

Network Management



Raj Jain

Washington University in Saint Louis
Saint Louis, MO 63130
Jain@wustl.edu

Audio/Video recordings of this lecture are available on-line at:

<http://www.cse.wustl.edu/~jain/cse473-10/>



- ❑ What is Network Management and How?
- ❑ OSI Net Management Standards
- ❑ ASN.1
- ❑ Management Information Base (MIB)
- ❑ SNMP: Protocol, Message formats
- ❑ SNMP V2 and SNMP V3

Note: This class lecture is based on Chapter 9 of the textbook (Kurose and Ross) and the figures provided by the authors.

What is Network Management?

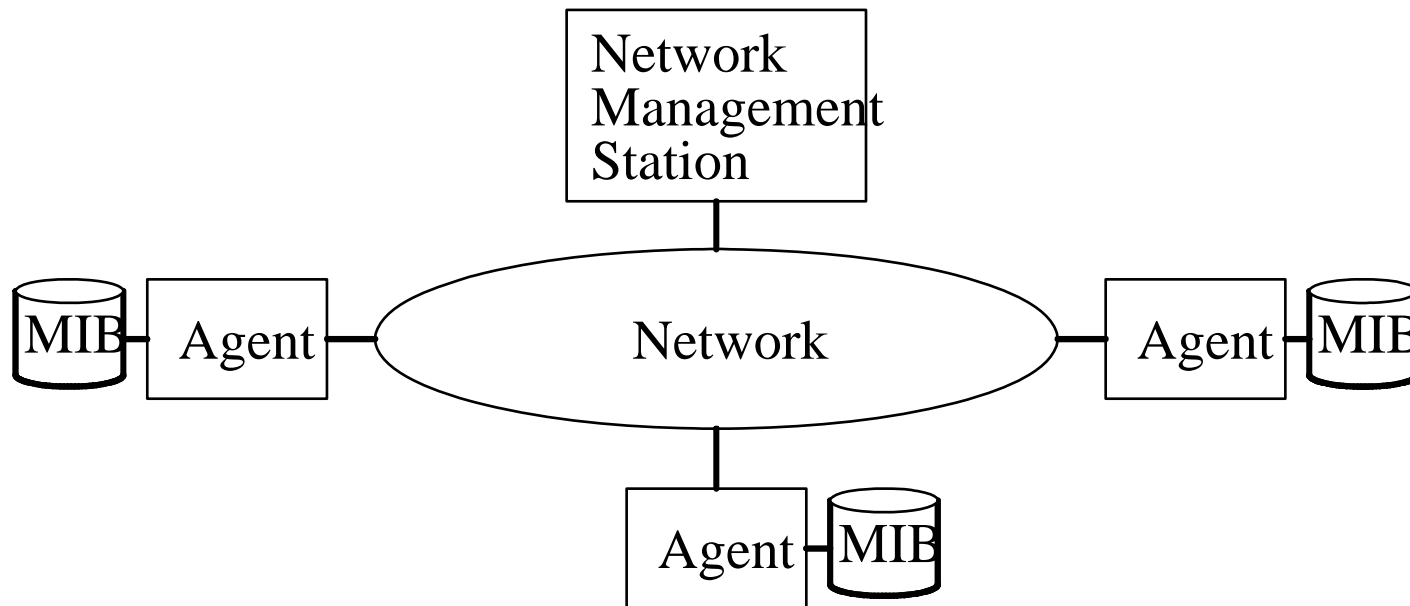
- ❑ Traffic on Network = Data + Control + Management
- ❑ **Data** = Bytes/Messages sent by users
- ❑ **Control** = Bytes/messages added by the system to properly transfer the data (e.g., routing messages)
- ❑ **Management** = Optional messages to ensure that the network functions properly and to handle the issues arising from malfunction of any component
- ❑ If all components function properly, control is still required but management is optional.
- ❑ Examples:
 - ❑ Detecting failures of an interface card at a host or a router
 - ❑ Monitoring traffic to aid in resource deployment
 - ❑ Intrusion Detection

Components of Network Management

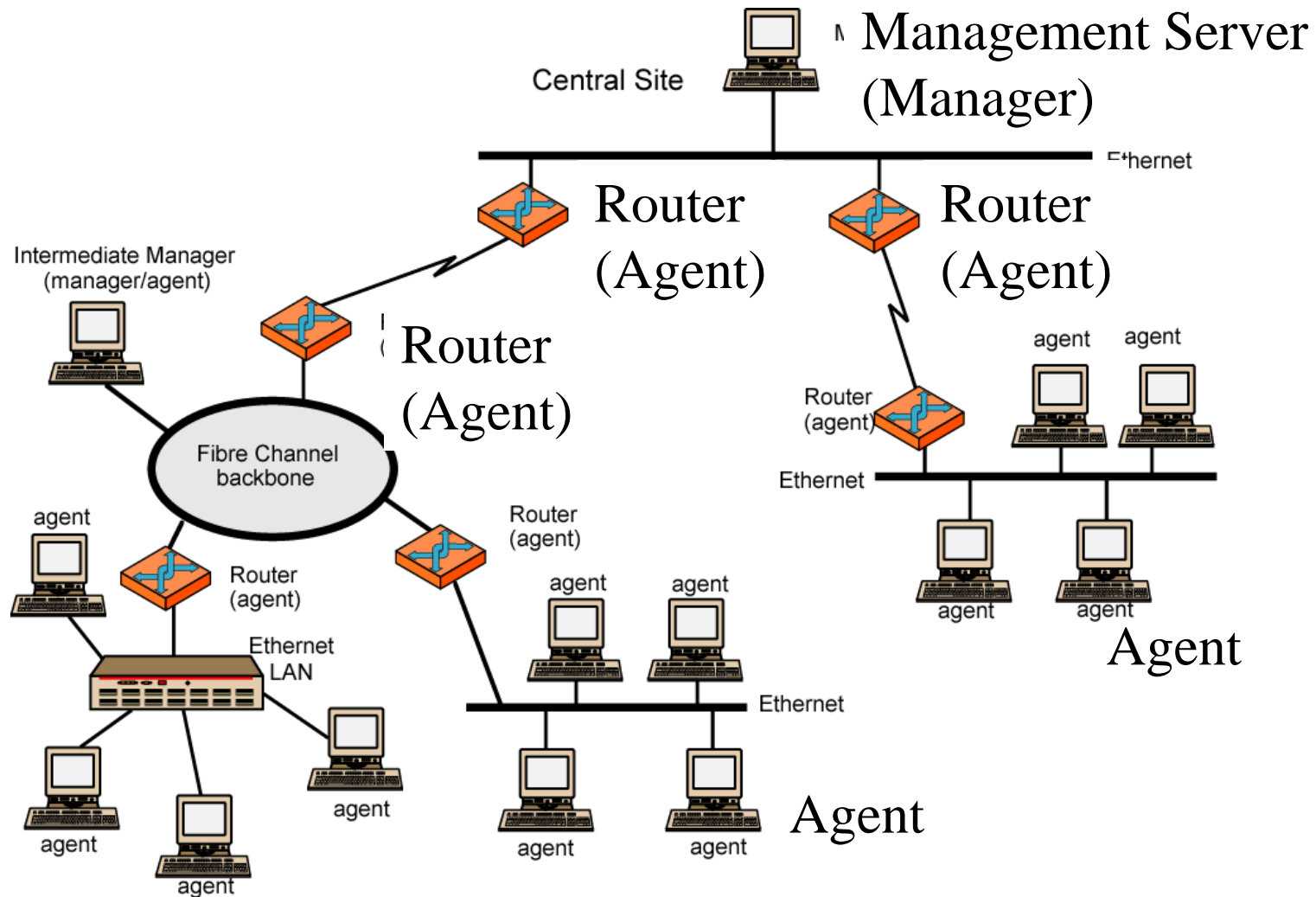
- 1. Performance Management:**
Measure, report, analyze, and control traffic, messages
- 2. Fault Management:**
Detect, log, and respond to fault conditions
- 3. Configuration Management:**
Track and control which devices are on or off
- 4. Accounting Management:**
Monitor resource usage for records and billing
- 5. Security Management:**
Enforce policy for access control, authentication, and authorization

How is Network Managed?

- ❑ Management = Initialization, Monitoring, Control
- ❑ Manager, Agents, and Management Information Base (MIB)



Example of Network Management



OSI Net Management Standards

- ❑ Common Management Information Protocol (CMIP)
- ❑ Common Management Information Service (CMIS)
- ❑ CMIP is the management (application layer) protocol
- ❑ CMIS is the service interface to CMIP
- ❑ It was expected that OSI management standards will eventually be used in the Internet. So a tentative simple solution was developed for the time being: Simple Network Management Protocol (SNMP)
- ❑ SNMP is now used throughout.
CMIP/CMIS is being replaced by SNMP.

Internet Management Framework

1. Structure of Management Information (SMI):
Data definition language for objects
ASN.1 was defined by ISO and is used in SNMP.
2. Management Information Base (MIB):
Distributed network management data
3. SNMP protocol:
Manager ↔ Managed object communication
4. Security, administration capabilities:
Major addition in SNMPv3

ASN.1

- ❑ Abstract Syntax Notation One
- ❑ Joint ISO and ITU-T standard, Original 1984, latest 2002.
- ❑ Used to specify protocol data structures
- ❑ X.400 electronic mail, X.500 and LDAP directory services, H.323 VOIP, SNMP, etc use ASN.1
- ❑ Pre-Defined: 1=Boolean, 2=Integer, 3=Bit String, 4=Octet String, 5=NULL, 6=Object Identifier, 9=Real
- ❑ Constructed: SEQUENCE (structure), SEQUENCE OF (lists), CHOICE, ...

SMI Base Data Types

Data Type	Description
INTEGER	ASN.1 32-bit integer between -2^{31} and $2^{31}-1$
Integer32	32-bit integer between -2^{31} and $2^{31}-1$
Unsigned32	Unsigned 32-bit integer between 0 and $2^{32}-1$
OCTET STRING	ASN.1 byte string for binary or text up to 65,535 bytes long
OBJECT IDENTIFIER	ASN.1 format administratively assigned object identifier
IPAddress	32-bit Internet address in network-byte order
Counter32	32-bit counter that increases from 0 to $2^{32}-1$ and wraps to 0
Counter64	64-bit counter
Gauge32	32-bit integer that does not count above $2^{32}-1$ or below 0
TimeTicks	Time interval measured in $1/100^{\text{th}}$ of a second
Opaque	Uninterpreted ASN.1 string (needed for backward compatibility)

ASN.1 Example

```
AddressType ::= SEQUENCE {  
  name      OCTET STRING,  
  number    INTEGER,  
  street     OCTET STRING,  
  city      OCTET STRING,  
  state     OCTET STRING,  
  zipCode   INTEGER  
}
```

Encoding Rules

- ❑ ASN.1 only specifies the structure.
- ❑ Encoding rules indicate how to encode the structure in to bits on the wire.
- ❑ Examples: Basic Encoding Rules (BER), Packed Encoding Rules (PER), XML Encoding rules (XER), Distinguished Encoding Rules (DER), ...
- ❑ In BER, everything is encoded as Tag-Length-Value.

BER Example

□ John Miller, 126 Main Street, Big City, MO 63130

30	2F	04	0B	4A	6F	68	6E	20	4D	69	6C	6C	65	72
Seq.	Len	Oct Str	Len	J	o	h	n		M	i	l	l	e	r

02	01	7E
Int	Len	126

04	0B	4D	61	69	6E	20	53	74	72	65	65	74
Oct str	Len	M	a	i	n		S	t	r	e	e	t

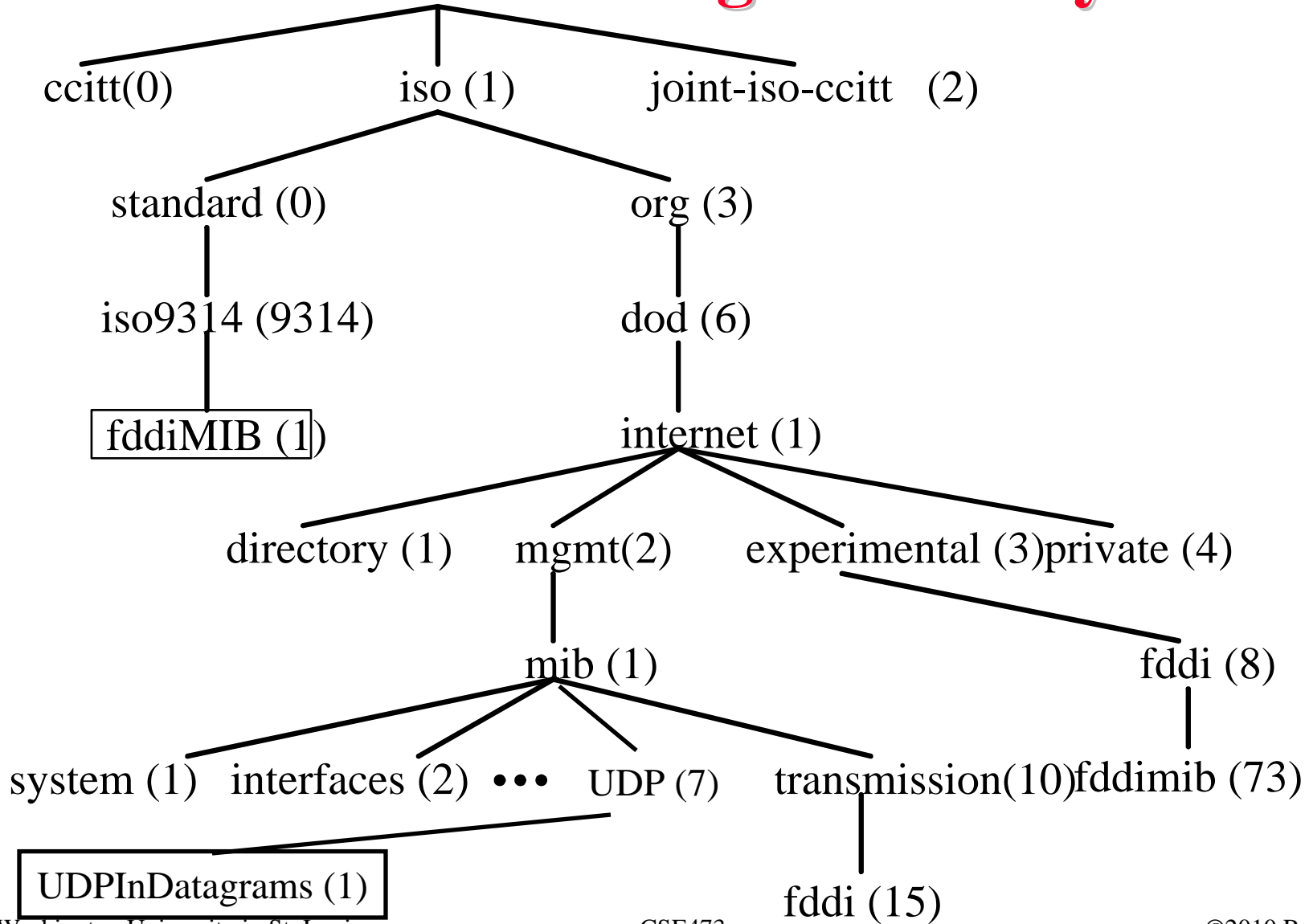
04	08	42	69	67	20	43	69	74	79
Oct Str	Len	B	i	g		C	i	t	y

04	02	4D	4F	02	02	F6	9A	0
Oct Str	Len	M	O	Int	len	63130	Null	

Management Information Base

- ❑ MIBs follow a fixed naming and structuring convention
⇒ Structure of Management Information (**SMI**)
- ❑ These conventions were adopted from Common management Information Protocol (**CMIP**) designed by ISO
- ❑ All names are globally unique
- ❑ All nodes of the name tree are assigned numeric values by standards authorities
iso.org.dod.internet.mgmt.mib.ip.ipInReceives
1.3.6.1.2.1.4.3
- ❑ Tables rows are referenced by appending the index
- ❑ All names are specified using a subset of Abstract Syntax Notation (ASN.1)
- ❑ ASN.1 specifies notation (that humans can read) and encoding (representation and ranges)

Global Naming Hierarchy



MIB Naming Example: UDP Module

<u>Object ID</u>	<u>Name</u>	<u>Type</u>	<u>Comments</u>
1.3.6.1.2.1.7.1	UDPinDatagrams	Counter32	total # datagrams delivered at this node
1.3.6.1.2.1.7.2	UDPNoPorts	Counter32	# undeliverable datagrams no app at port
1.3.6.1.2.1.7.3	UDInErrors	Counter32	# undeliverable datagrams all other reasons
1.3.6.1.2.1.7.4	UDPOutDatagrams	Counter32	# datagrams sent
1.3.6.1.2.1.7.5	udpTable	SEQUENCE	one entry for each port in use by app, gives port # and IP address

MIB Definition: Example

```
ipAddrTable ::= SEQUENCE of ipAddrEntry
ipAddrEntry ::= SEQUENCE {
  ipAdEntAddr ipAddress,
  ipAdEntIfIndex INTEGER,
  ipAdEntNetMask ipAddress,
  ipAdEntBcastAddr ipAddress,
  ipAdEntReasmMaxSize INTEGER (0..65535)
}
ipAddrEntry {ipAddrTable 1}
ipAdEntNetMask {ipAddrTable 3}
```

SNMP

- ❑ Based on Simple Gateway Management Protocol (SGMP) – RFC 1028 – Nov 1987
- ❑ SNMP = **S**imply **N**ot **M**y **P**roblem [Marshall Rose]
Simple Network Management Protocol
- ❑ RFC 1058, April 1988
- ❑ Only Five commands

Command

Meaning

get-request

Fetch a value

get-next-request

Fetch the next value (in a tree)

get-response

Reply to a fetch operation

set-request

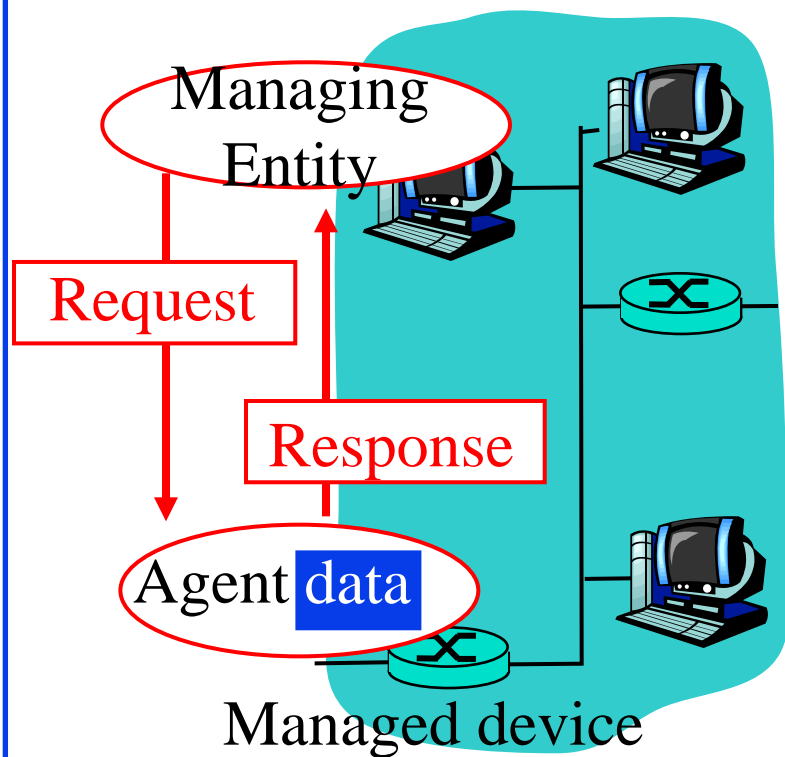
Store a value

trap

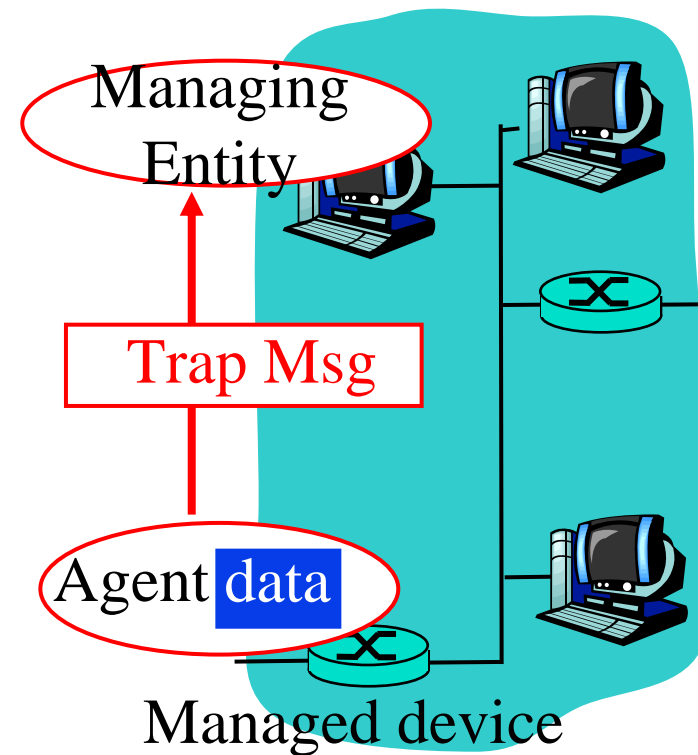
An event

SNMP protocol

Two ways to convey MIB info, commands:



Request/response mode

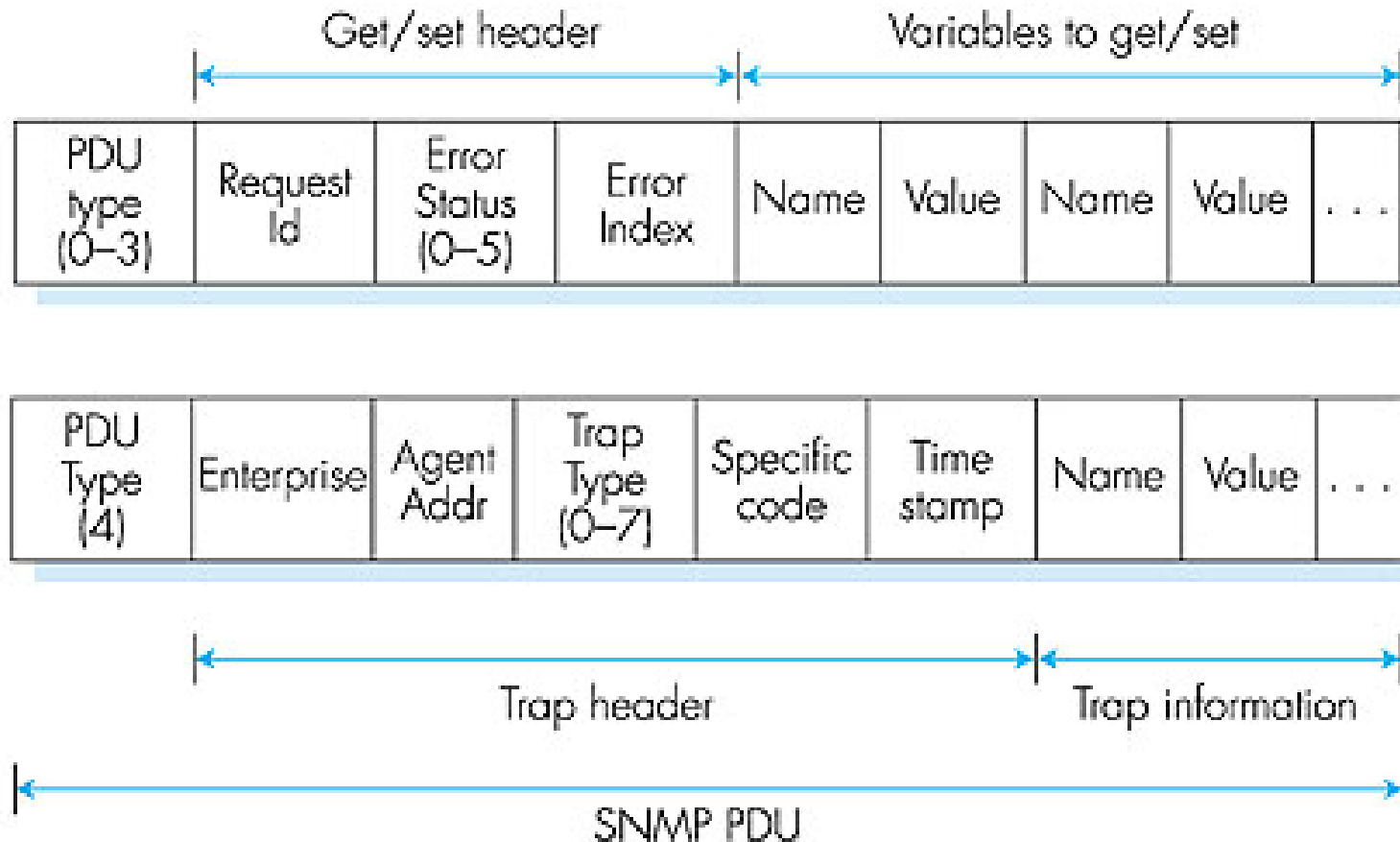


Trap mode

SNMPv2 PDU Types

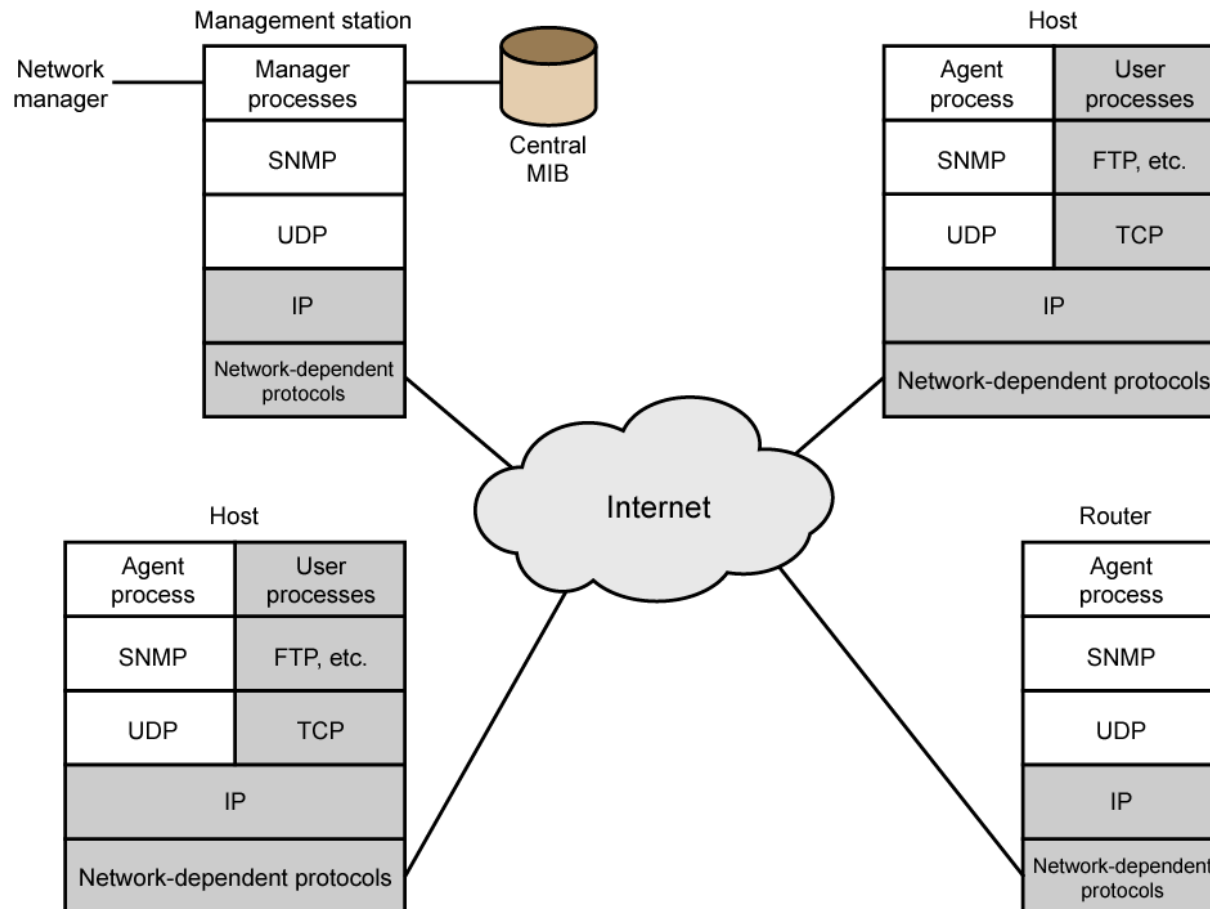
SNMPv2 PDU Type	Sender-Receiver	Description
GetRequest	Manager-to-agent	Get value of one or more MIB object instances
GetNextRequest	Manager-to-agent	Get value of next MIB object instance in list or table
GetBulkRequest	Manager-to-agent	Get values in large block of data, e.g., whole table
InformRequest	Manager-to-manager	Inform remote managing entity of MIB values
SetRequest	Manager-to-agent	Set value of one or more MIB object
Response	Agent-to-Manager	GetRequest, GetNextRequest, GetBulkRequest, SetRequest or InformRequest
SNMPv2 Trap	Agent-to-	Inform manager of exceptional

SNMP Message Formats



SNMPv1 Configuration

- ❑ Manager sends request to UDP port 161.
Agents send traps to UDP port 162



SNMPv2

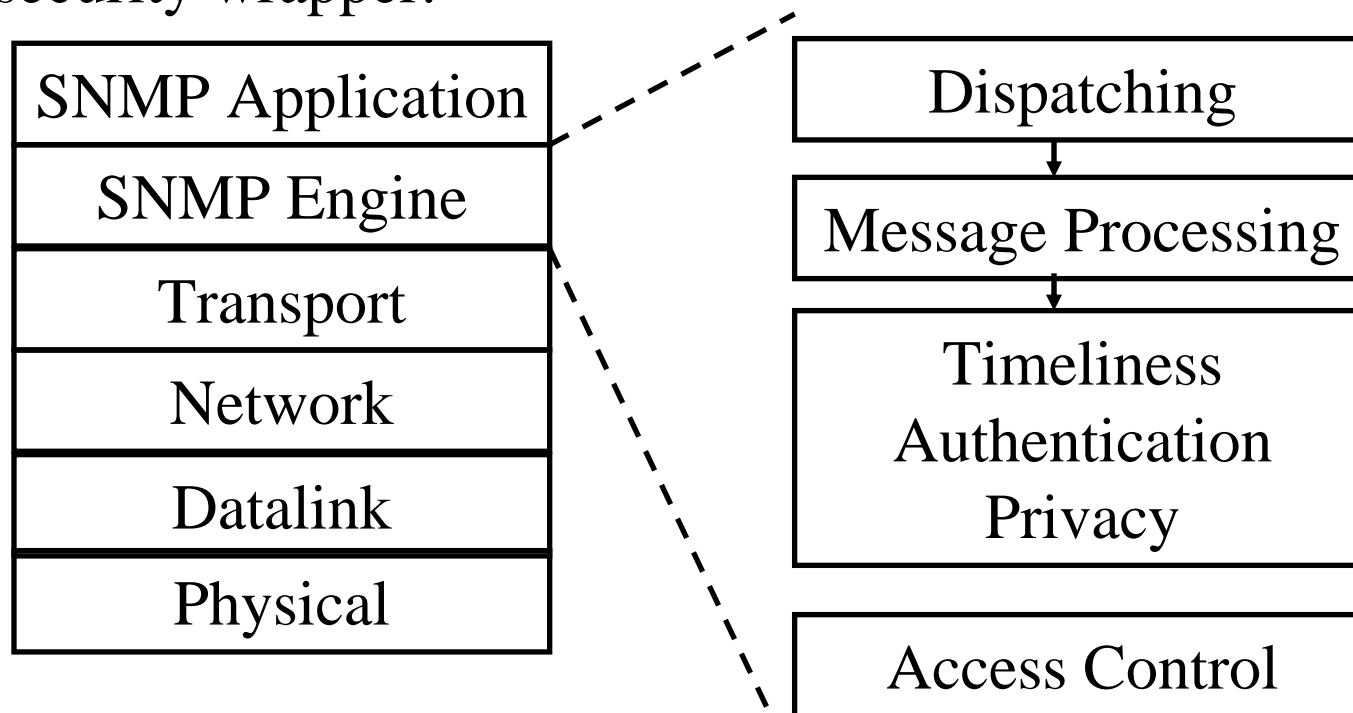
- ❑ Improved security: authentication and integrity using Data Encryption Standard (DES)
- ❑ *inform request* ⇒ Multiple manager coordination
Locking mechanisms prevent multiple managers from writing at the same time
- ❑ *get bulk* ⇒ Better table handling
- ❑ Confirmation option for Traps
⇒ Agents can ensure that trap was received correctly.
- ❑ New Error codes: noSuchName, badValue, readOnly
- ❑ Reference: RFC 1441, April 1993 and more

SNMPv3

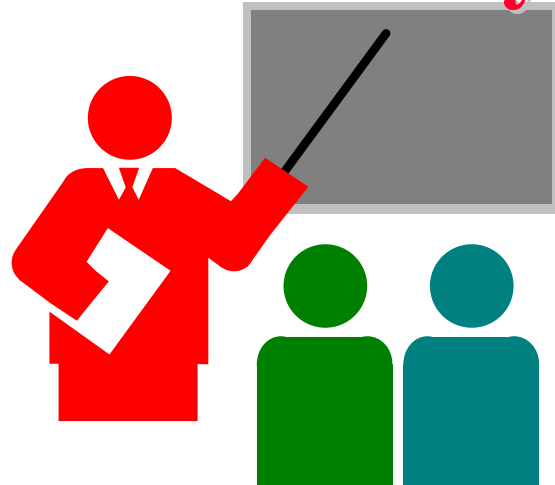
- ❑ Security update of SNMPv2
- ❑ Authentication: Message authentication code with a shared secret key
- ❑ Privacy: Encryption using a shared secret key
- ❑ Access Control: Each manager can have a different set of read/write permission for various component of MIB
- ❑ Ref: RFC 2570, April 1999 and more

SNMPv3 Engine

- ❑ SNMP Applications generate GetRequest, SetRequest, ..., commands
- ❑ SNMP Engine where SNMP version is determined, wrapped in a header containing version, message ID, size and then in a security wrapper.



Summary



- ❑ Management = Initialization, Monitoring, and Control
- ❑ SNMP = Only 5 to 7 commands
- ❑ Standard MIBs defined for each object
- ❑ Uses ASN.1 encoding
- ❑ SNMPv2 fixed issues with bulk requests and simple security
- ❑ SNMPv3 added security

Review Exercises

- ❑ **Try but do not submit**
- ❑ Review Questions: R1 through R12
- ❑ Problems P1 through P8
- ❑ Read Pages 771-800

Homework 9

- What would be the BER encoding of {firstname “Ed”} {weight 259}? ASN.1 type for octet strings is 4 and for integers it is 2.