SNMP

SIMPLE NETWORK MANAGEMENT PROTOCOL

WHAT IS NETWORK MANAGEMENT?

Basic tasks that fall under this category are

- **Configuration management**
  - Keeping track of device settings and how they function
- **Fault Management**
  - Dealing with problems and emergencies in the network (router stops routing, server loss power etc..)
- **Performance Management**
  - How smoothly is the network running?
  - Can it handle the workload it currently has?
- **Network management interface must be standardized, extendible, and portable**
- **The management mechanism must be inexpensive and implemented as software only.**

FUNCTIONAL AREAS OF NETWORK MANAGEMENT

Configuration Management – inventory, configuration, provisioning

Fault Management – reactive and proactive network fault management

Performance Management – No. of packets dropped, timeouts, collisions, CRC errors

Security Management –controlling access to the network

Accounting Management – cost management and chargeback assessment

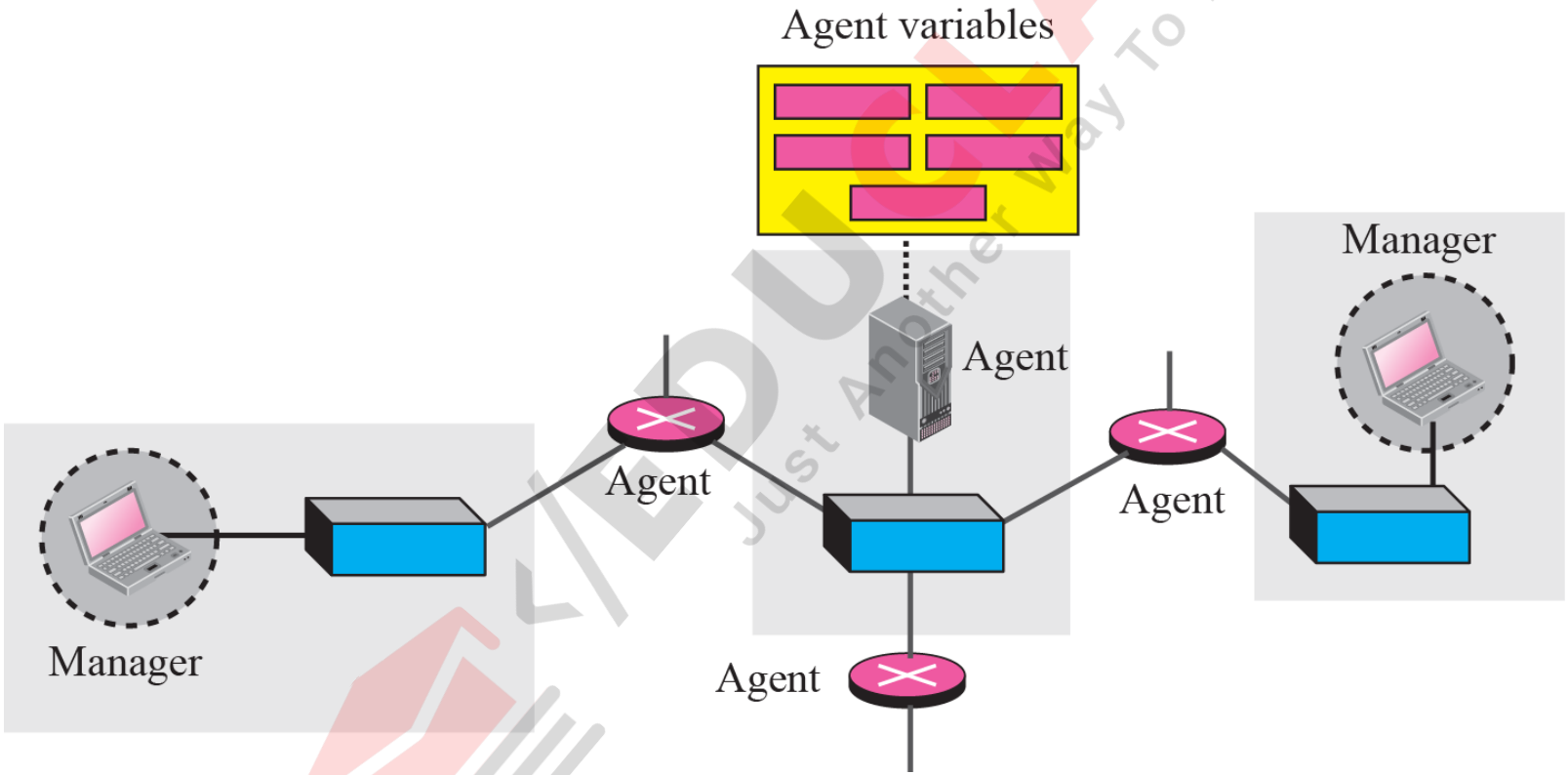
Asset Management – Statistics of equipment, facility and administration personnel

Planning Management – Analysis of trends to help justify a network upgrade or bandwidth increase

WHAT IS SNMP?

- **SNMP is a tool (protocol) that allows for remote and local management of items on the network including servers, workstations, routers, switches and other managed devices**
- **Comprised of agents and managers**
  - Agent – process running on each managed node collecting information about the device it is running on
  - Manager – process running on a management workstation that requests information about devices on the network.

SNMP CONCEPT



CLIENT PULL & SERVER PUSH

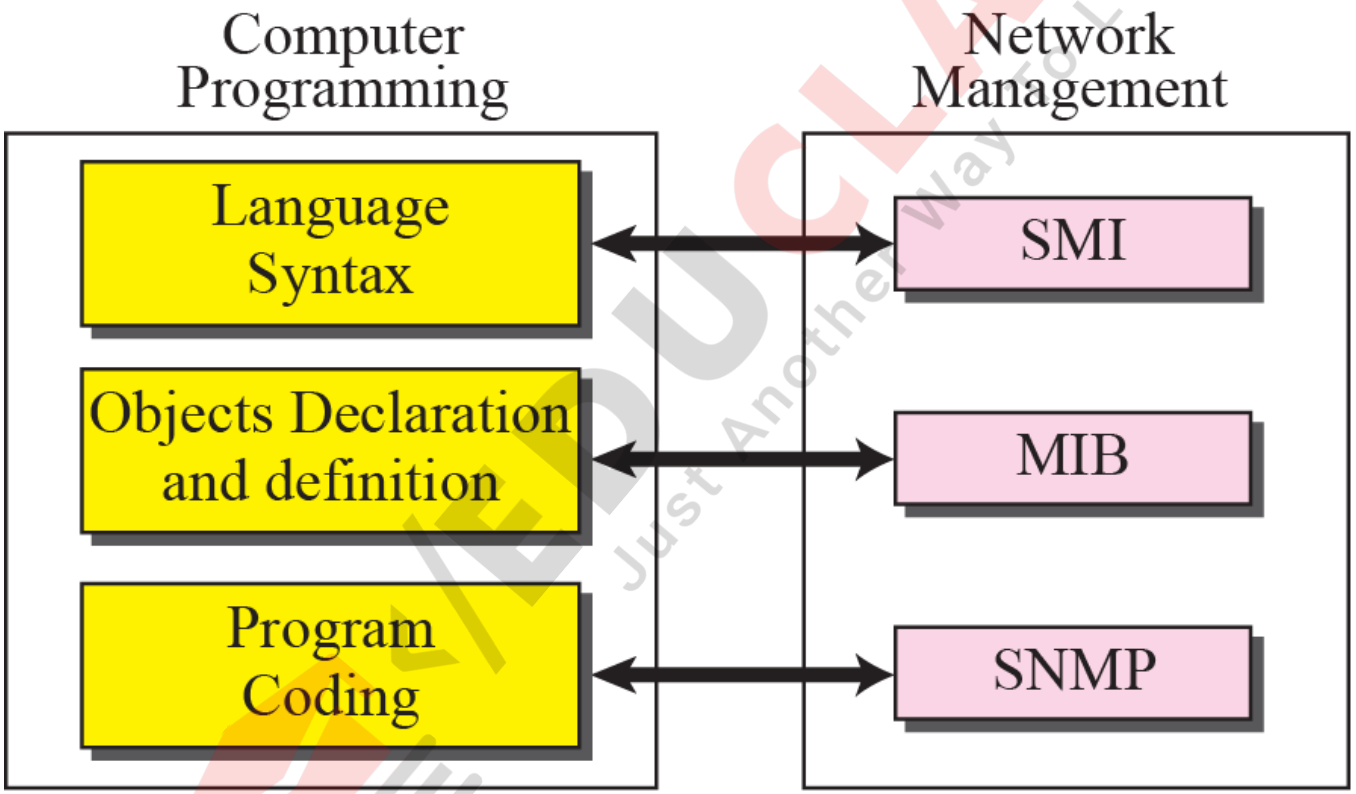
- **SNMP is a “client pull” model**
  - The management system (client) “pulls” data from the agent (server)

- **SNMP is a “server push” model**
  - The agent (server) “pushes” out a trap message to a (client) management system

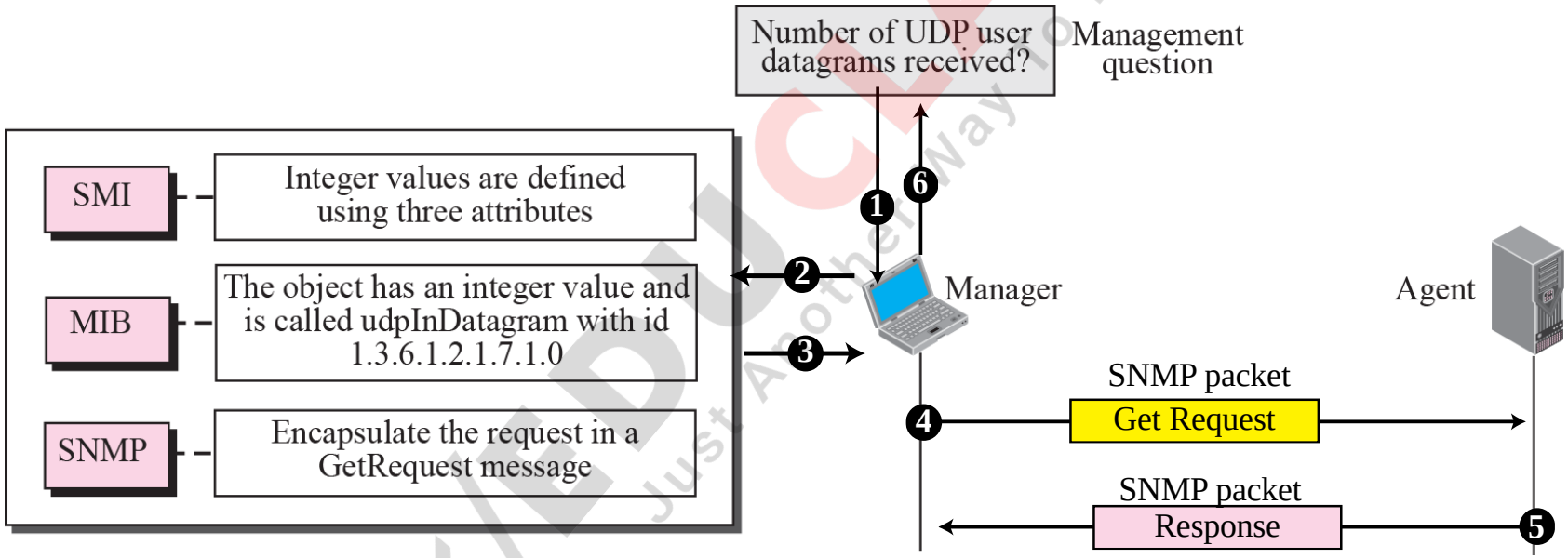
COMPONENTS OF SNMP

- **SNMP network management is based on three parts**
  - SNMP Protocol
    - Defines format of messages exchanged between agents and managers
    - It reads and changes the status of objects in SNMP packets
  - Structure of Management Information (SMI)
    - Rules specifying the format used to define objects managed on the network that the SNMP protocol accesses
  - Management Information Base (MIB)
    - A map of the hierarchical order of all managed objects and how they are accessed

COMPARISON – PROGRAMMING VS NETWORK MANAGEMENT



EXAMPLE



LANGUAGES OF SNMP

- **SMI**
  - Specifies the format for defining managed objects that are accessed via the SNMP protocol
- **Abstract Syntax Notation One (ASN.1)**
  - Used to define the format of SNMP messages and managed objects using an unambiguous data description format
- **Basic Encoding Rules (BER)**
  - Used to encode the SNMP messages into a format suitable for transmission across a network

SMI

- **The functions of SMI are**
  - To name objects
  - To define the type of data that can be stored in an object
  - To show how to encode data for transmission over the network

OBJECT IDENTIFIER

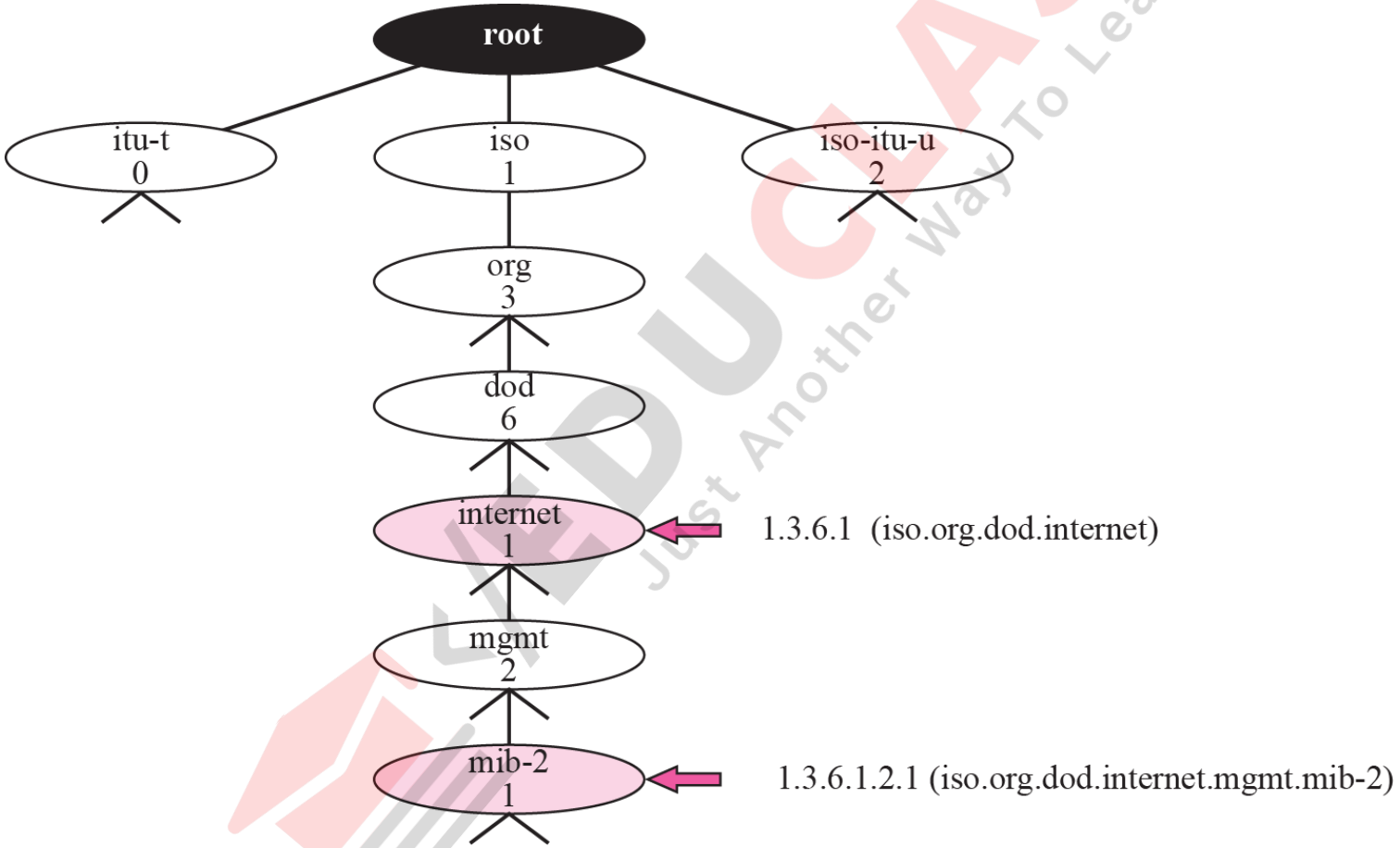
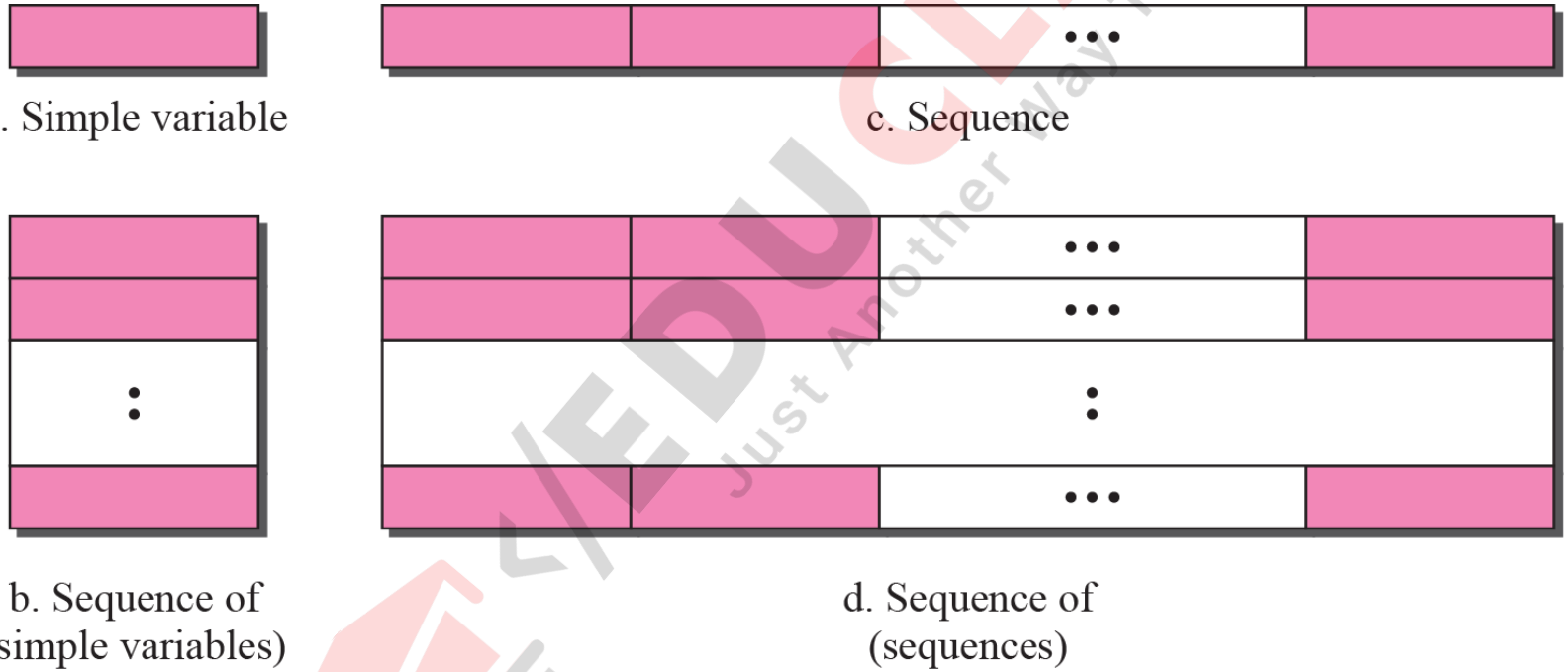


Table 24.1 *Data Types*

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

CONCEPTUAL DATA TYPES



a. Simple variable

c. Sequence

b. Sequence of (simple variables)

d. Sequence of (sequences)

ENCODING FORMAT

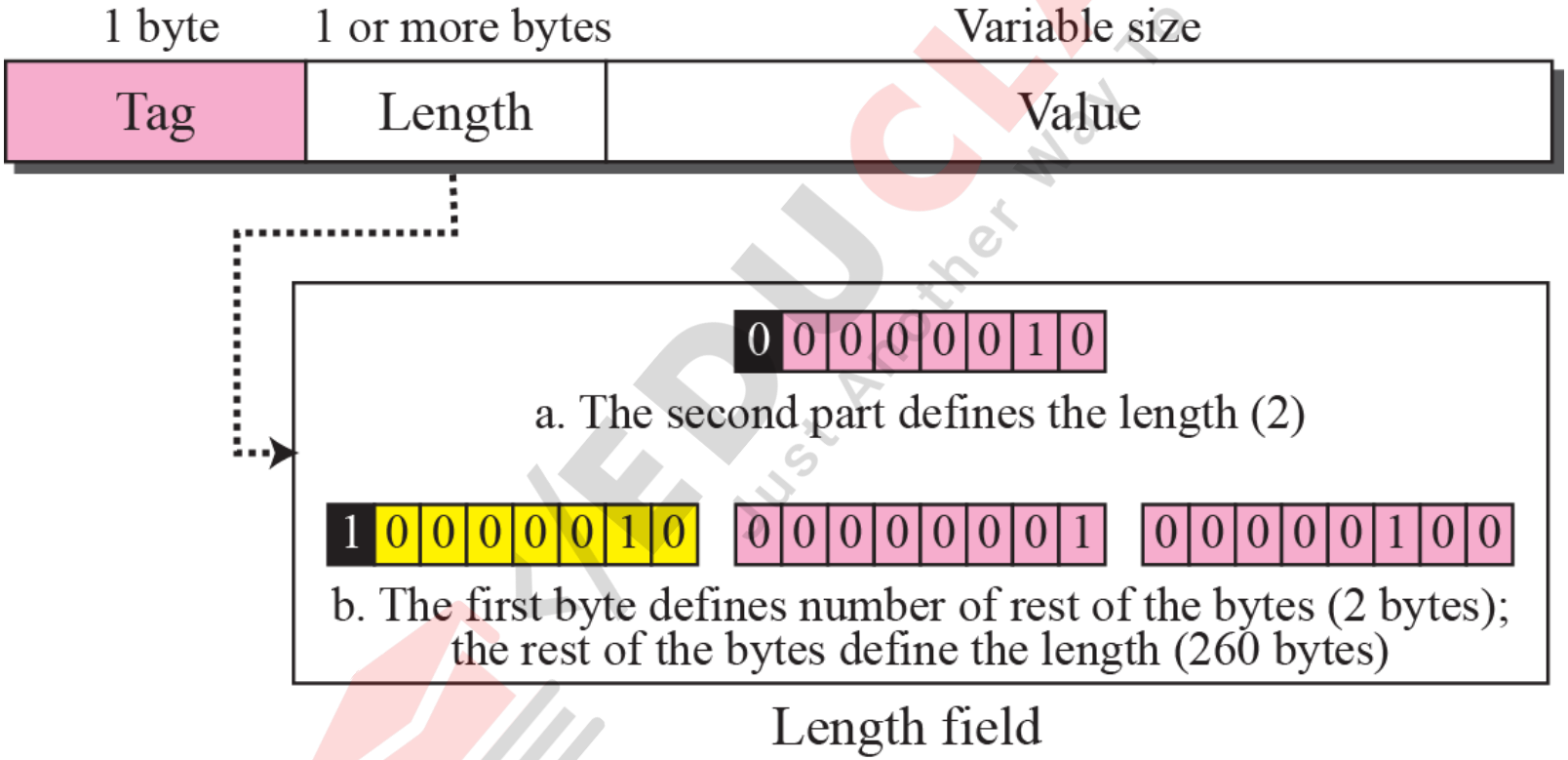
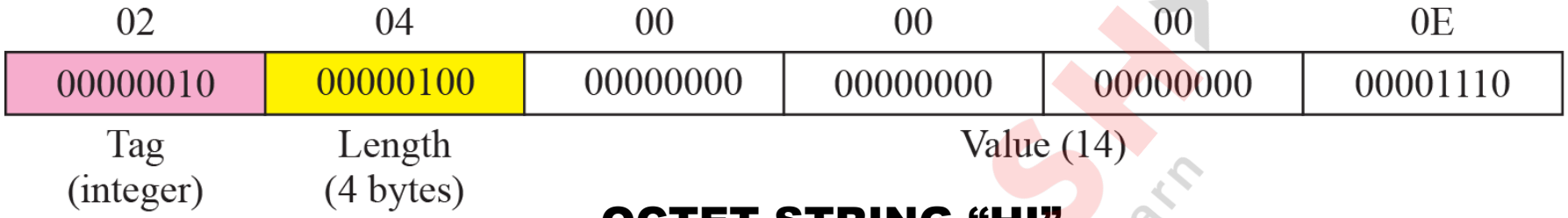


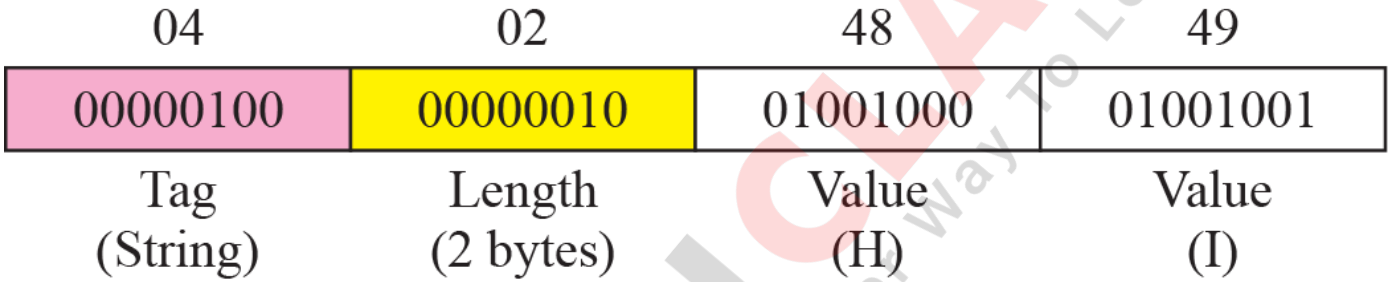
Table 24.2 *Codes for Data Types*

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**

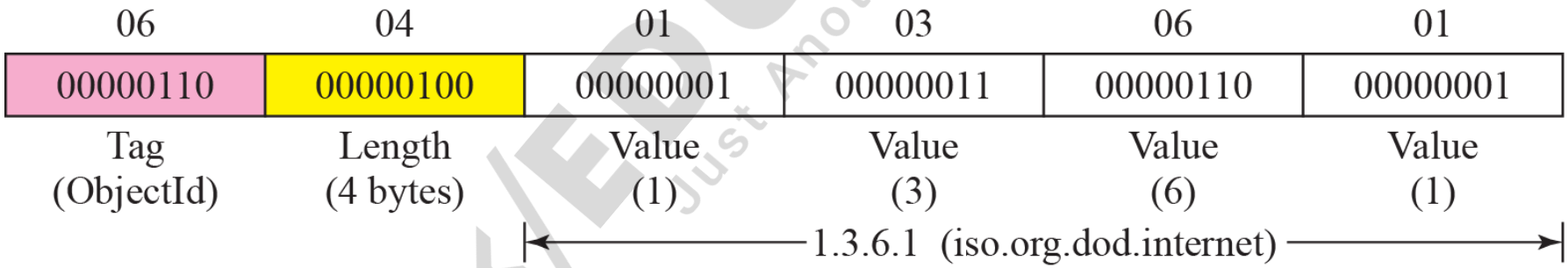
INTEGER 14



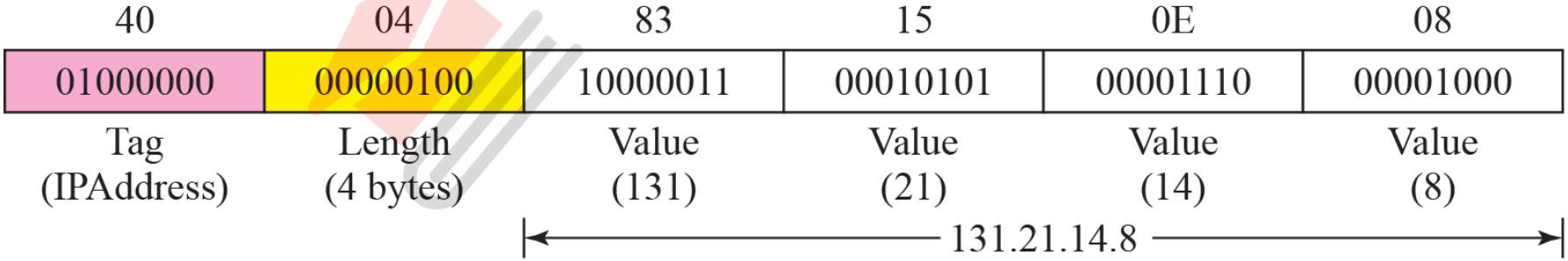
OCTET STRING "HI"



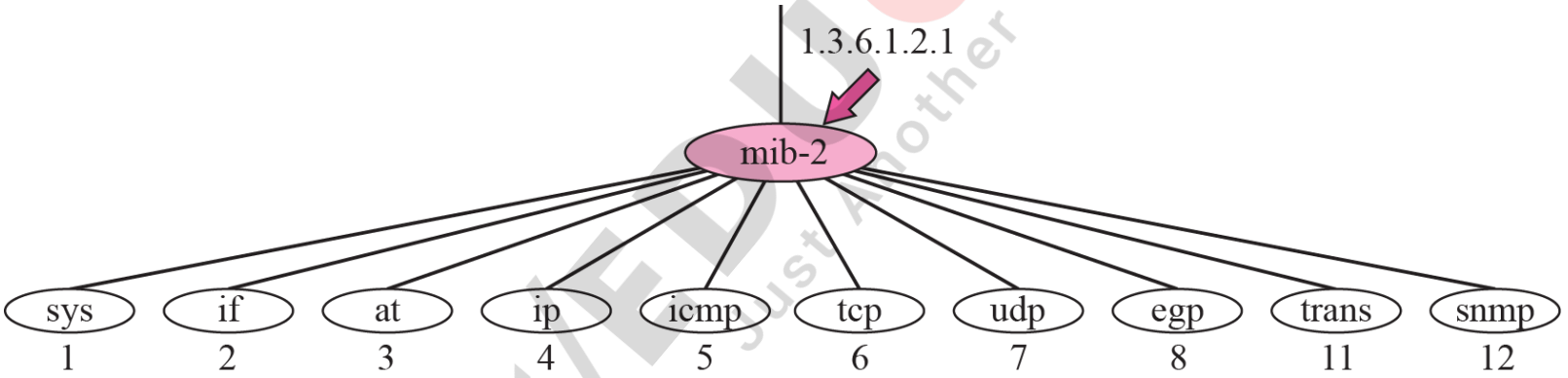
Object Identifier 1.3.6.1



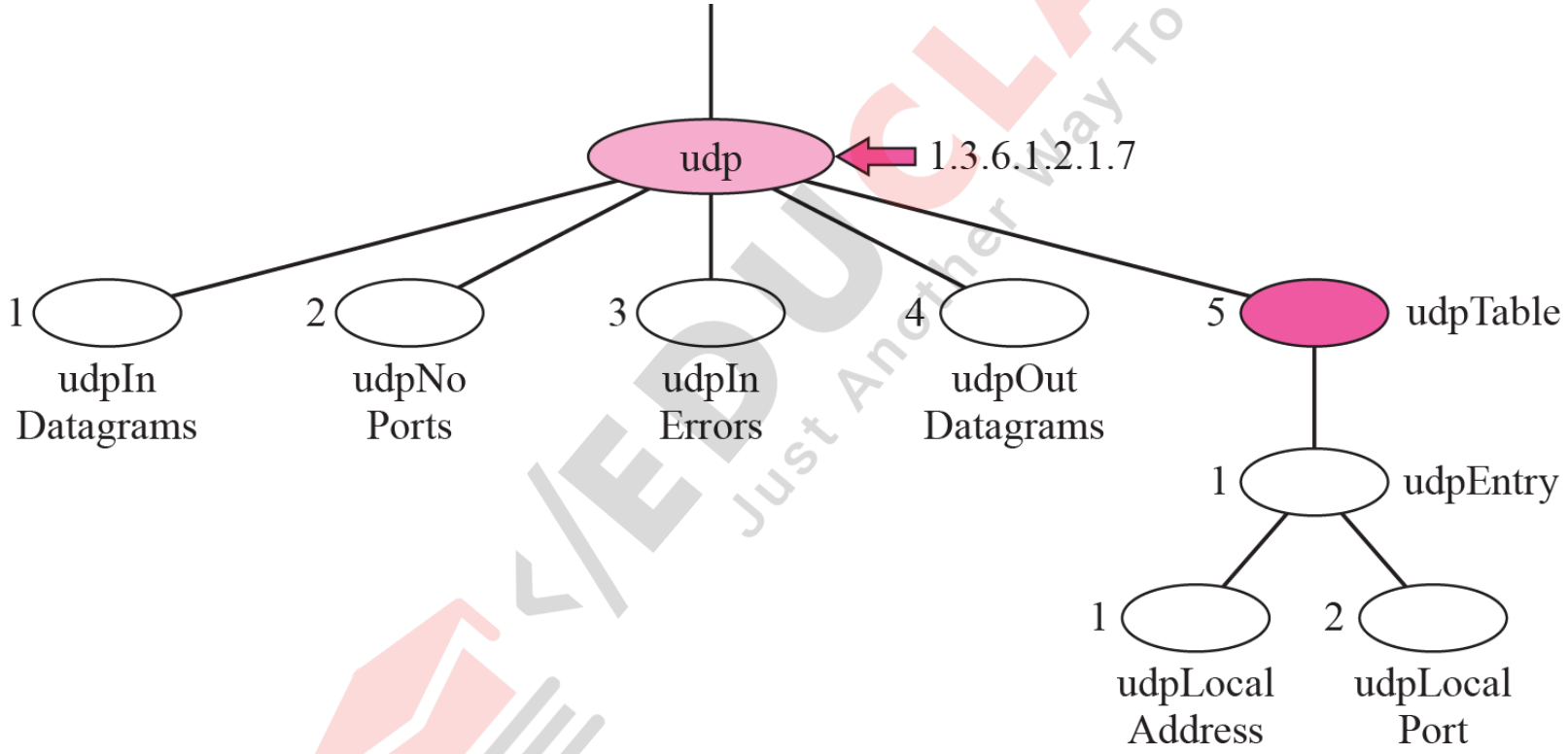
IPAddress 131.21.14.8



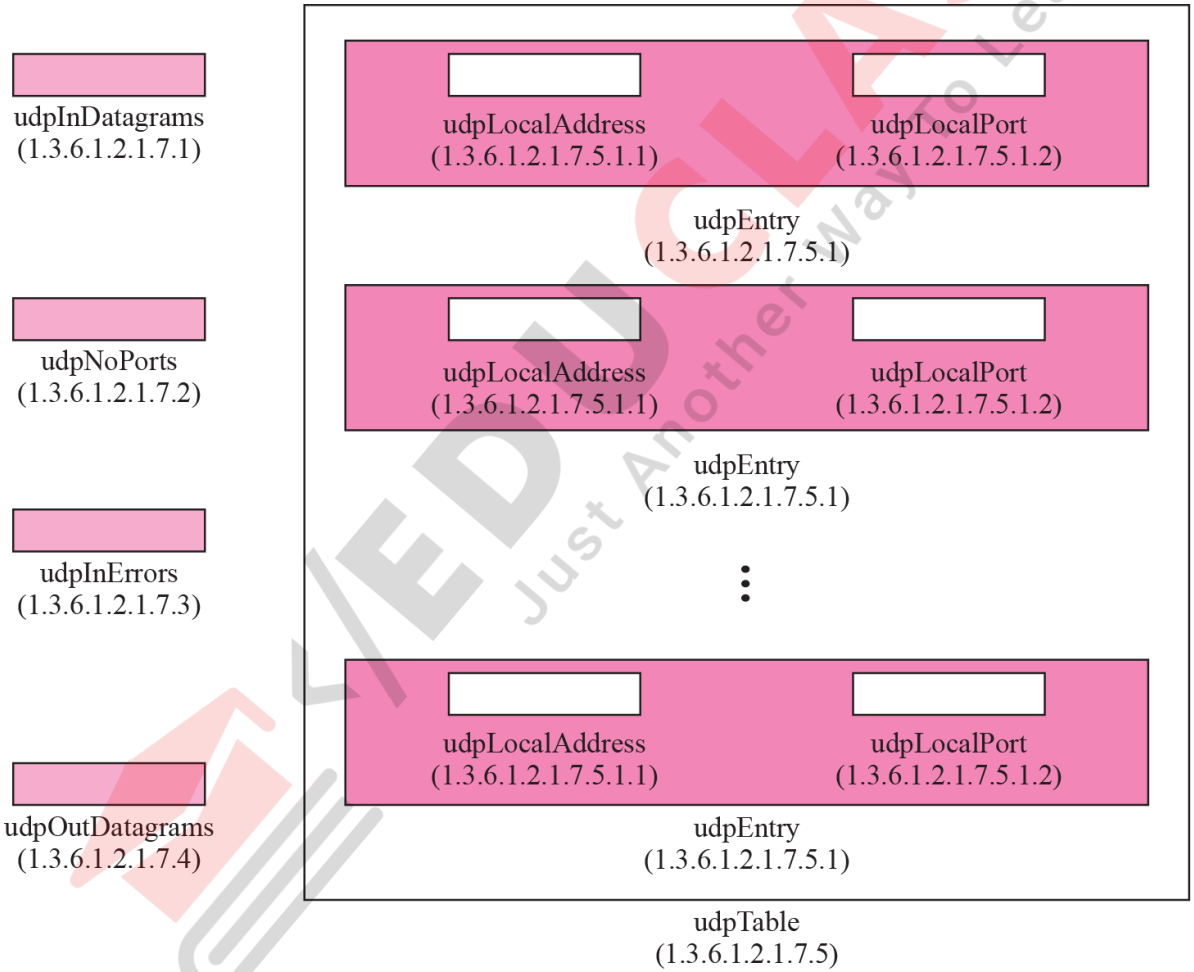
MIB-2


1.3.6.1.2.1
mib-2
sys
1
if
2
at
3
ip
4
icmp
5
tcp
6
udp
7
egp
8
trans
11
snmp
12

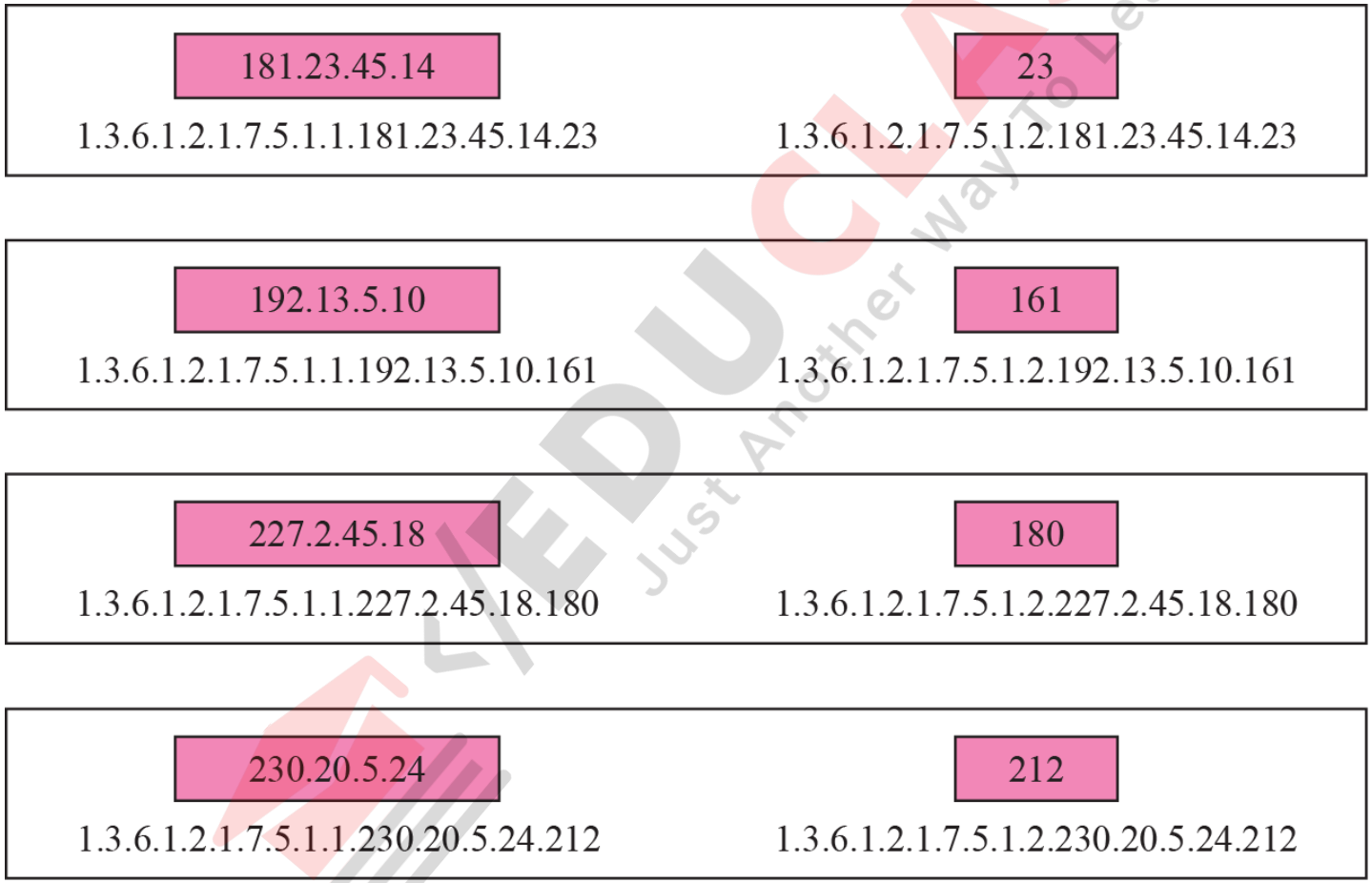
UDP GROUP



UDP VARIABLES AND TABLES



INDEXES FOR UDPTABLE



SNMP

- **SNMP uses both SMI and MIB in network management. It is an application program that allows**
  - A manager to retrieve the value of an object defined in an agent
  - A manager to store a value in an object defined in an agent
  - An agent to send an alarm message about an abnormal situation to the manager.

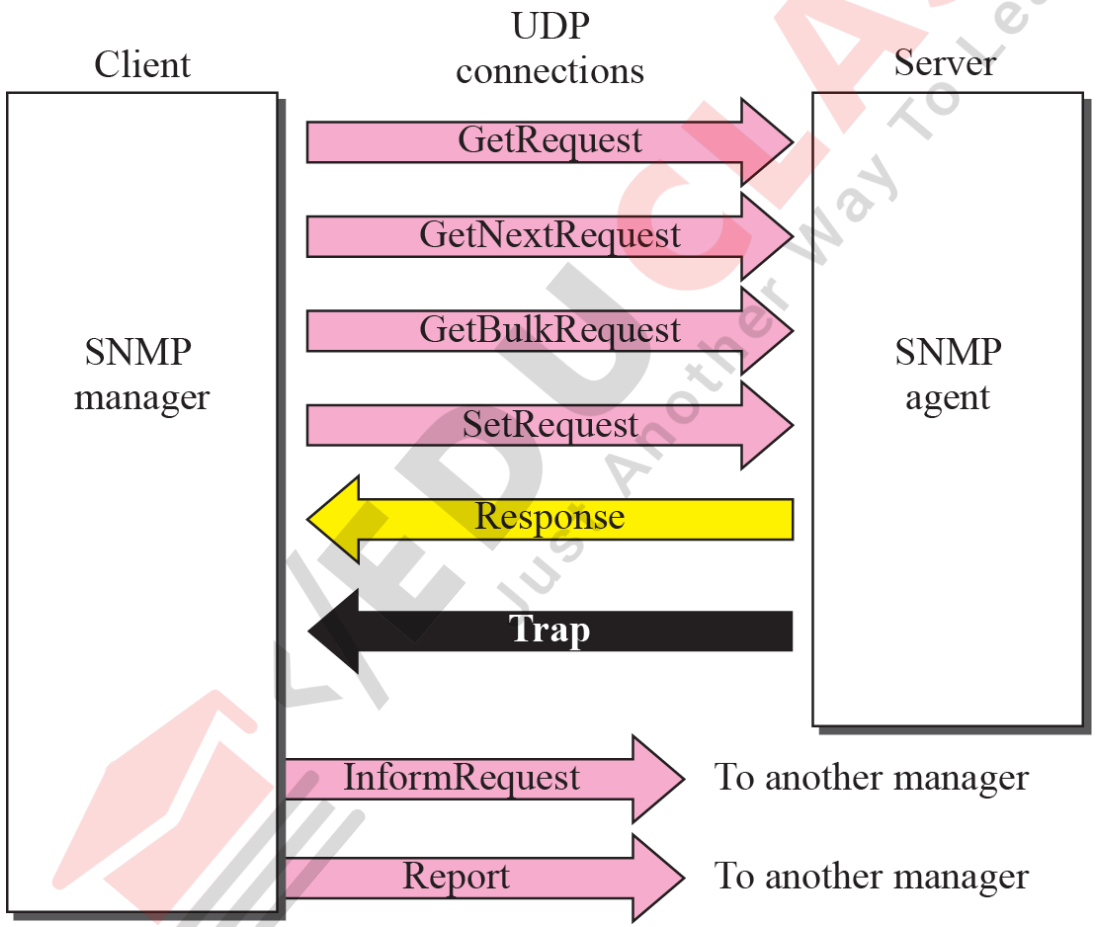
BASIC OPERATIONS

- **Get**
  - Retrieves the value of MIB variable stored on the agent machine
- **GetNext**
  - Retrieves the next value of the next lexical MIB variable
- **Set**
  - Changes the value of a MIB variable
- **Trap**
  - An unsolicited notification sent by an agent to a management application

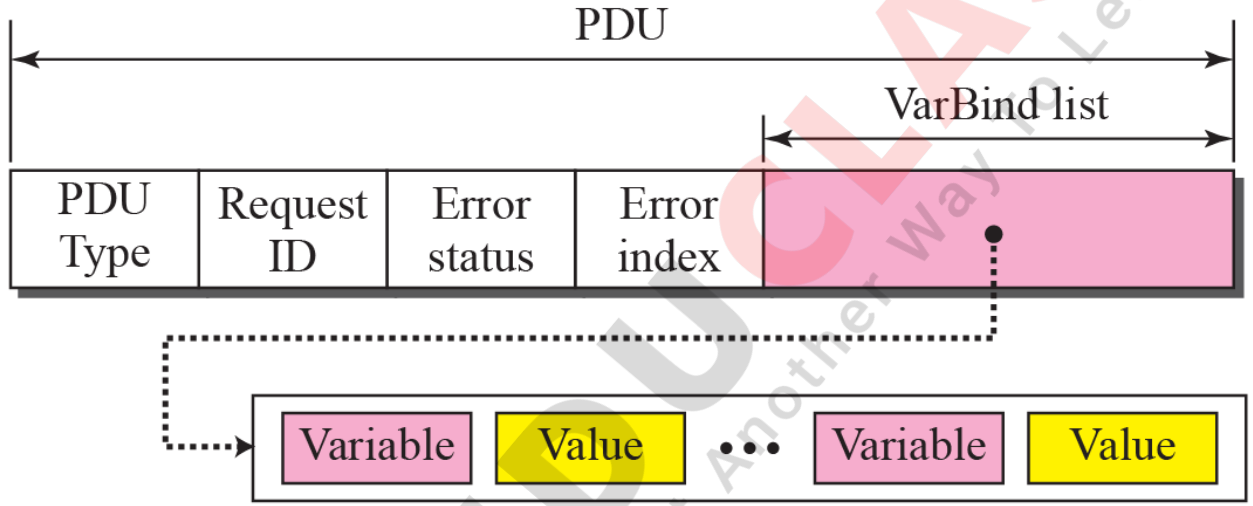
TRAPS

- Traps are unrequested event reports that are sent to a management system by an SNMP agent process
- When a trappable event occurs, a trap message is generated by the agent and is sent to a trap destination (a specific, configured network address)
- Many events can be configured to signal a trap, like a network cable fault, failing NIC or Hard Drive, a “General Protection Fault”, or a power supply failure
- Traps can also be throttled -- You can limit the number of traps sent per second from the agent
- Traps have a priority associated with them -- Critical, Major, Minor, Warning, Marginal, Informational, Normal, Unknown

SNMP PDUS


Client
UDP connections
Server
SNMP manager
SNMP agent
GetRequest
GetNextRequest
GetBulkRequest
SetRequest
Response
Trap
InformRequest
To another manager
Report
To another manager

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.

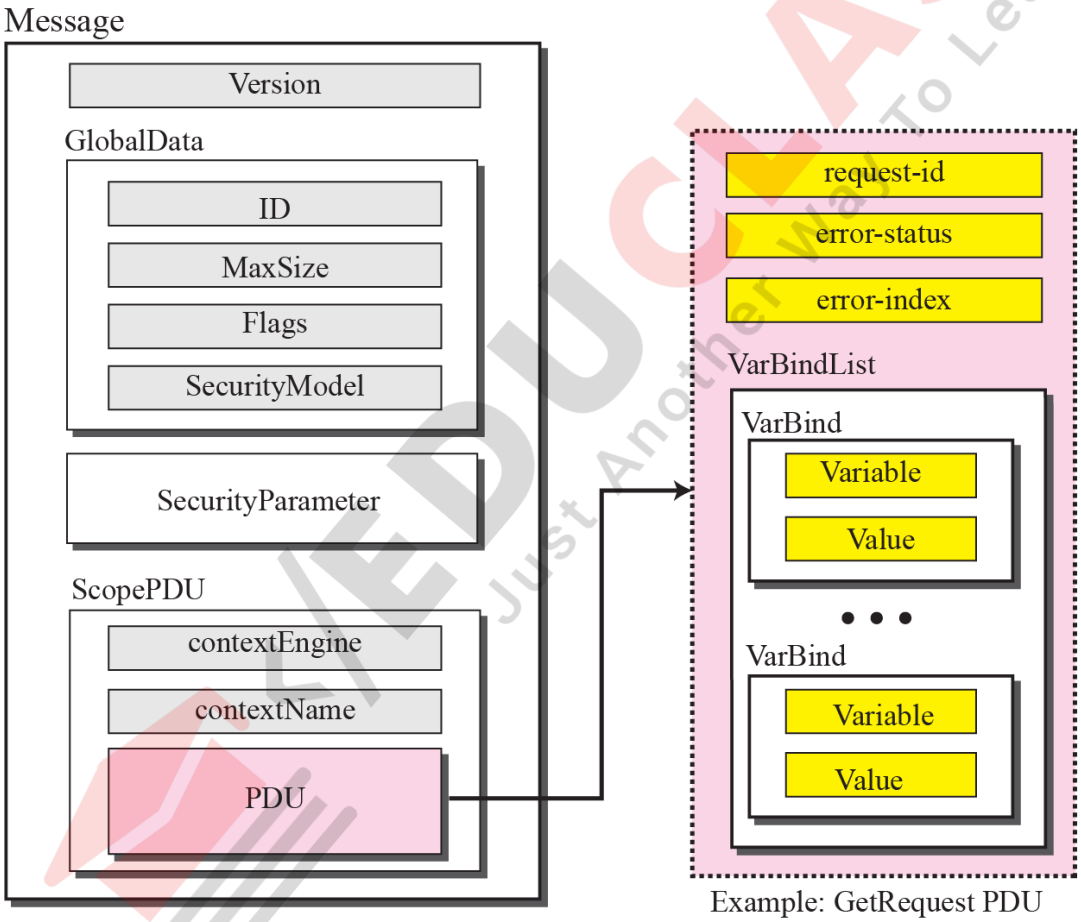
Table 24.3 *PDU Types*

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

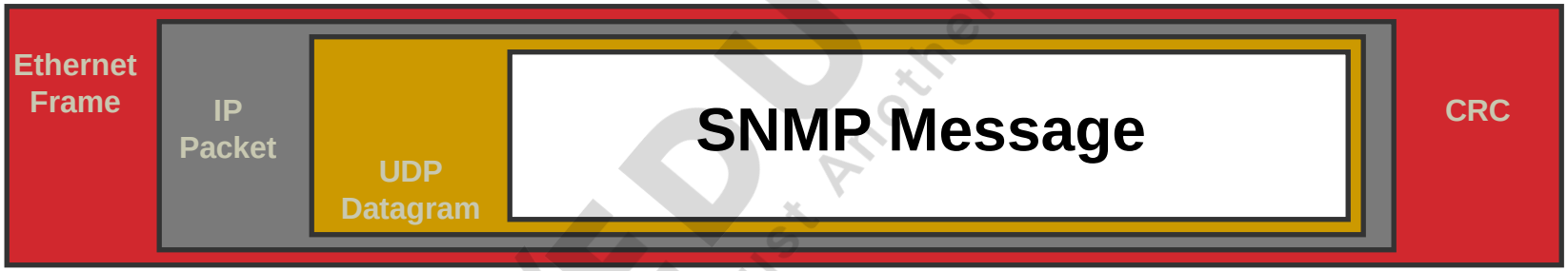
SNMP MESSAGE



Example: GetRequest PDU

PORTS & UDP

- **SNMP uses User Datagram Protocol (UDP) as the transport mechanism for SNMP messages**



- **It uses two well-knows ports**
  - Port 161 – SNMP messages
  - Port 162 – SNMP Trap Messages

PORT NUMBERS FOR SNMP