Network Management (SNMP)

Raj Jain
Washington University
Saint Louis, MO 63131
Jain@cse.wustl.edu

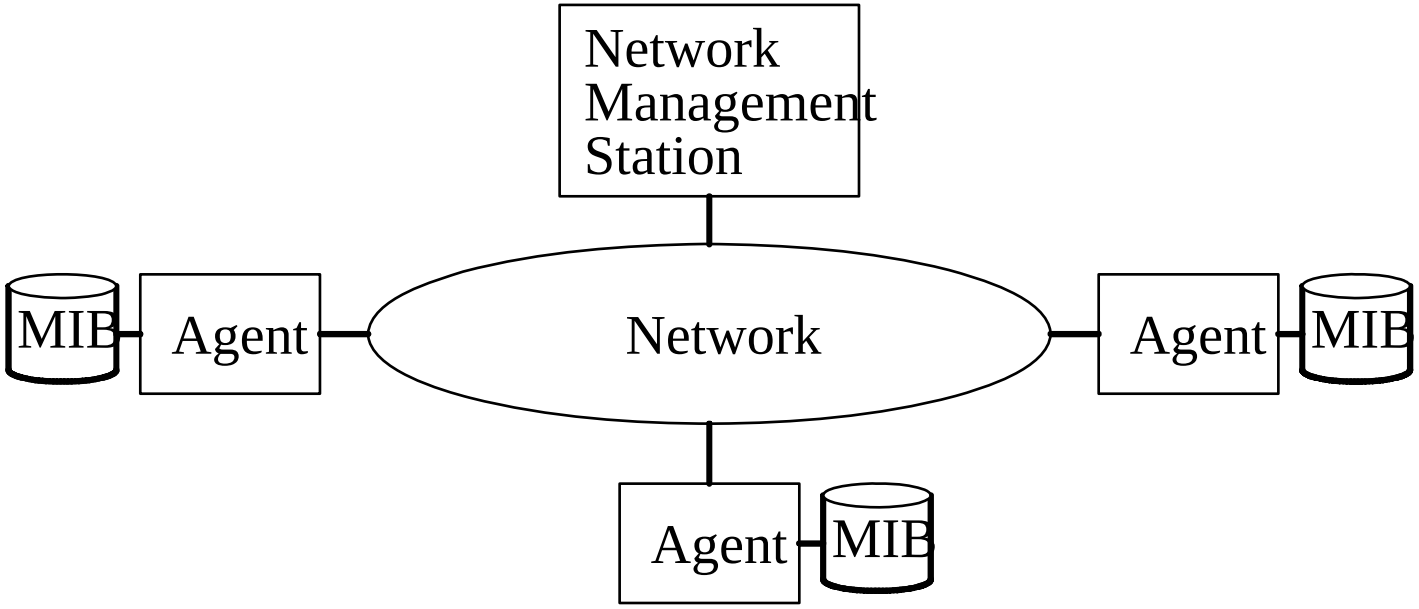
These slides are available on-line at:

http://www.cse.wustl.edu/~jain/cse473-05/

- Network Management
- SNMP
- Management information base (MIB)
- ASN.1 Notation
- SNMPv2
- SNMPv3

Network Management

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



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

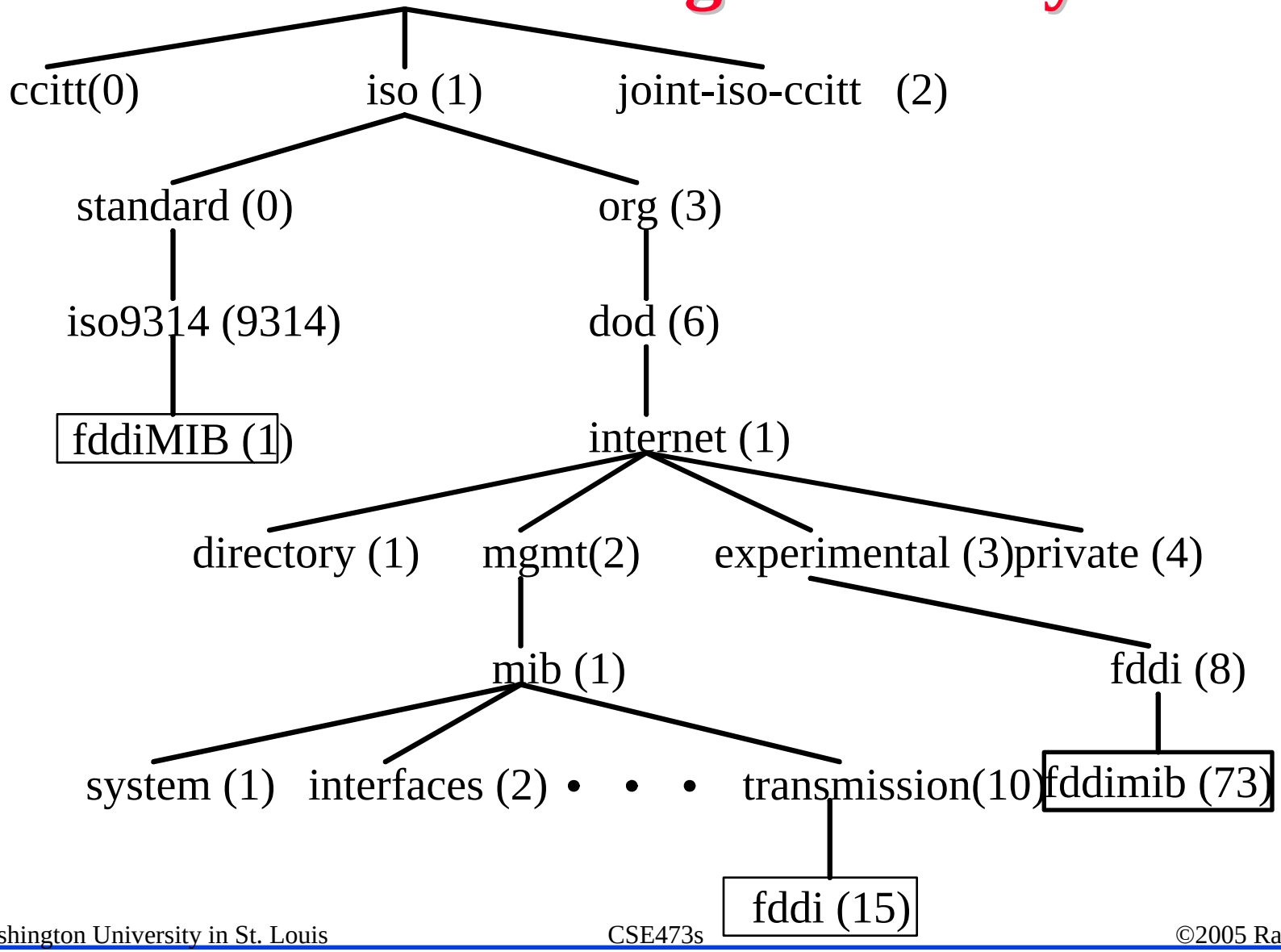
Management Information Base

- MIBs follow a fixed naming and structuring convention
  $\Rightarrow$ 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

MIB (Cont)

- 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)
- Only INTEGER, OCTET STRING, OBJECT IDENTIFIER, NULL types
- Only SEQUENCE, SEQUENCE OF, CHOICE constructors

Global Naming Hierarchy



Variable	Category	Meaning
sysUpTime	system	Time since last reboot
ifNumber	interfaces	# of Interfaces
ifMTU	interfaces	MTU
ipDefaultTTL	ip	Default TTL
ipInReceives	ip	# of datagrams received
ipForwDatagrams	ip	# of datagrams forwarded
icmpInEchos	icmp	# of Echo requests received
tcpRtoMin	tcp	Min retrans time
tcpMaxConn	tcp	Max connections allowed

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}

Example of Network Management

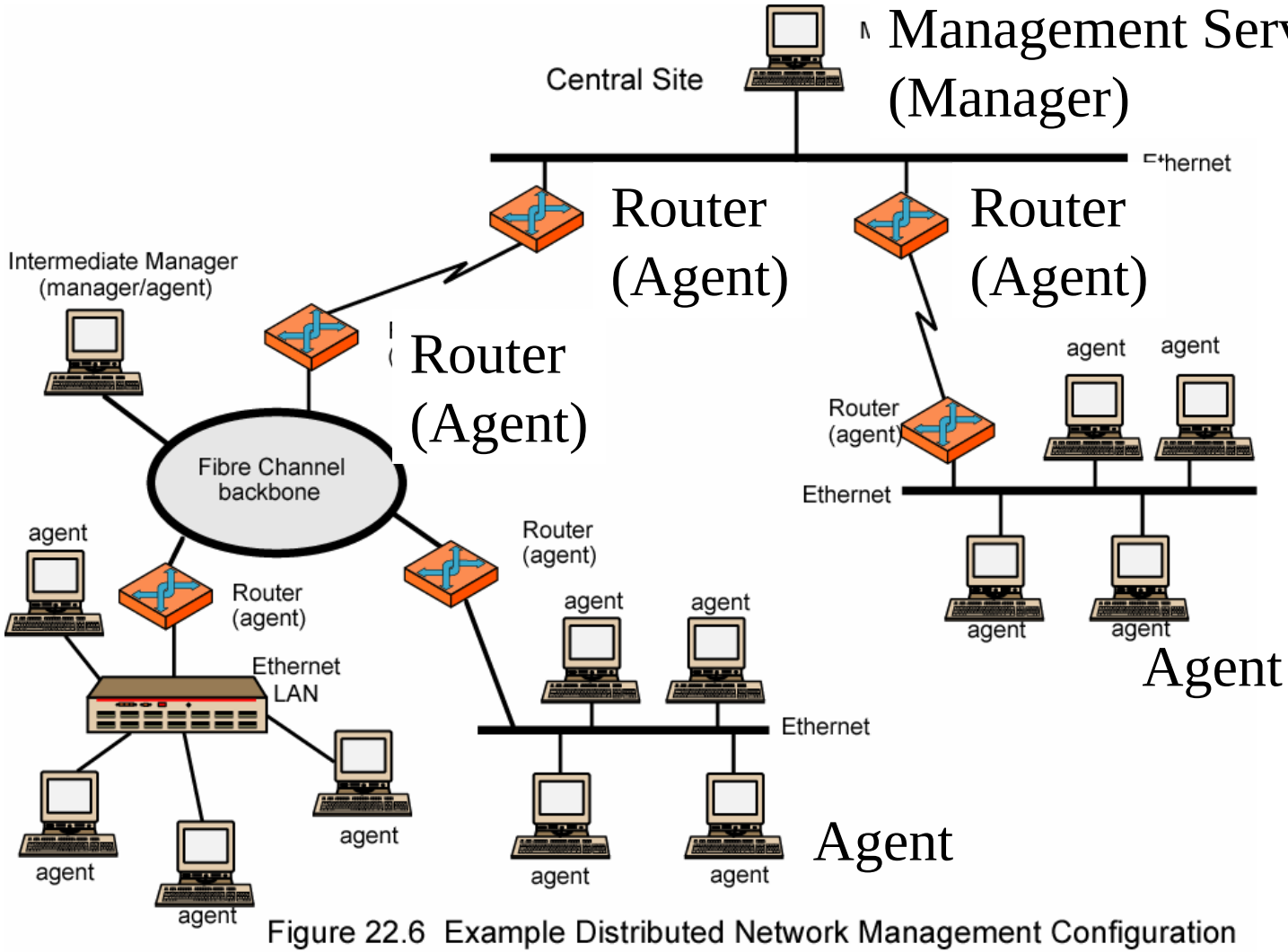
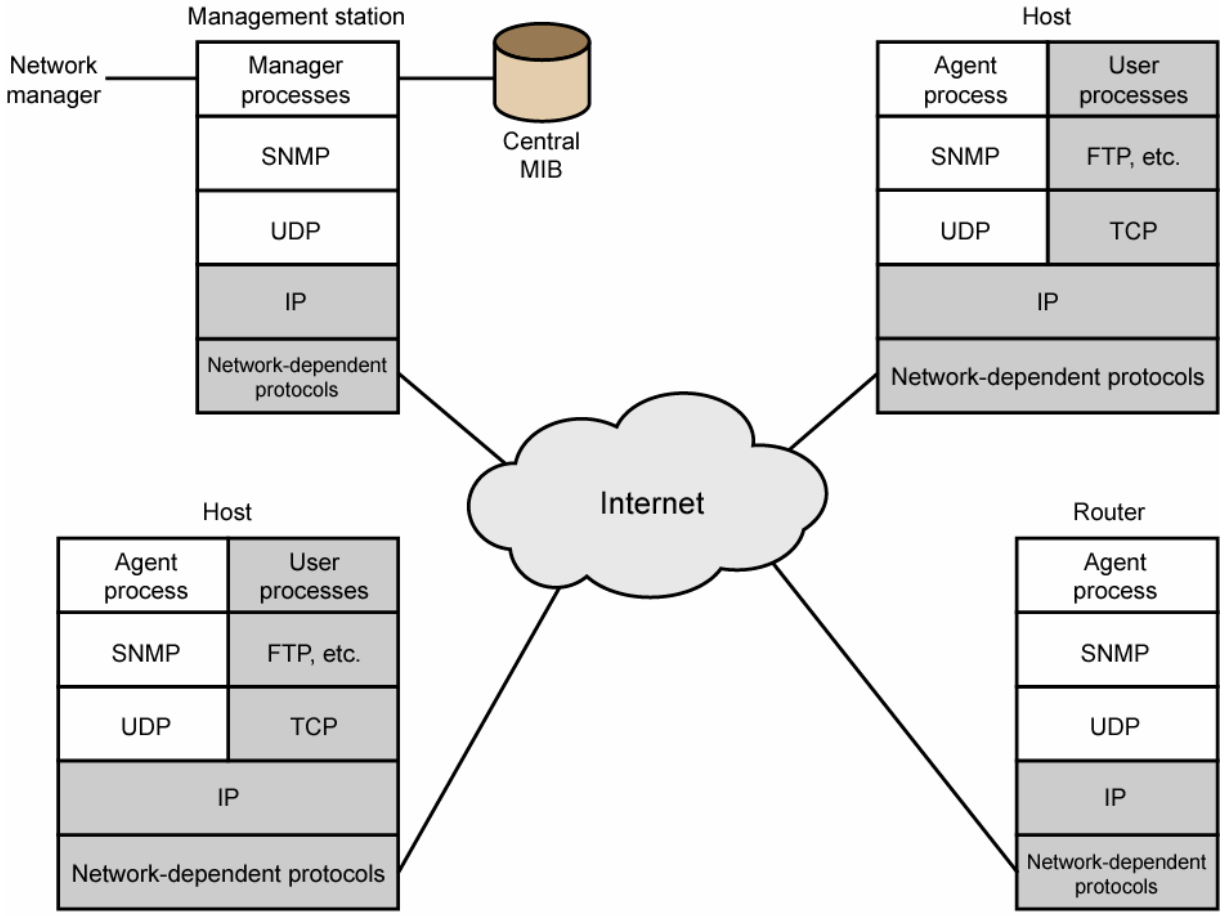


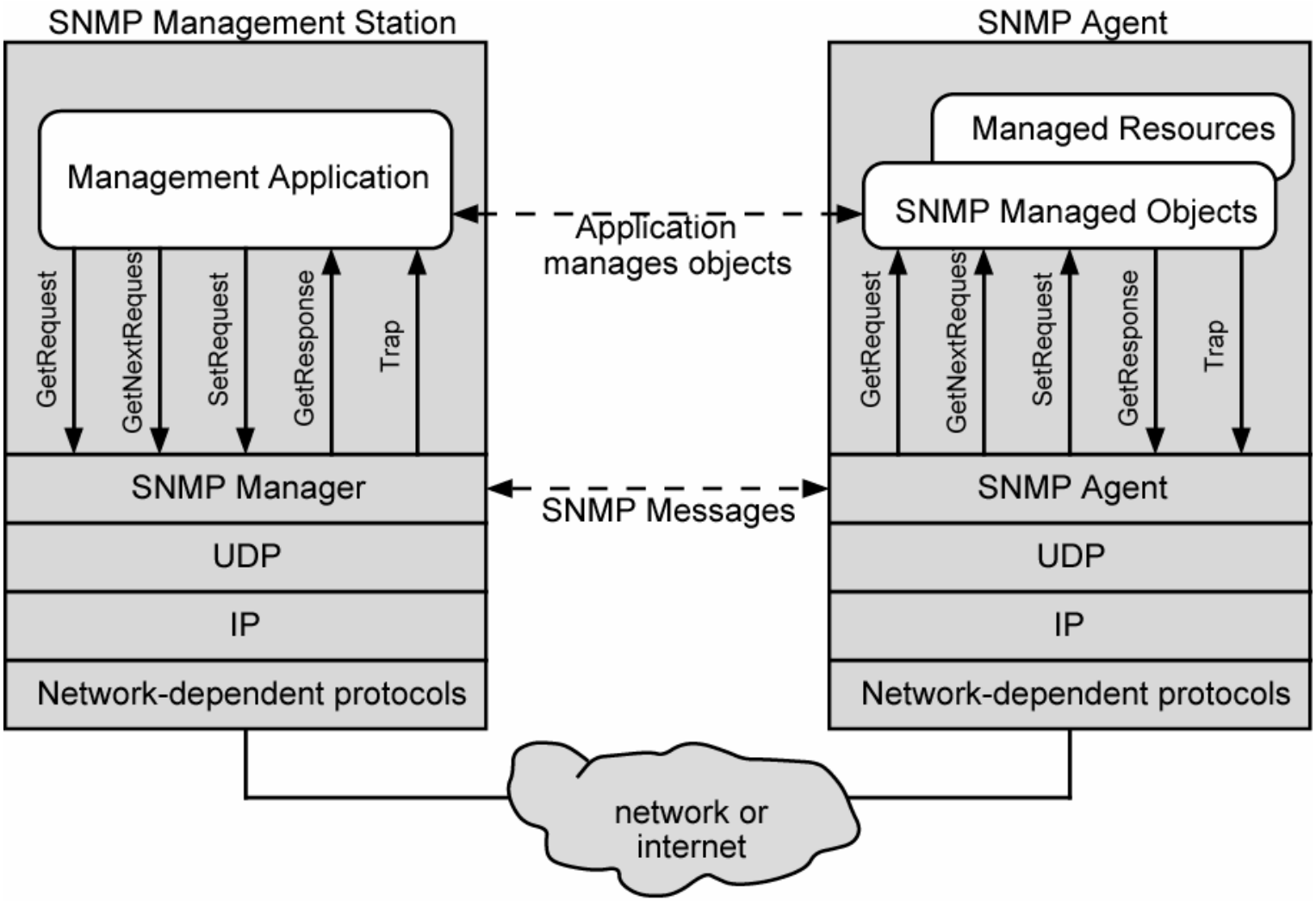
Figure 22.6 Example Distributed Network Management Configuration

SNMPv1 Configuration

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



Role of SNMP v1



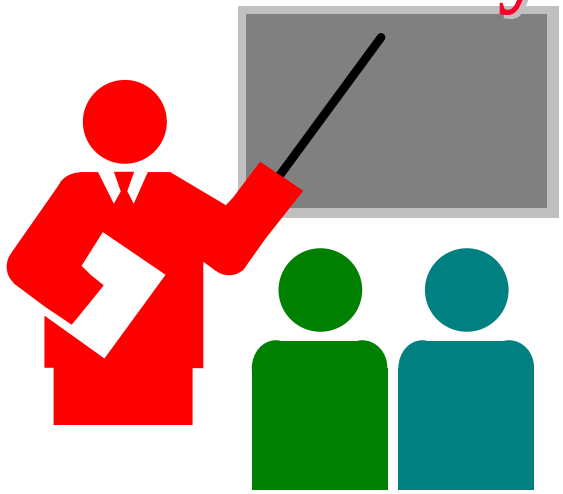
SNMPv2

- 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

Summary



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

Reading Assignment

- Read section 22.3 of Stallings' 7th edition
- Try to answer review questions 22.6 through 22.9 and problem 22.5. There is no need to submit the answers.