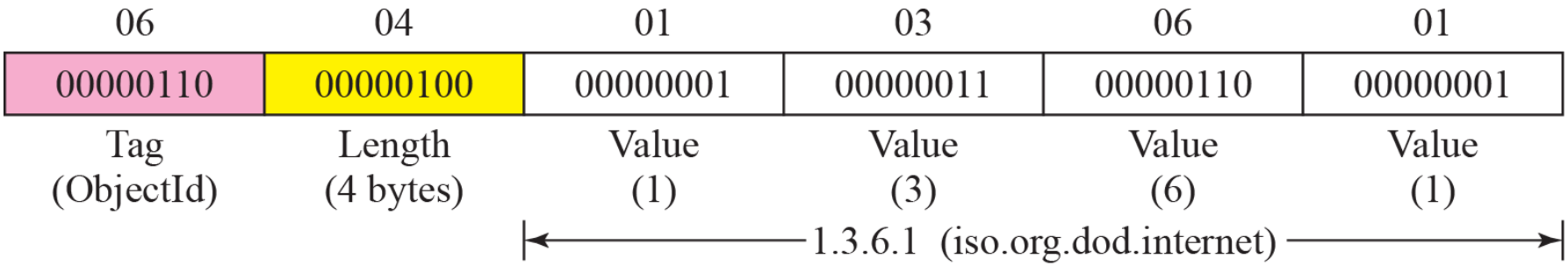
Figure 24.9 *Example 24.2: OCTET STRING "HI"*



Example 24.3

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

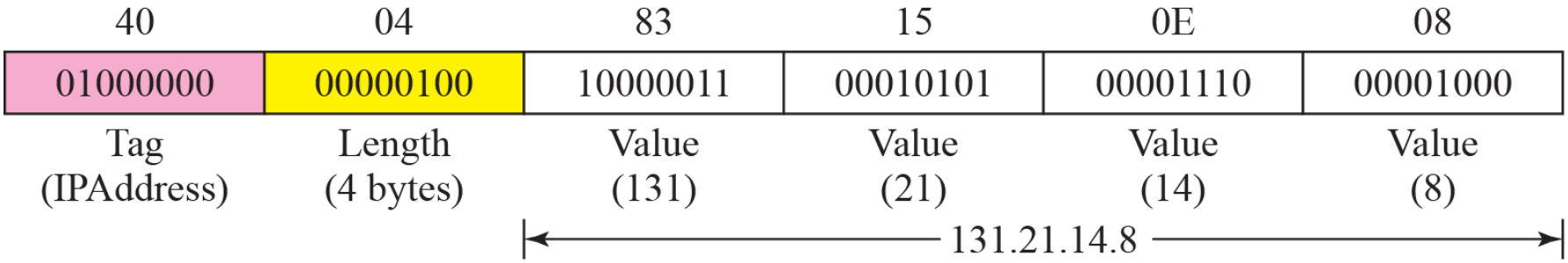
Figure 24.10 *Example 24.3: ObjectIndentifier 1.3.6.1*



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. Each group has defined variables and/or tables.

Figure 24.12 *mib-2*

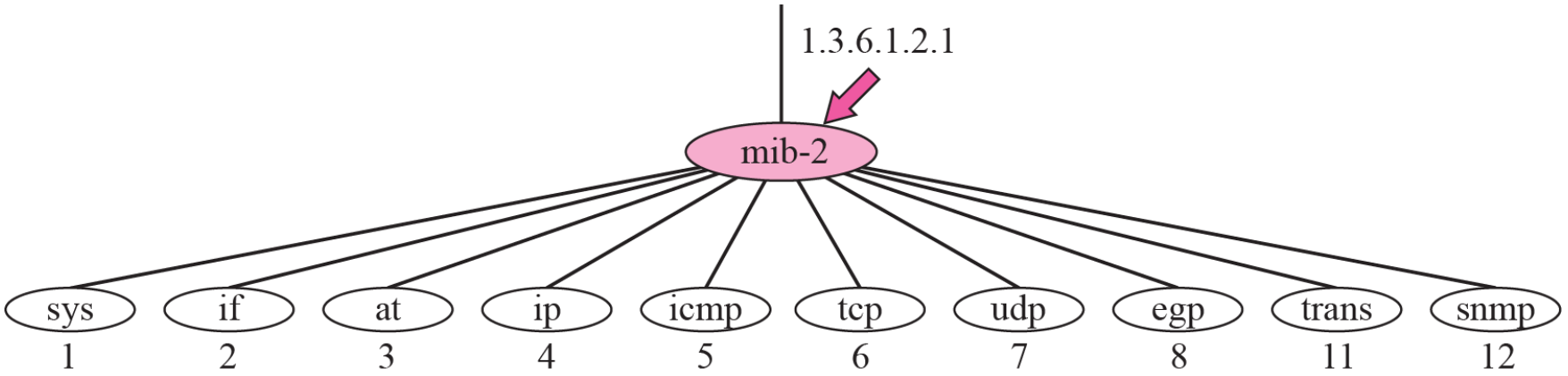
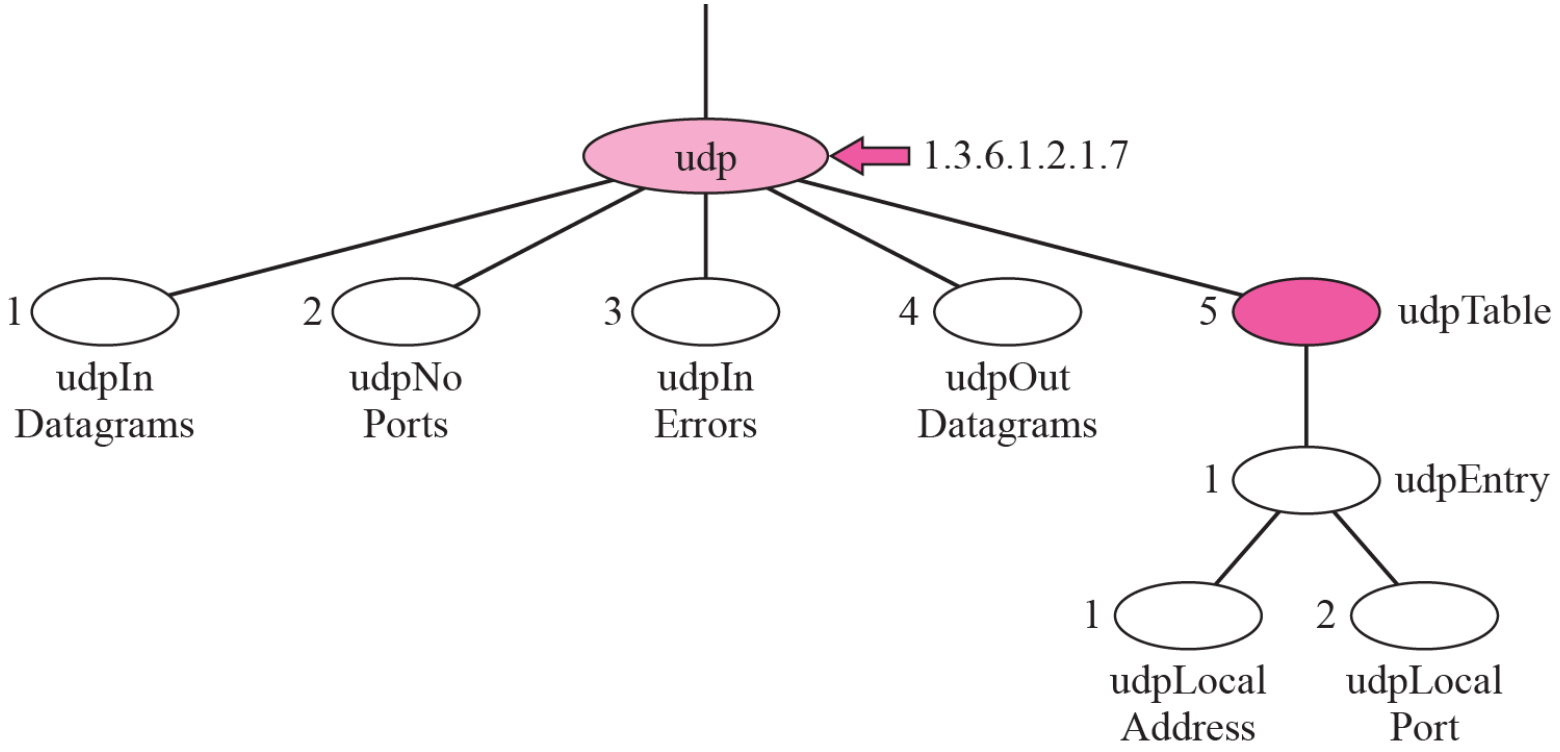


Figure 24.13 *udp group*



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.**

Figure 24.17 *SNMP PDUs*

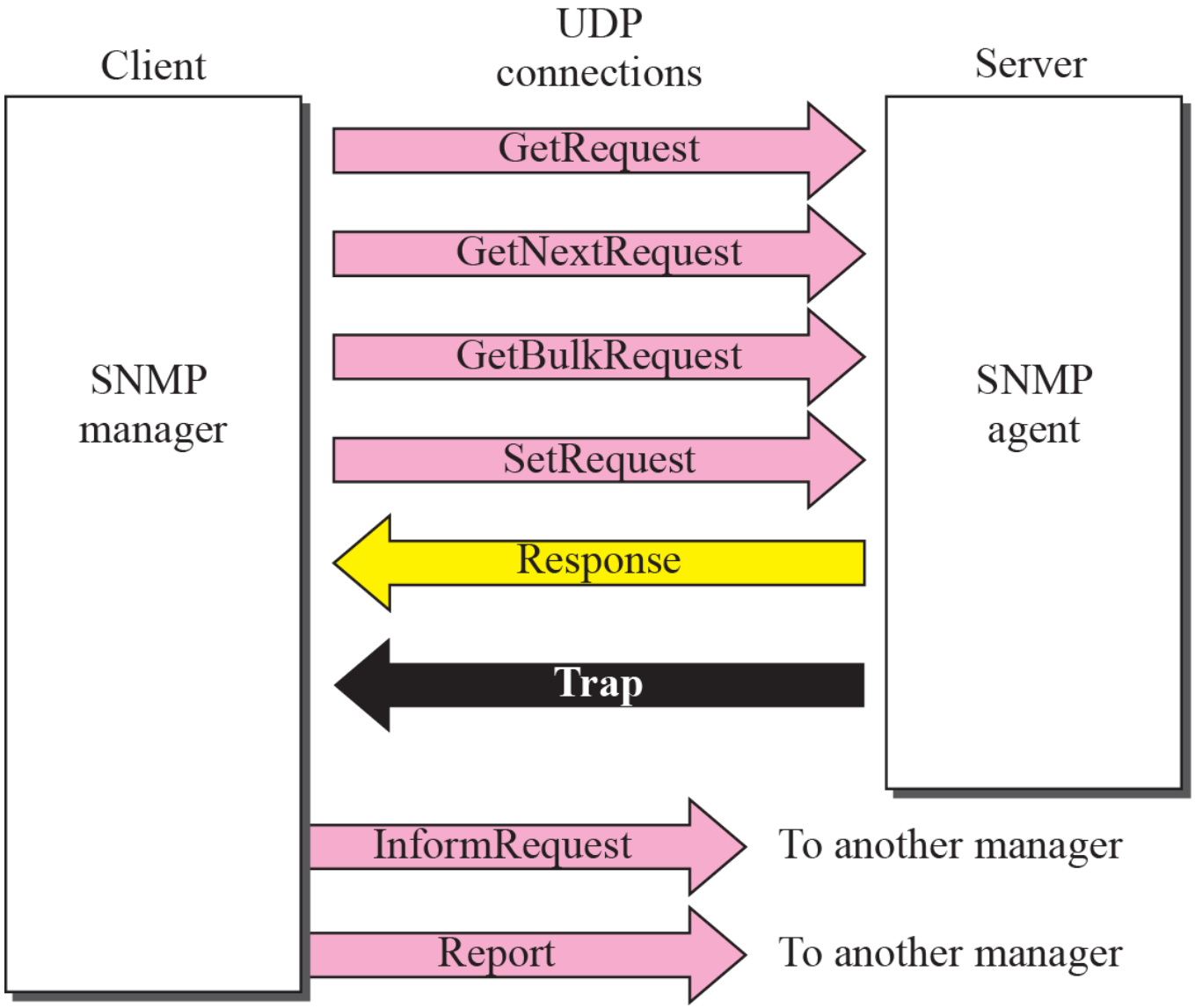
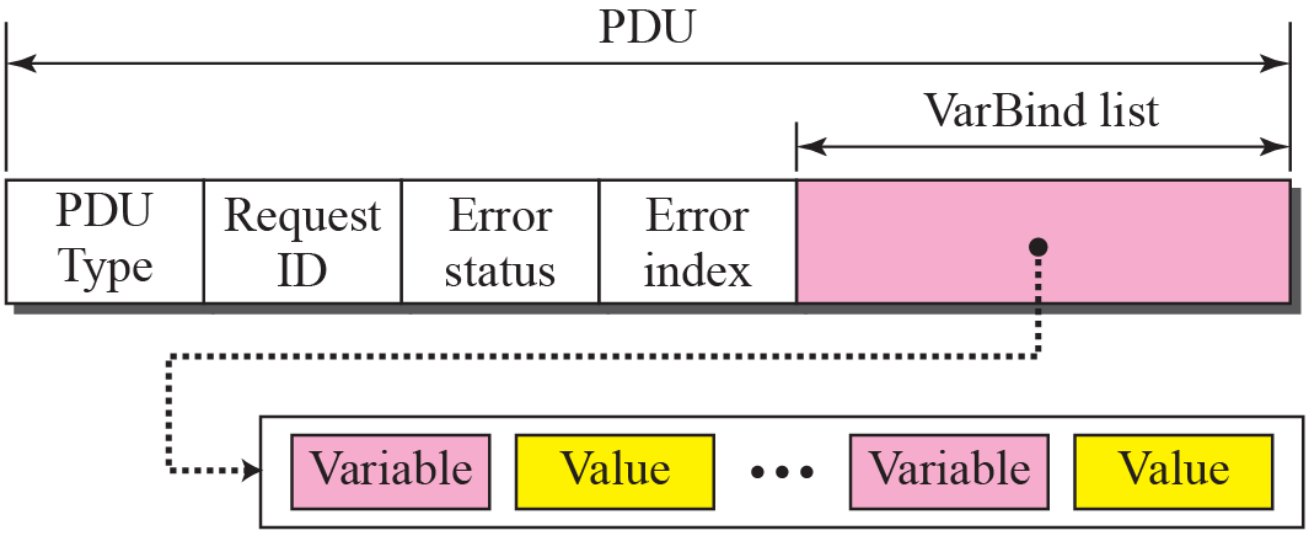


Figure 24.18 *SNMP PDU format*



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.

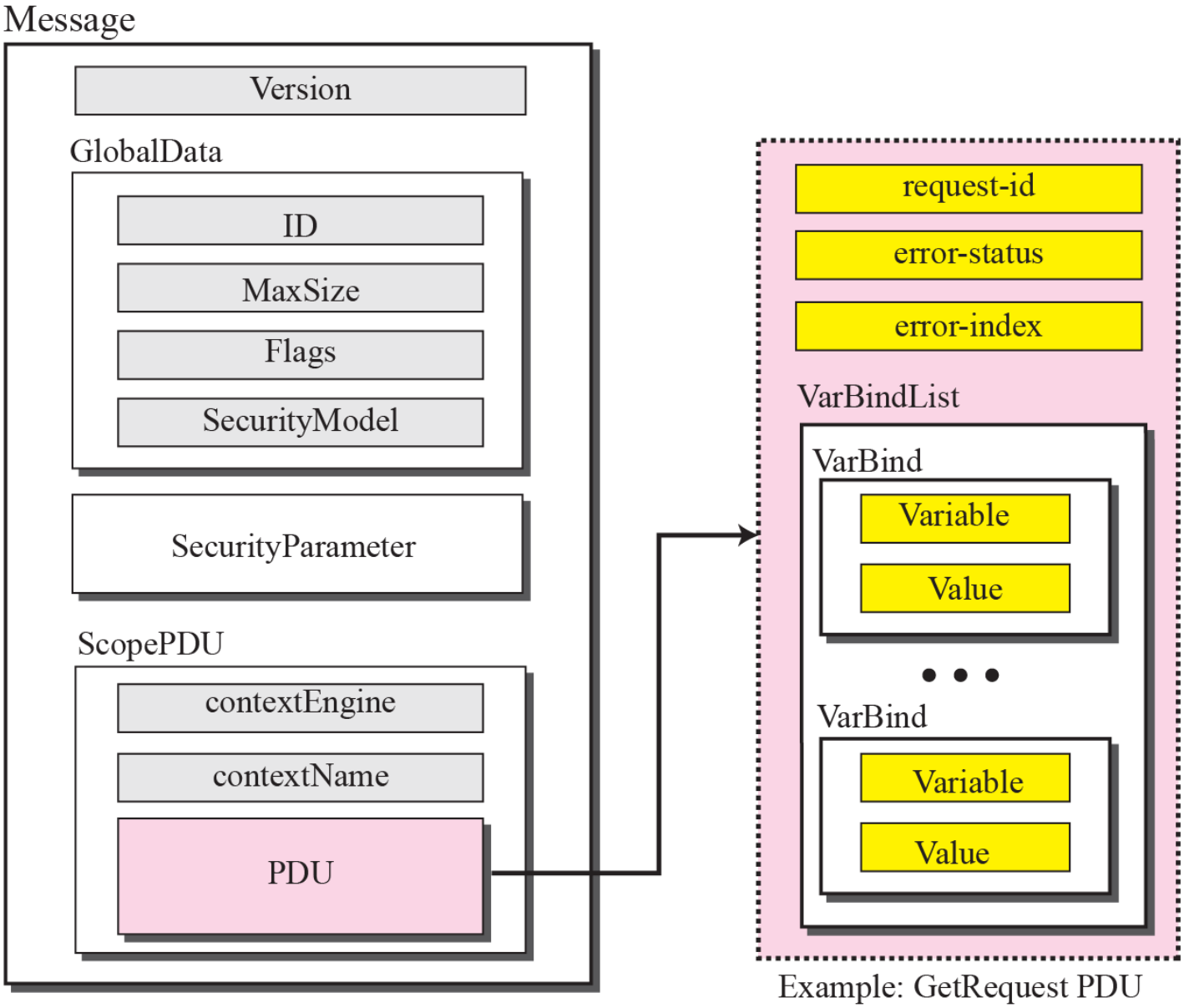
Table 24.3 *PDU Types*

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*



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).

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 located.