NETWORKS, PROTOCOLS & SECURITY (DNPS)
23EC2210 R/A/E

TOPIC:
SNMP

Session-30

AIM OF THE SESSION

To familiarize the students with the basic concept of the and the working of the simple network management protocol

INSTRUCTIONAL OBJECTIVES

The session is design to understand the:

1. To understand the concepts of the working of simple network management protocol.

LEARNING OUTCOMES

At the end of this session, you should be able to:

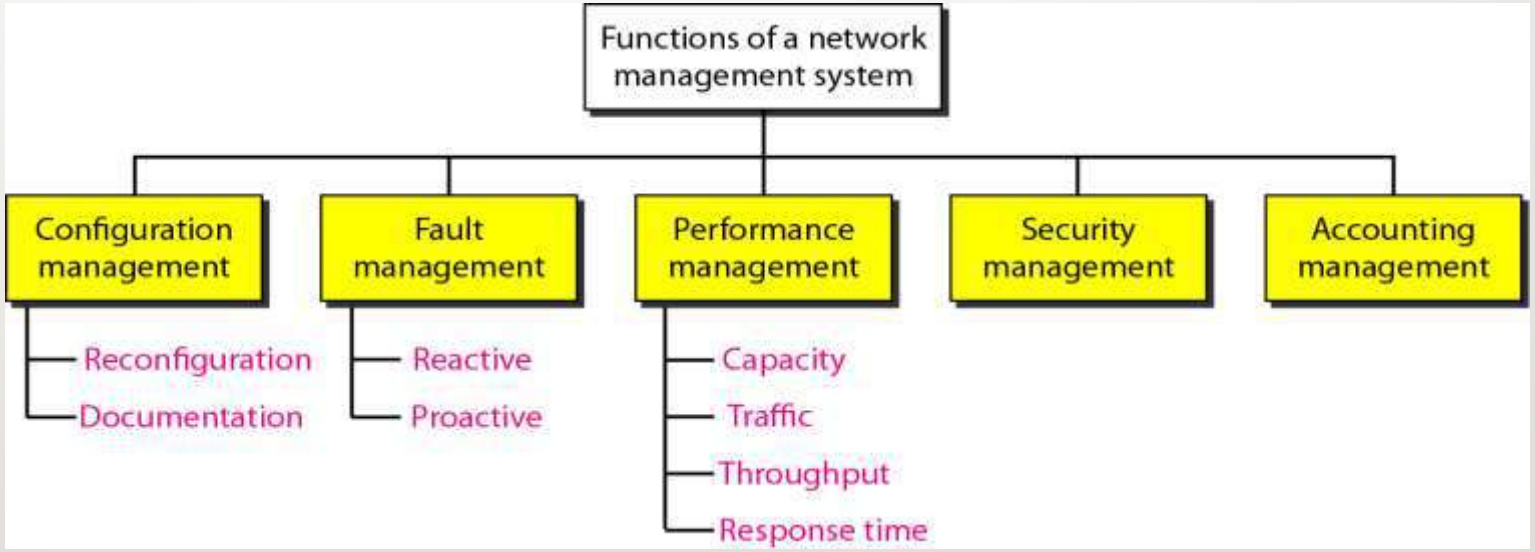
1. Describe the working of simple network management protocol.

SYLLABUS

SNMP

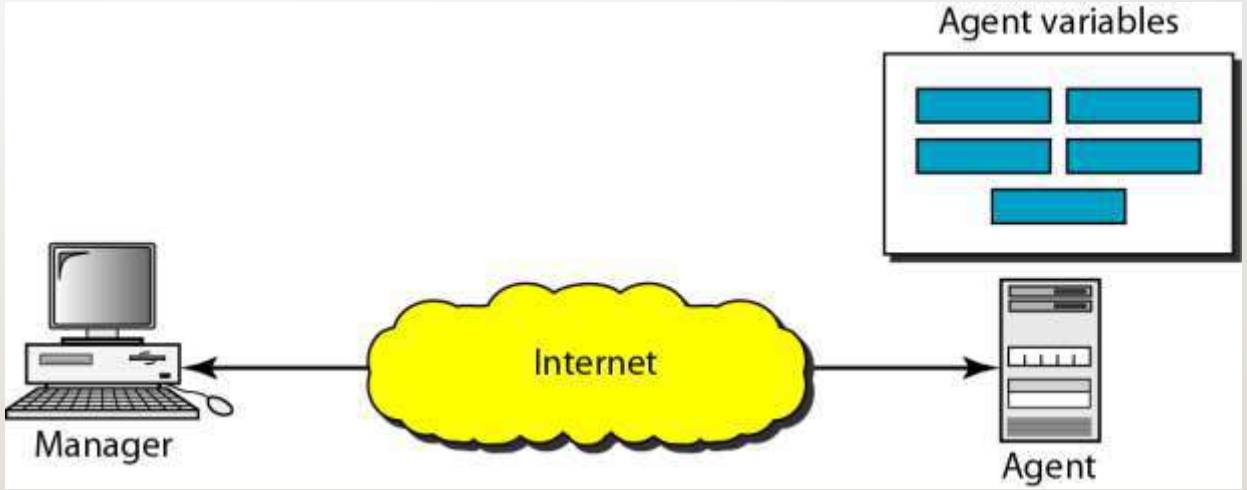
SIMPLE NETWORK MANAGEMENT PROTOCOL (SNMP)

- Function of the Network Management System
  - *The functions performed by a network management system can be divided into five broad categories:*



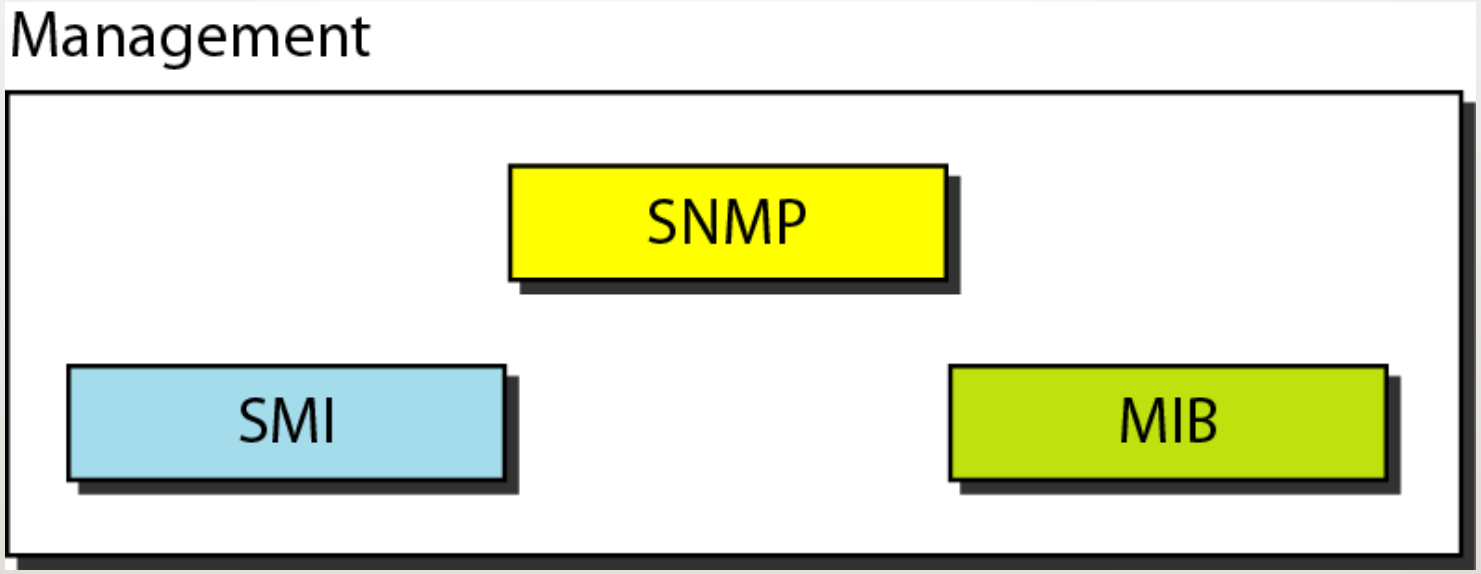
SIMPLE NETWORK MANAGEMENT PROTOCOL (SNMP)

- *The Simple Network Management Protocol (SNMP) is a framework for managing devices in an internet using the TCP/IP protocol suite. It provides a set of fundamental operations for monitoring and maintaining an internet.*
- *SNMP Concept*



SIMPLE NETWORK MANAGEMENT PROTOCOL (SNMP)

- Component of the SNMP



SIMPLE NETWORK MANAGEMENT PROTOCOL (SNMP)

- 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.
- SMI defines the general rules for naming objects, defining object types (including range and length), and showing how to encode objects and values. SMI does not define the number of objects an entity should manage or name the objects to be managed or define 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.

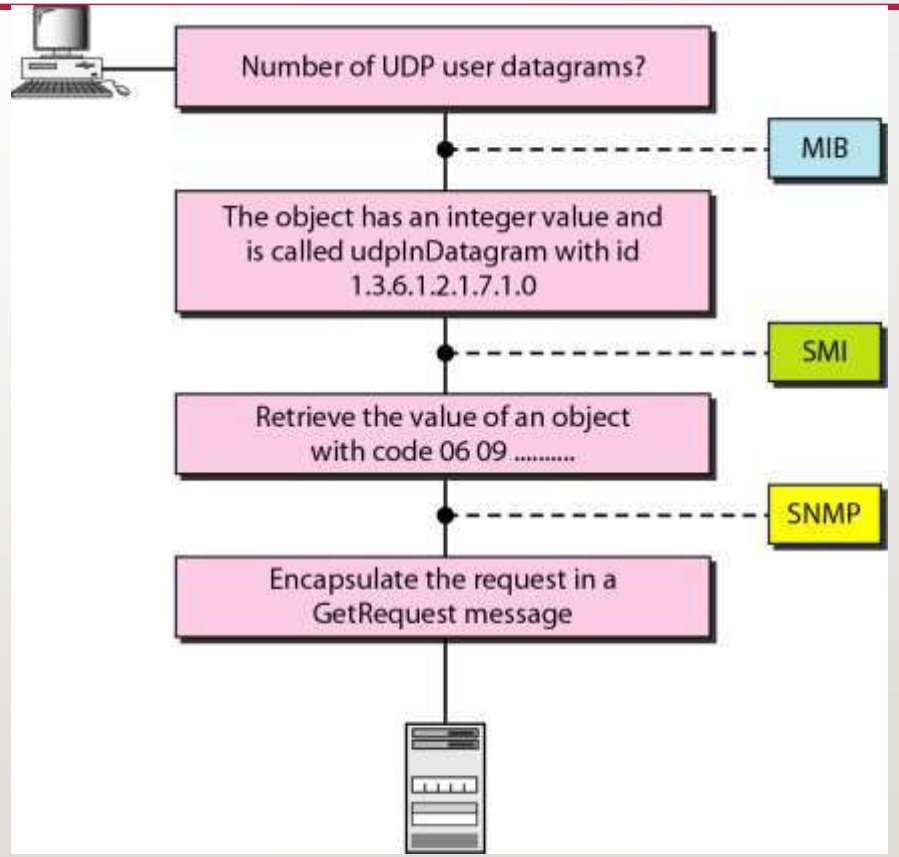
SIMPLE NETWORK MANAGEMENT PROTOCOL (SNMP)

- We can compare the task of network management to the task of writing a program.

  - Both tasks need rules. In network management this is handled by SMI.
  - Both tasks need variable declarations. In network management this is handled by MIB.
  - Both tasks have actions performed by statements. In network management this is handled by SNMP.

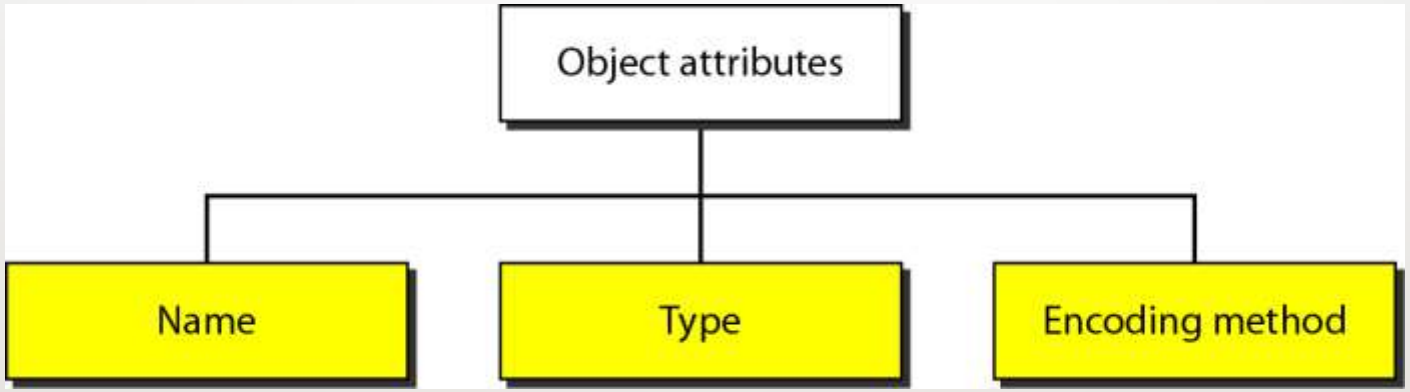
SIMPLE NETWORK MANAGEMENT PROTOCOL (SNMP)

- Overview of Managements



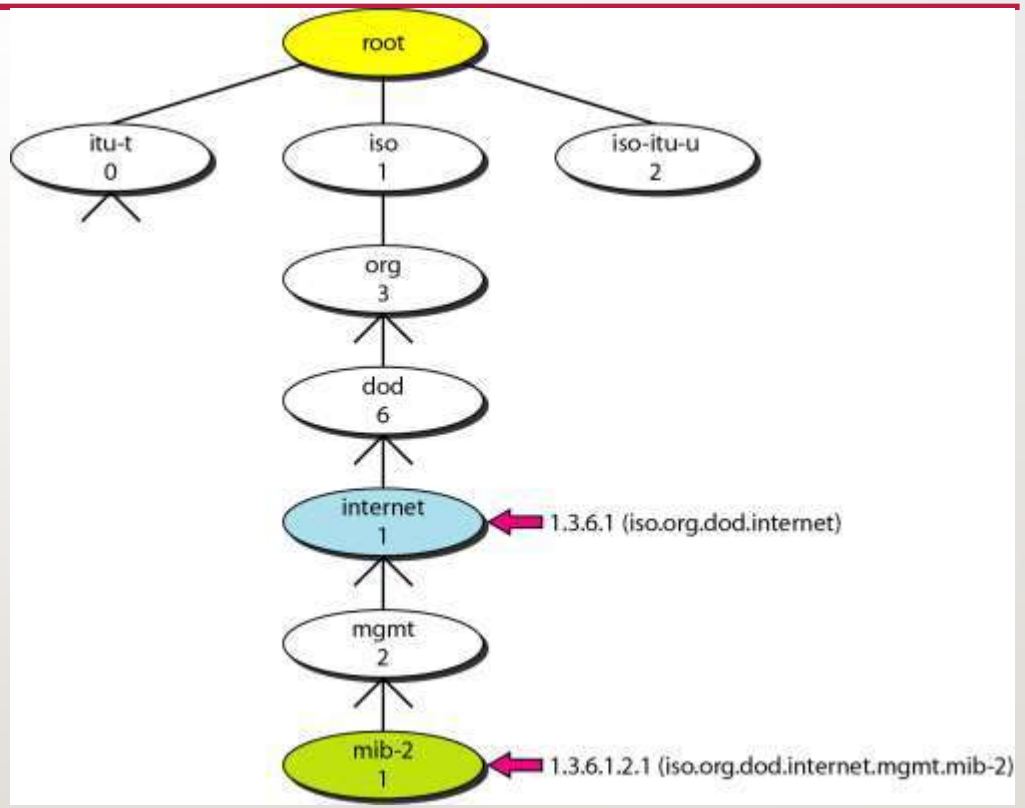
SIMPLE NETWORK MANAGEMENT PROTOCOL (SNMP)

- Object Attributes



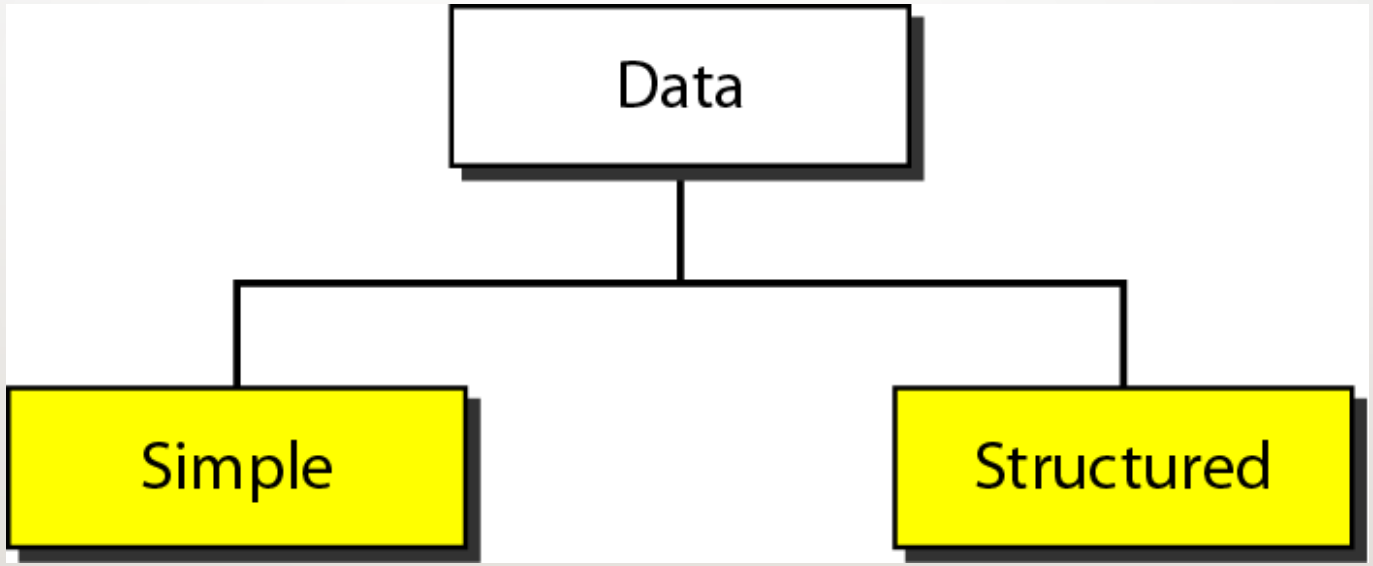
SIMPLE NETWORK MANAGEMENT PROTOCOL (SNMP)

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



SIMPLE NETWORK MANAGEMENT PROTOCOL (SNMP)

- Data Type



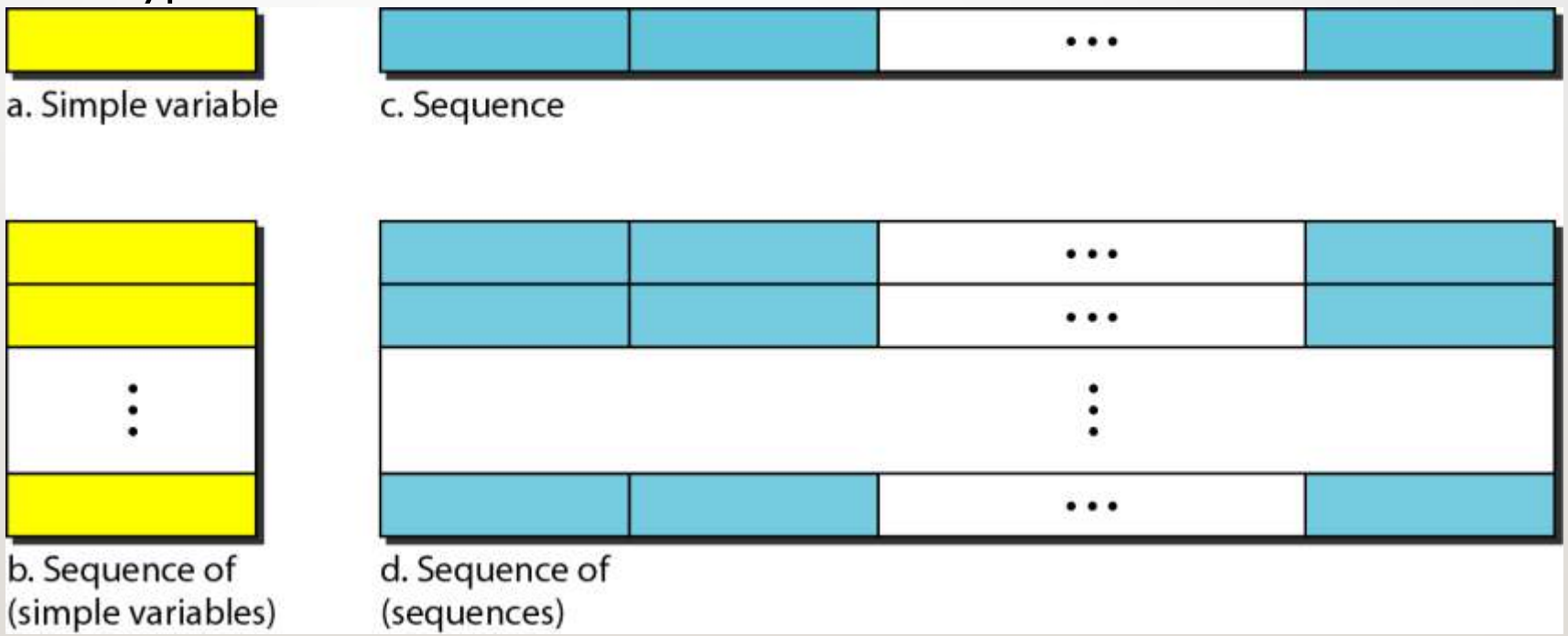
SIMPLE NETWORK MANAGEMENT PROTOCOL (SNMP)

- Data Type

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 0 to 2^{32}; when it reaches its maximum value, it wraps back to 0.
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 $\frac{1}{100}$ s
BITS		A string of bits
Opaque	Variable	Uninterpreted string

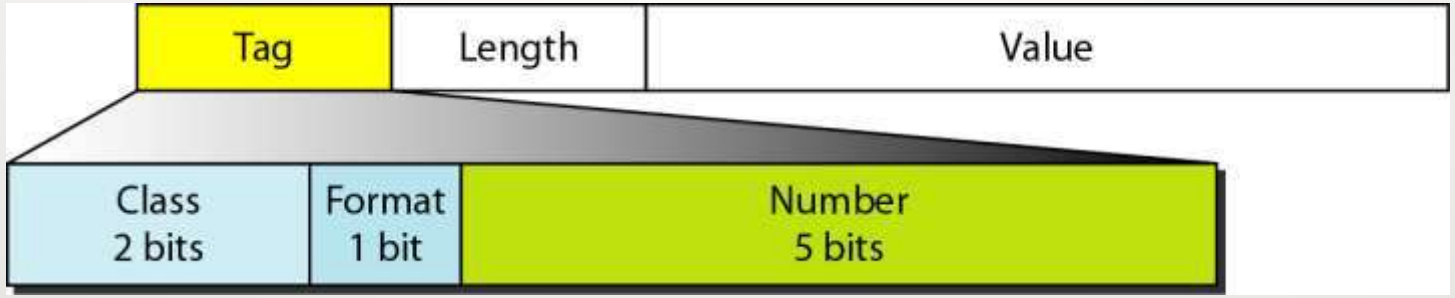
SIMPLE NETWORK MANAGEMENT PROTOCOL (SNMP)

- Conceptual Data Type



SIMPLE NETWORK MANAGEMENT PROTOCOL (SNMP)

- Encoding Format



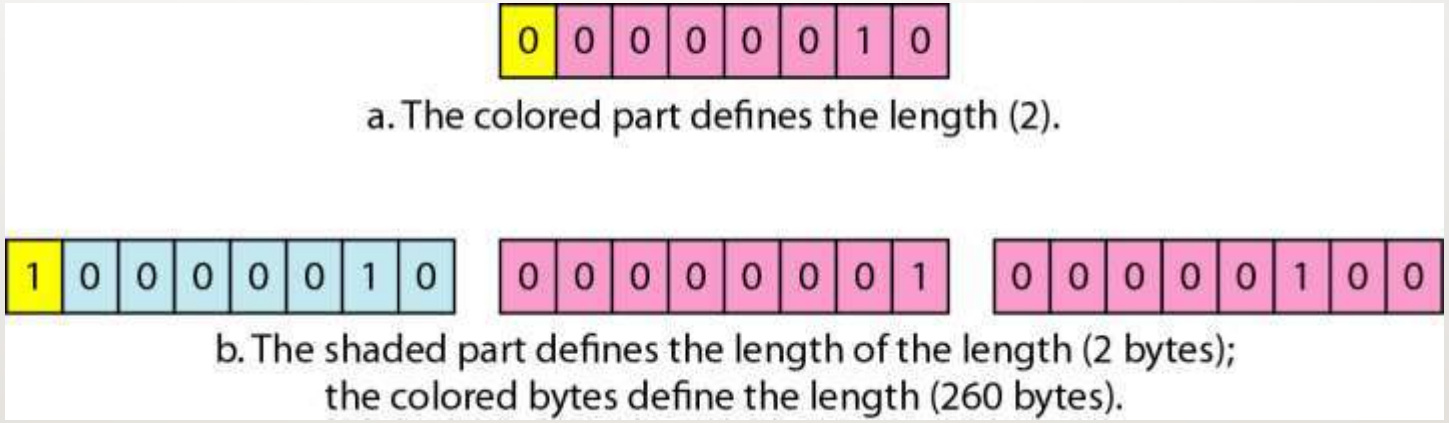
SIMPLE NETWORK MANAGEMENT PROTOCOL (SNMP)

- Codes for data type

Data Type	Class	Format	Number	Tag (Binary)	Tag (Hex)
INTEGER	00	0	00010	**00000010**	**02**
OCTET STRING	00	0	00100	**00000100**	**04**
OBJECT IDENTIFIER	00	0	00110	**00000110**	**06**
NULL	00	0	00101	**00000101**	**05**
Sequence, sequence of	00	1	10000	**00110000**	**30**
IPAddress	01	0	00000	**01000000**	**40**
Counter	01	0	00001	**01000001**	**41**
Gauge	01	0	00010	**01000010**	**42**
TimeTicks	01	0	00011	**01000011**	**43**
Opaque	01	0	00100	**01000100**	**44**

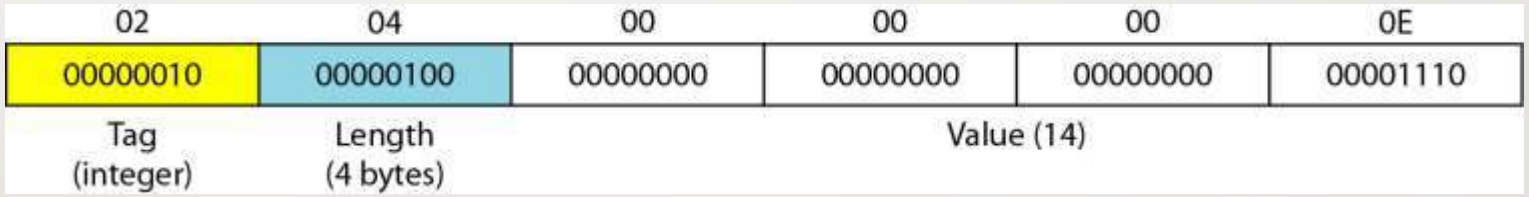
SIMPLE NETWORK MANAGEMENT PROTOCOL (SNMP)

- Length Format



SIMPLE NETWORK MANAGEMENT PROTOCOL (SNMP)

- Example
- Example to show how to define INTEGER 14



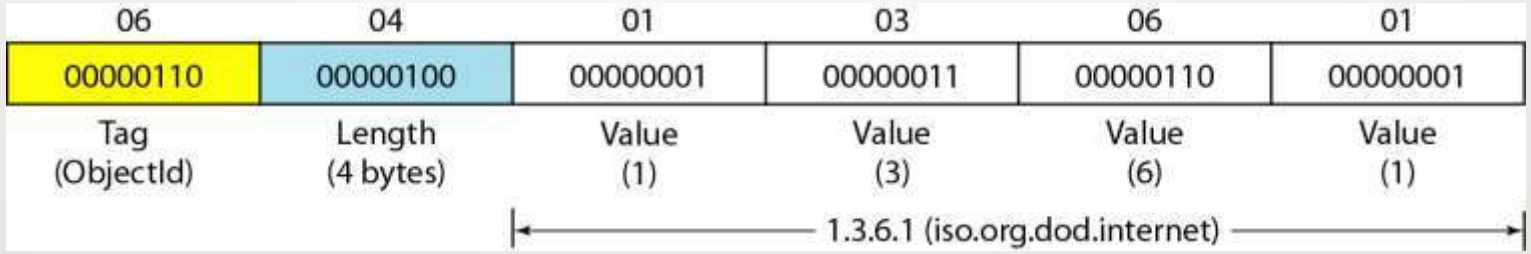
SIMPLE NETWORK MANAGEMENT PROTOCOL (SNMP)

- Example to show OCTATE String "HI"

04	02	48	49
00000100	00000010	01001000	01001001
Tag (String)	Length (2 bytes)	Value (H)	Value (I)

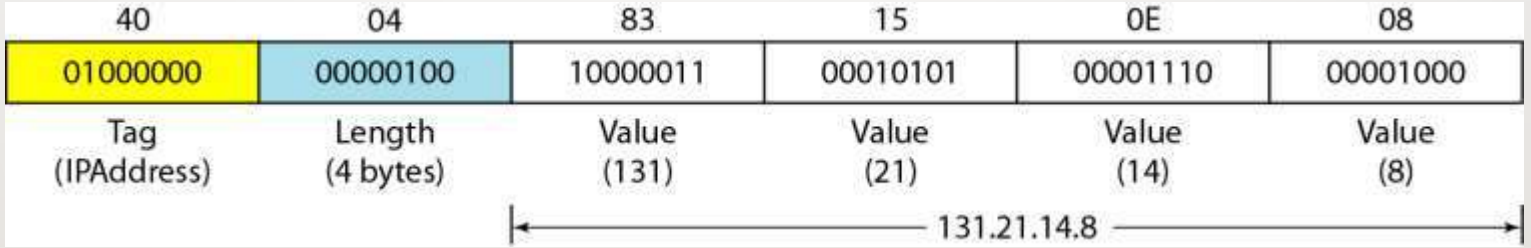
SIMPLE NETWORK MANAGEMENT PROTOCOL (SNMP)

- *Example to shows how to define Object Identifier 1.3.6.1 (iso.org.dod.internet).*



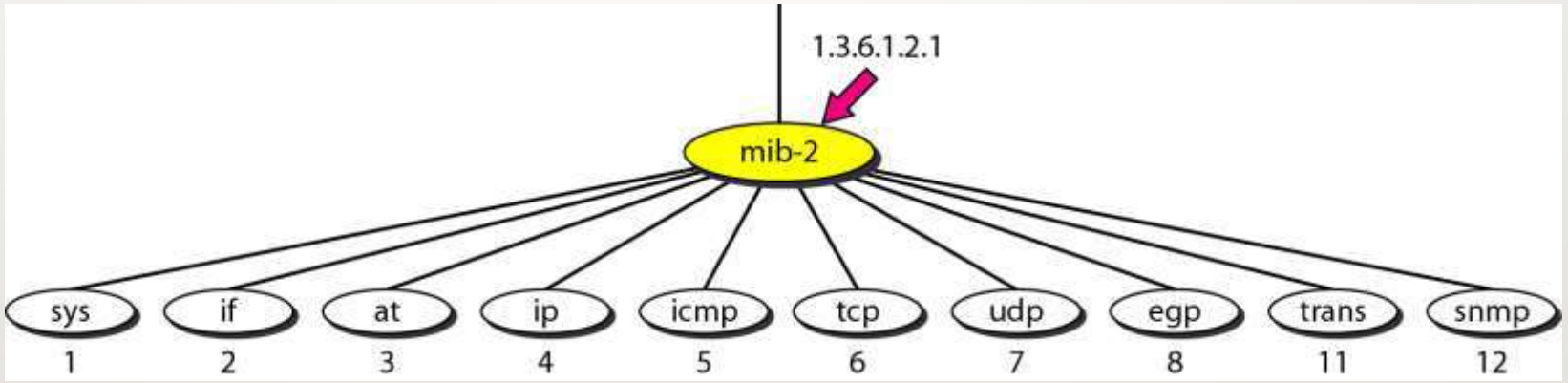
SIMPLE NETWORK MANAGEMENT PROTOCOL (SNMP)

- *Example to shows how to define IP Address 131.21.14.8*



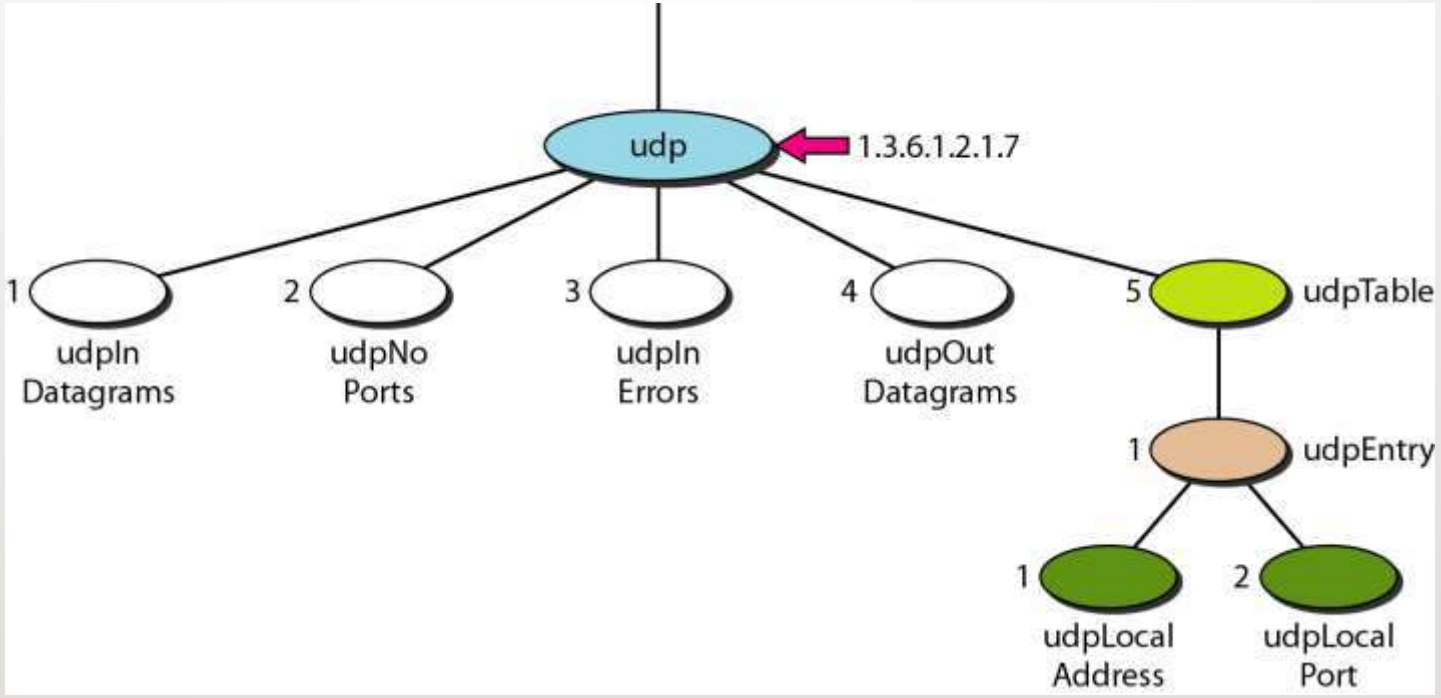
SIMPLE NETWORK MANAGEMENT PROTOCOL (SNMP)

- MIB 2



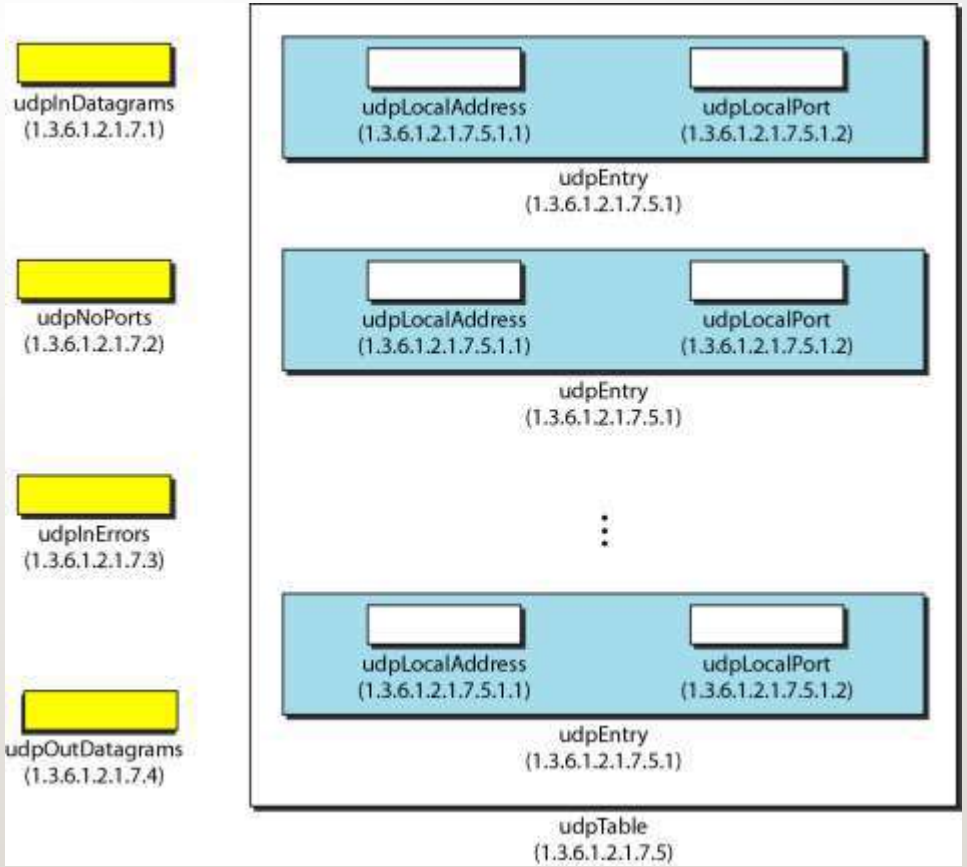
SIMPLE NETWORK MANAGEMENT PROTOCOL (SNMP)

- UDP Group



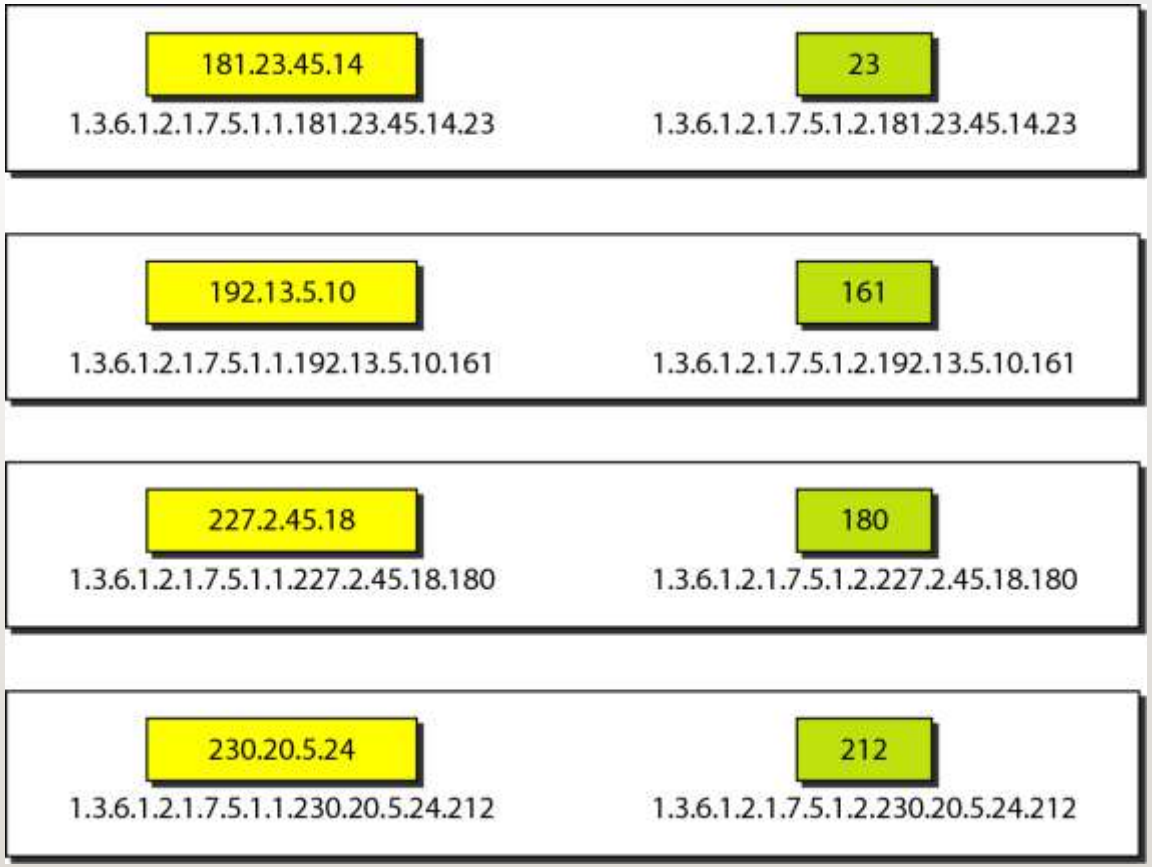
SIMPLE NETWORK MANAGEMENT PROTOCOL (SNMP)

- UDP variables and Tables



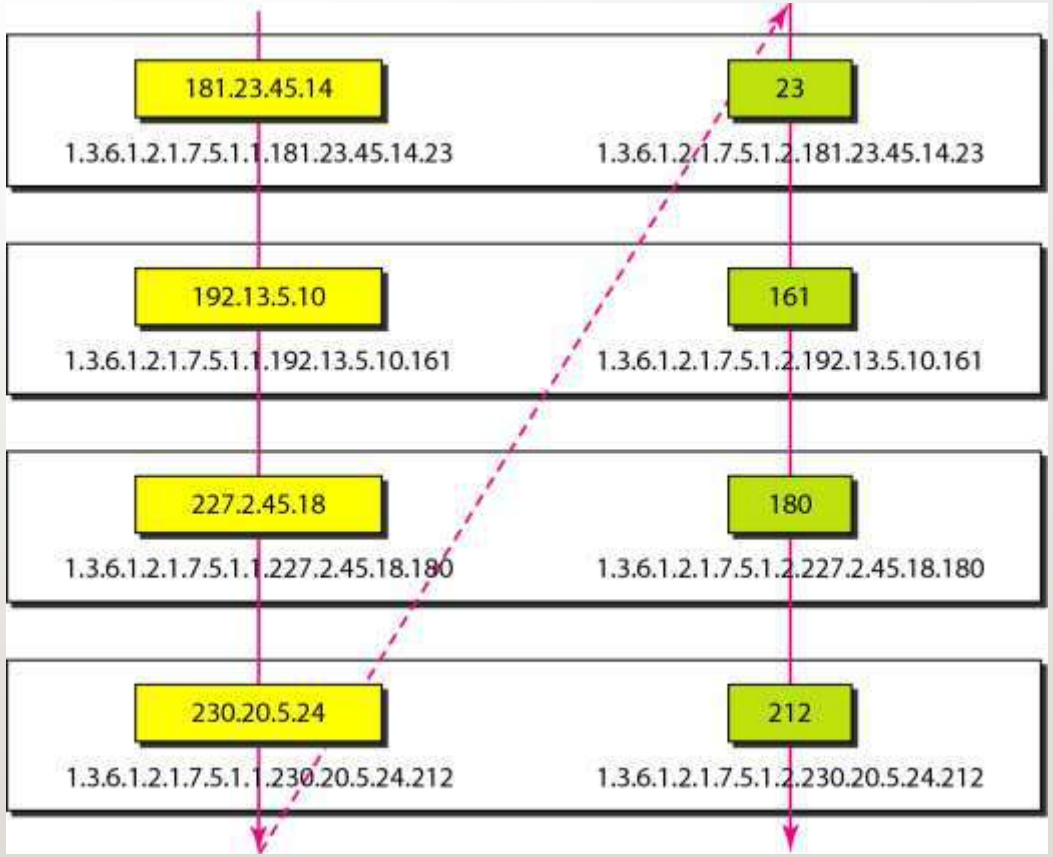
SIMPLE NETWORK MANAGEMENT PROTOCOL (SNMP)

- Indexes for UDP table



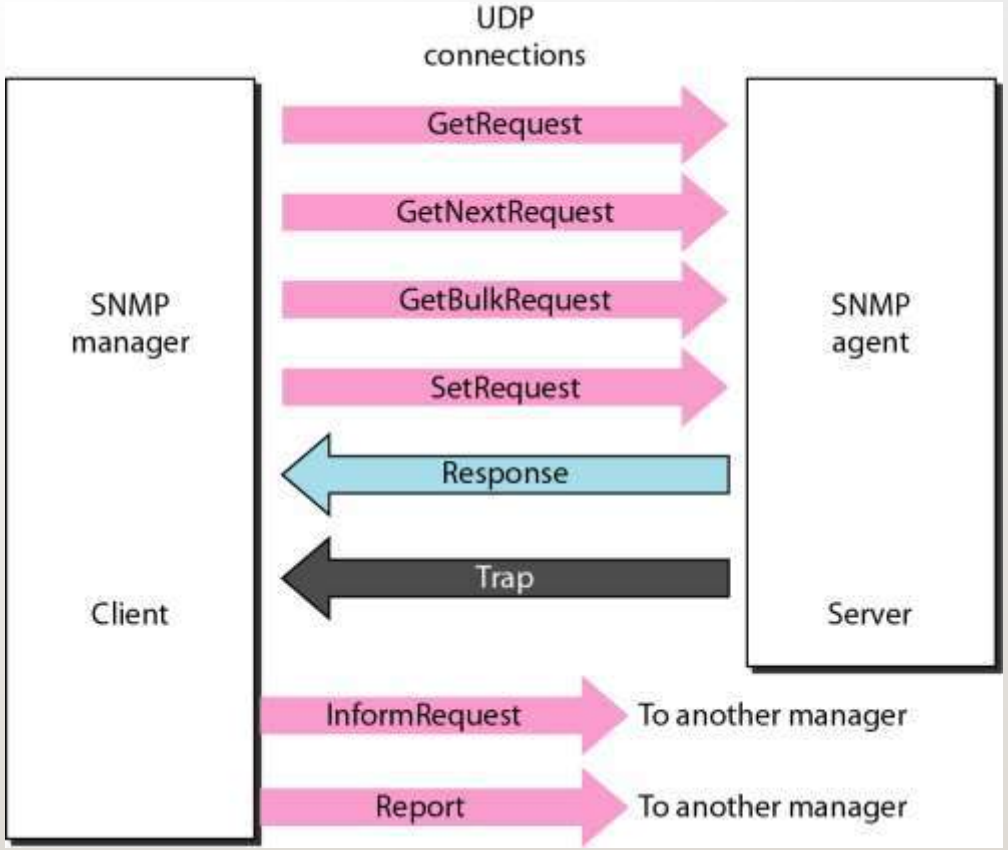
SIMPLE NETWORK MANAGEMENT PROTOCOL (SNMP)

- Lexicographic Ordering



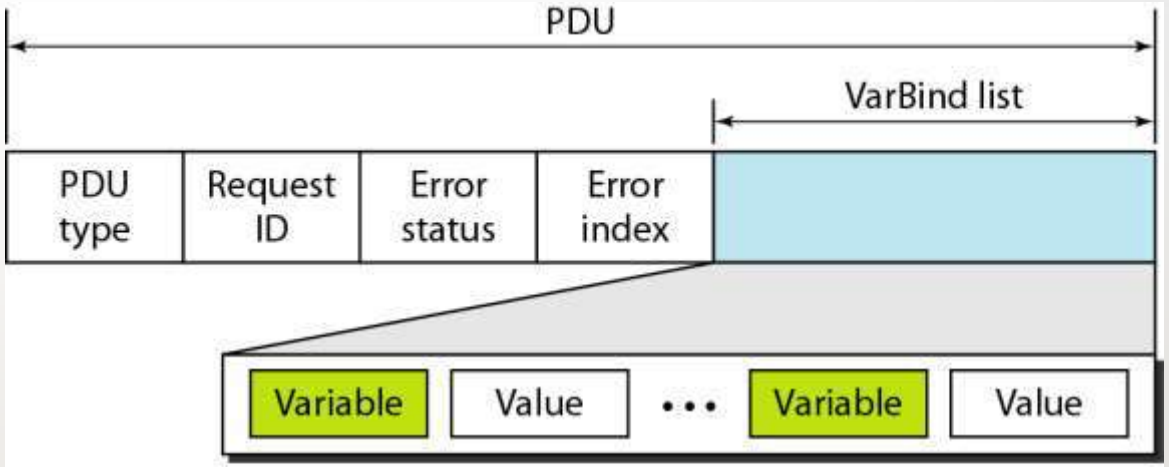
SIMPLE NETWORK MANAGEMENT PROTOCOL (SNMP)

- SMTP UDP



SIMPLE NETWORK MANAGEMENT PROTOCOL (SNMP)

- SMTP 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 nonrepeater field and error index field is replaced by max-repetitions field in GetBulkRequest.

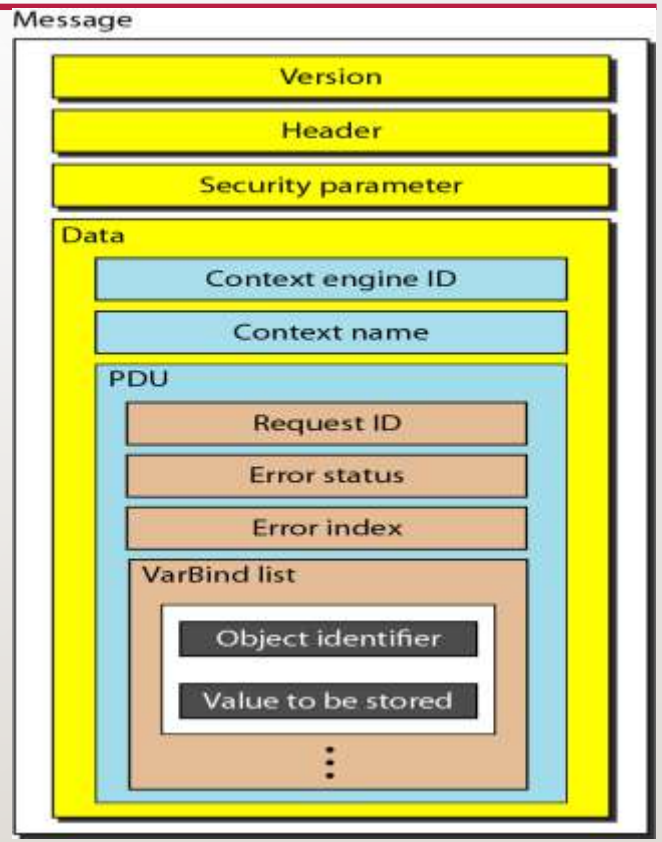
SIMPLE NETWORK MANAGEMENT PROTOCOL (SNMP)

- Types of Error

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

SIMPLE NETWORK MANAGEMENT PROTOCOL (SNMP)

- SNMP message



SIMPLE NETWORK MANAGEMENT PROTOCOL (SNMP)

- Codes for SNMP message

Data	*Class*	*Format*	*Number*	*Whole Tag (Binary)*	*Whole Tag (Hex)*
GetRequest	10	1	00000	**10100000**	**A0**
GetNextRequest	10	1	00001	**10100001**	**A1**
Response	10	1	00010	**10100010**	**A2**
SetRequest	10	1	00011	**10100011**	**A3**
GetBulkRequest	10	1	00101	**10100101**	**A5**
InformRequest	10	1	00110	**10100110**	**A6**
Trap (SNMPv2)	10	1	00111	**10100111**	**A7**
Report	10	1	01000	**10101000**	**A8**

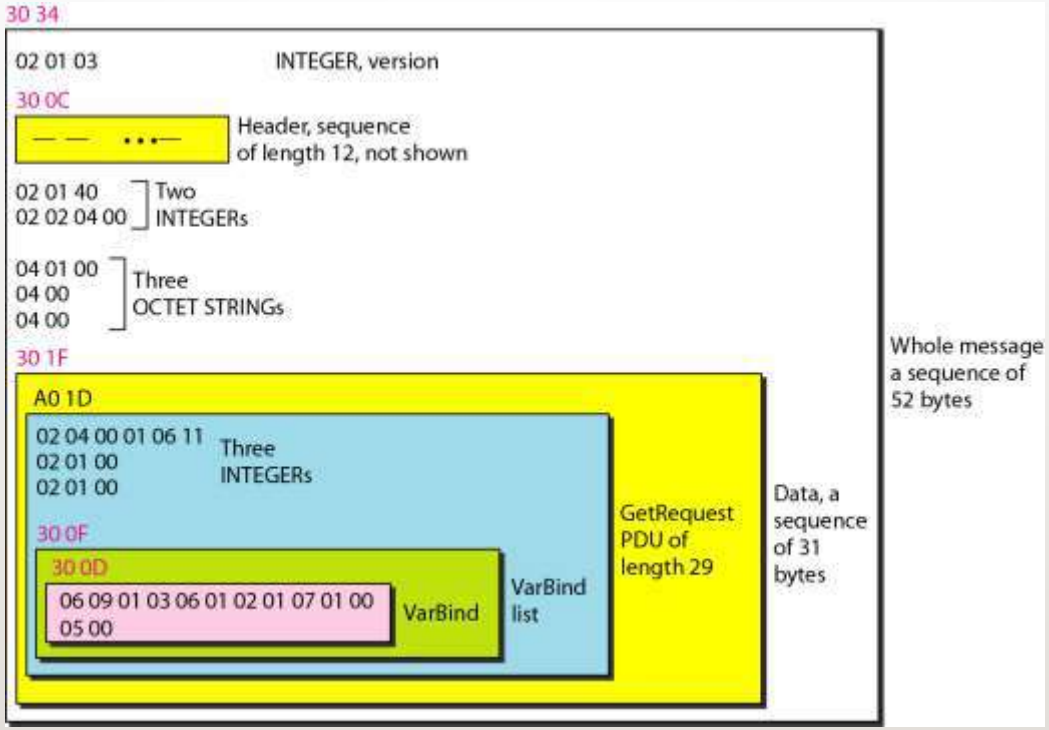
SIMPLE NETWORK MANAGEMENT PROTOCOL (SNMP)

- Example
- *In this example, a manager station (SNMP client) uses the GetRequest message to retrieve the number of UDP datagrams that a router has received. There is only one VarBind entity. 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. Figure 28.23 shows the conceptual view of the packet and the hierarchical nature of sequences. We have used white and colored boxes for the sequences and a gray one for the PDU. The VarBind list has only one VarBind.*

SIMPLE NETWORK MANAGEMENT PROTOCOL (SNMP)

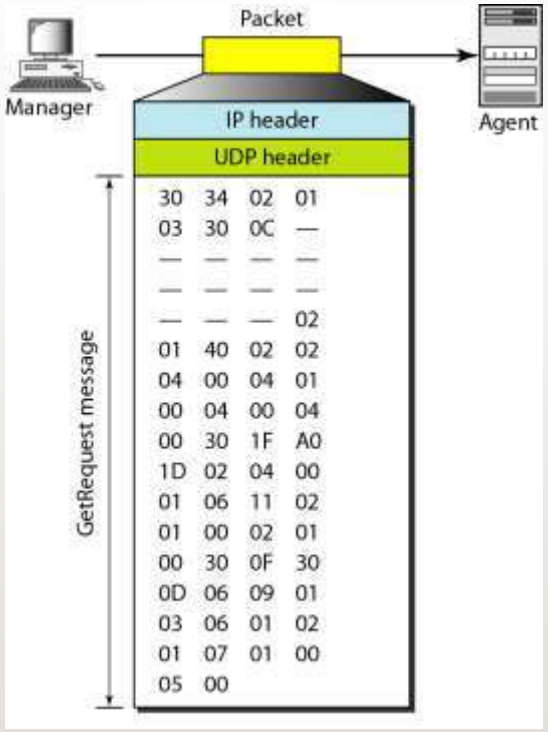
- Example (Continued)
- *The variable is of type 06 and length 09. The value is of type 05 and length 00. The whole VarBind is a sequence of length 0D (13). The VarBind list is also a sequence of length 0F (15). The GetRequest PDU is of length ID (29). Now we have three OCTET STRINGs related to the security parameter, security model, and flags. Then we have two integers defining maximum size (1024) and message ID (64). The header is a sequence of length 12, which we left blank for simplicity. There is one integer, version (version 3). The whole message is a sequence of 52 bytes. Figure 28.24 shows the actual message sent by the manager station (client) to the agent (server).*

SIMPLE NETWORK MANAGEMENT PROTOCOL (SNMP)



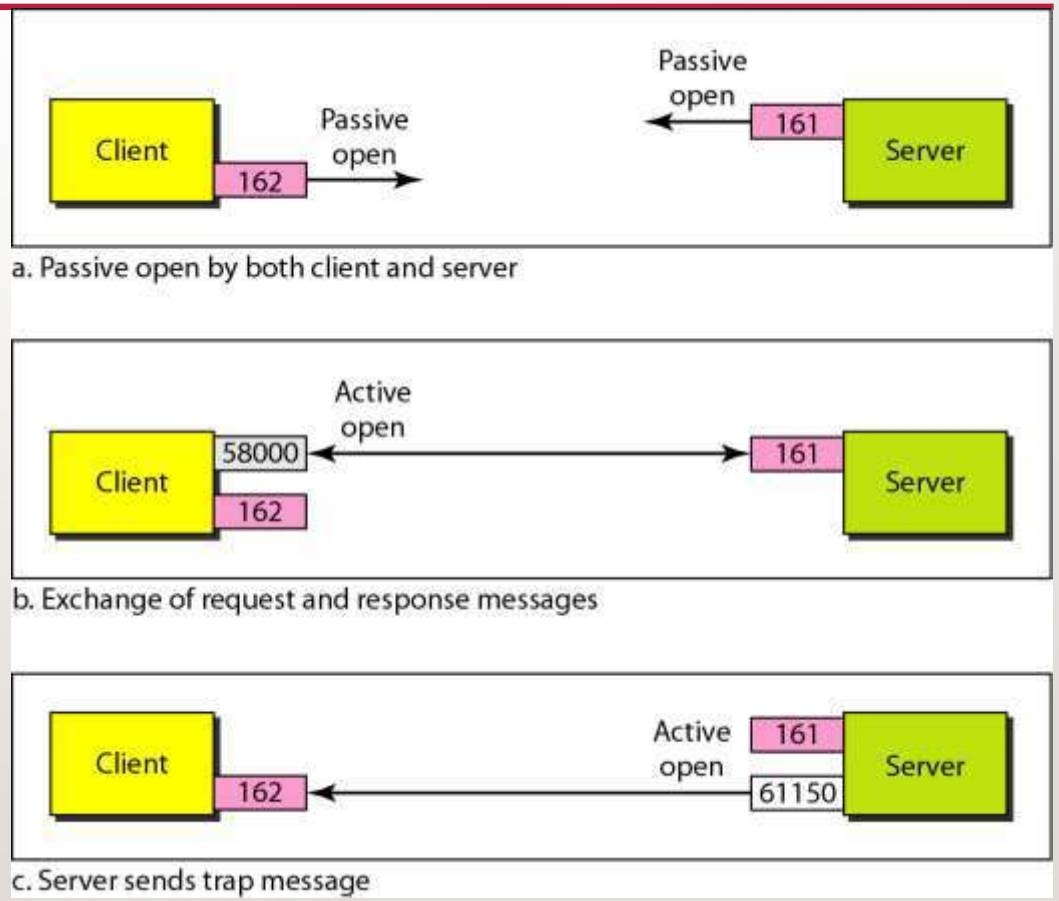
SIMPLE NETWORK MANAGEMENT PROTOCOL (SNMP)

GetRequest Message



SIMPLE NETWORK MANAGEMENT PROTOCOL (SNMP)

- Port Number of SNMP



REFERENCES FOR FURTHER LEARNING OF THE SESSION

Reference Books:

1. Data Communications and Networking (3rd Ed.) "–B. A. Ferouzan – TMH
2. Computer Networks (4th Ed.)", A. S. Tanenbaum – – Pearson Education/PHI

Sites and Web links:

1. https://www.scaler.com/topics/computer-network/socket-programming/
2. https://www.geeksforgeeks.org/socket-in-computer-network/
3. https://www.cloudflare.com/learning/ssl/what-is-ssl/
4. https://www.geeksforgeeks.org/secure-socket-layer-ssl/
5. https://www.javatpoint.com/simple-network-management-protocol
6. https://www.manageengine.com/network-monitoring/what-is-snmp.html

THANK YOU

TEAM –NETWORK PROTOCOLS & SECURITY (NPS)