

# Chapter 6 Network Management

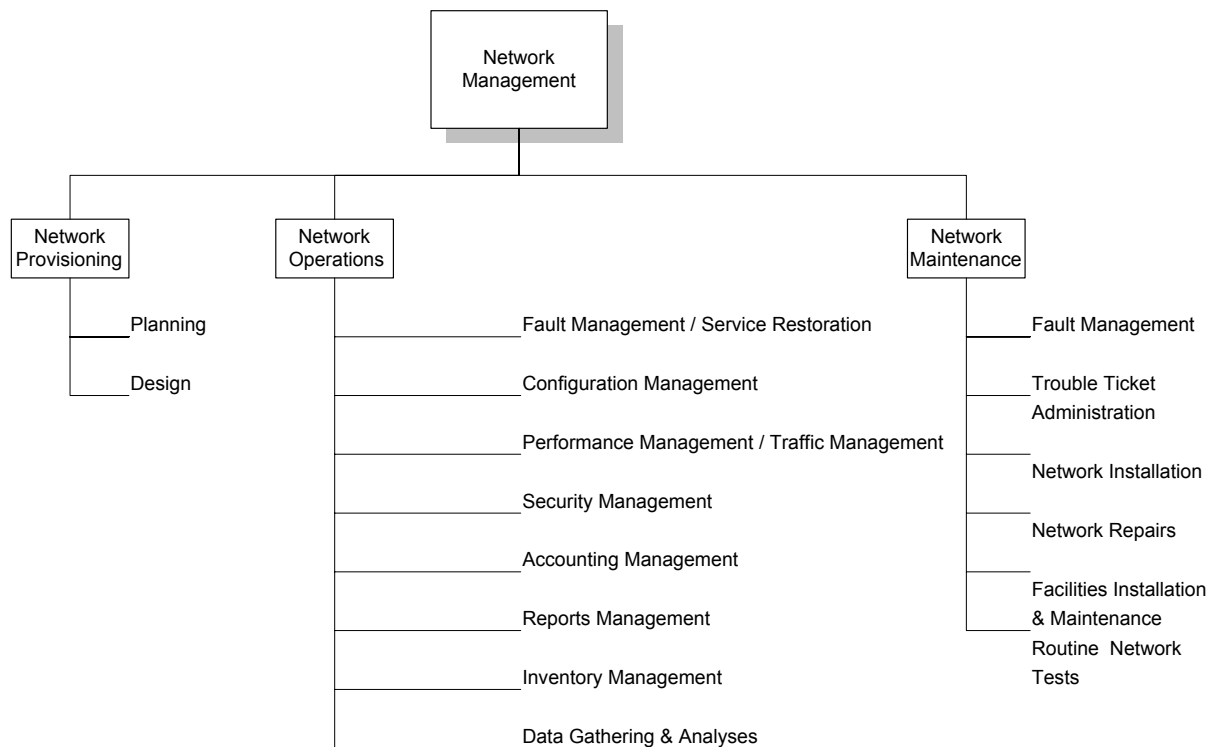
## Topics covered:

Network management standards & models. ISO Functional areas of management. Network management tools and systems. SNMP architecture & operations. Network administration.

**Note:** Most of the information in this chapter is taken from [1], and accompanying slides that are © Mani Subramanian 2000

## 6.1 Introduction

- Network Management is the management of the network resources comprising nodes (e.g., hubs, switches, routers) and links (e.g., connectivity between two nodes).
- System Management is the management of systems and system resources in the network.
- Network Management can also be defined as OAM&P (Operations, Administration, Maintenance, and Provisioning) of network and services.



I Network Management Functional Groupings

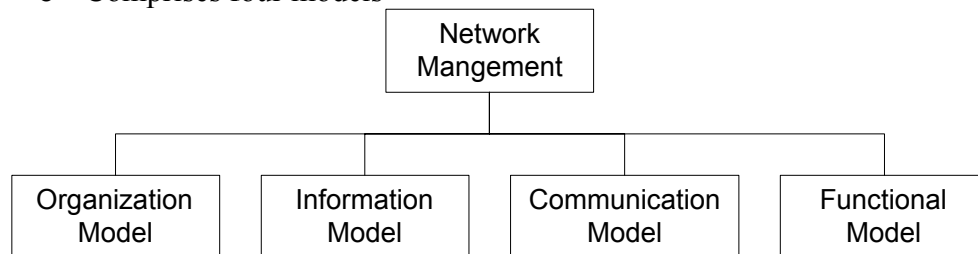
- Common Network Problems
  - Loss of connectivity
  - Duplicate IP address
  - Intermittent problems
  - Network configuration issues
  - Non-problems
  - Performance problems

## 6.2 Network Management Standards

- NM Standards:
  - OSI/CMIP: Common Management Information Protocol
  - SNMP/Internet: Simple Network Management Protocol (IETF)
  - TMN: Telecommunications Management Network (ITU-T)
  - IEEE standards
  - Web-based Management
- SNMP is the most widely used
- SNMP and CMIP:
  - Use polling methodology → additional load on the network
  - Requires dedicated workstations for the NMS (Network Management System)

## 6.3 Network Management Model

- OSI Network Management Architecture and Model
  - Most superior of all models
  - Comprises four models



**OSI Network Management Model**

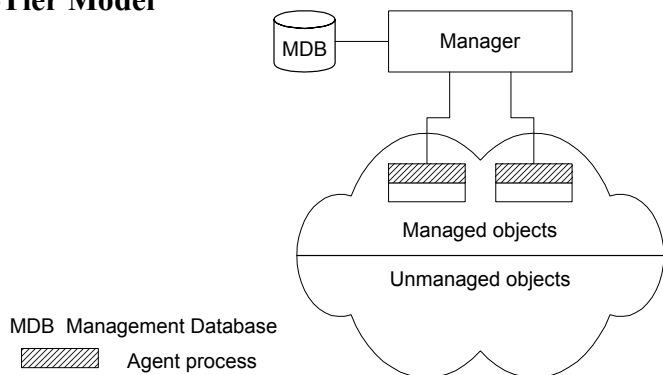
➤ SNMP Network Management Architecture and Model:

- Not defined explicitly.
- The first 3 models are similar to the OSI models.
- Addresses the functional model in terms of operations, administration, and security.

### 6.3.1 Organization Model

- Describes components of network management and their relationship
- Defines the terms: object, agent and manager
- Manager
  - Manages the managed elements
  - Sends requests to agents
  - Monitors alarms
  - Houses applications
  - Provides user interface
- Agent
  - Gathers information from objects
  - Configures parameters of objects
  - Responds to managers' requests
  - Generates alarms and sends them to managers
- Managed object
  - Network element that is managed
  - Houses management agent
  - All objects are either managed or unmanaged

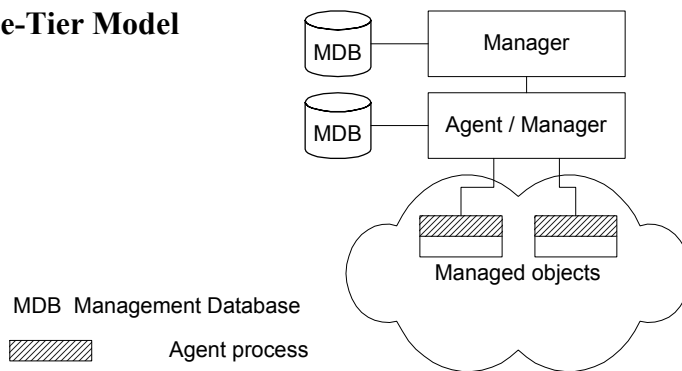
#### ❖ Two-Tier Model



**Two-Tier Network Management Organization Model**

- Agent built into network element
  - Example: Managed hub, managed router
- A manager can manage multiple elements
  - Example: Switched hub, ATM switch
- MDB is a physical database
- Unmanaged objects are network elements that are not managed - both physical (unmanaged hub) and logical (passive elements)

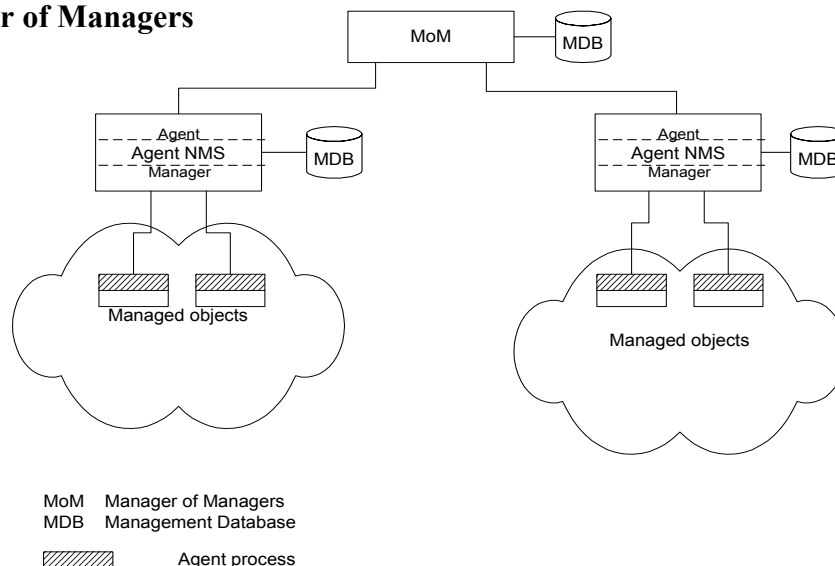
❖ **Three-Tier Model**



**Three-Tier Network Management Organization Model**

- Middle layer plays the dual role
  - Agent to the top-level manager
  - Manager to the managed objects
- Example of middle level: Remote monitoring probe/agent (RMON)

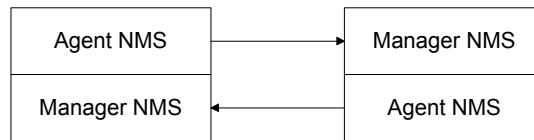
❖ **Manager of Managers**



**Network Management Organization Model with MoM**

- Agent NMS manages the domain
- MoM presents integrated view of domains
- Domain may be geographical, administrative, vendor-specific products, etc.

#### ❖ Peer NMSs



**Dual Role of Management Process**

- Dual role of both NMSs
- Network management system acts as peers
- Notice that the manager and agent functions are processes and not systems

### 6.3.2 Information Model

- Concerned with the structure and the storage of information. Similar to information stored in the library (e.g., ISBN)
- Specifies the information base to describe managed objects and their relationships
- The **Structure of Management Information (SMI)** defines for a managed object:
  - Syntax
  - Semantics
  - plus additional information such as status

#### Example

```

sysDescr: { system 1 }
  Syntax:   OCTET STRING
  Definition: "A textual description of the entity."
  Access:   read-only
  Status:   mandatory

```

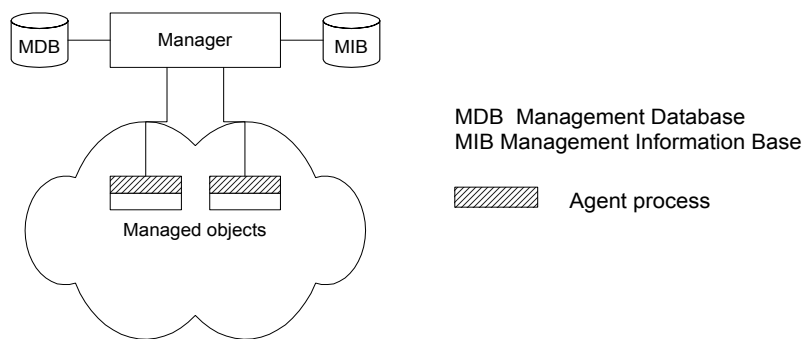
- **Management Information Base (MIB)**
  - Information base contains information about objects
  - Organized by grouping of related objects
  - Defines relationship between objects
  - It is NOT a physical database. It is a **virtual database** that is compiled into management module

➤ **MIB View and Access of an Object**

- A managed object has many attributes - its information base
- There are several operations that can be performed on the objects
- A user (manager) can view and perform only certain operations on the object by invoking the management agent
- The view of the object attributes that the agent perceives is the **MIB view**
- The operation that a user can perform is the MIB access

➤ **Management Data Base / Information Base**

- Distinction between MDB and MIB
  - MDB physical database; e.g., Oracle, Sybase
  - MIB virtual database; schema compiled into management software
- An NMS can automatically discover a managed object, such as a hub, when added to the network
- The NMS can identify the new object as hub only after the MIB schema of the hub is compiled into NMS software



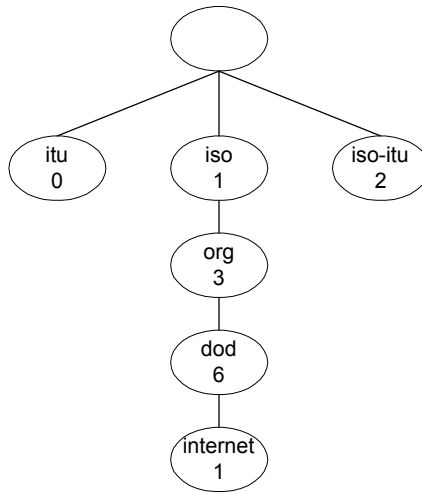
**Network Configuration with Data and Information Base**

➤ **Managed Objects can be:**

- Network elements (hardware, system): hubs, bridges, routers, transmission facilities
- Software (non-physical): programs, algorithms
- Administrative information: contact person, name of group of objects (IP group)

### 6.3.2.1 Management Information Tree (MIT)

- Managed objects are uniquely defined by a tree structure specified by the OSI model.

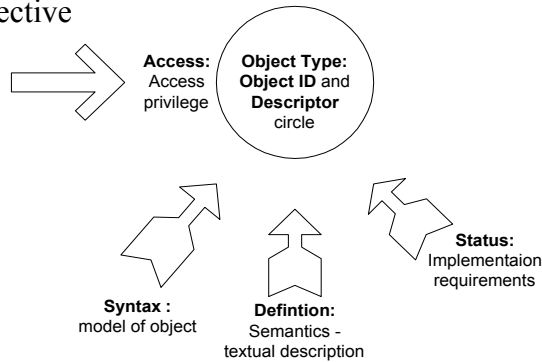


**OSI Management Information Tree**

- Each node is a managed object (e.g., the Internet is designated as 1.3.6.1)
  - All Internet-managed objects start with 1.3.6.1

### 6.3.2.2 Managed Objects

- Internet Perspective



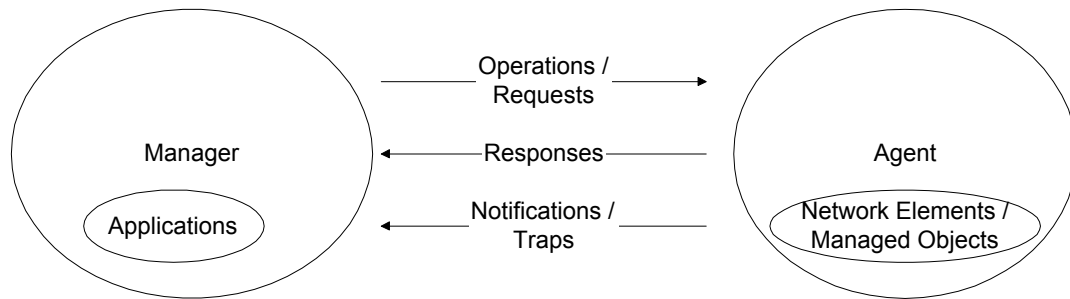
a) Internet Perspective

- Internet specifications for the object “Packet Counter”

Characteristics	Example
<i>Object type</i>	PktCounter
<i>Syntax</i>	Counter
<i>Access</i>	Read-only
<i>Status</i>	Mandatory
<i>Description</i>	Counts number of packets

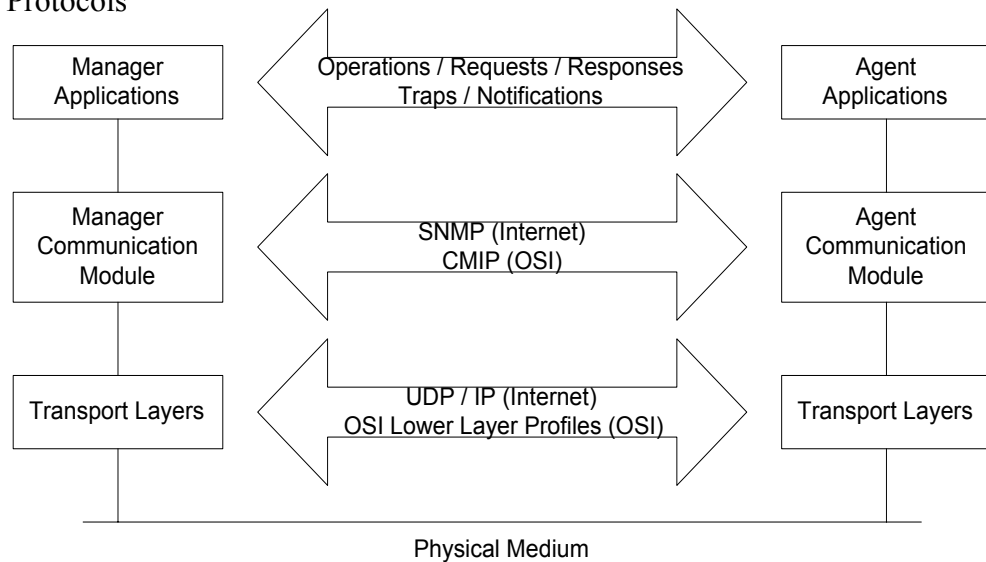
### 6.3.3 Communication Model

- Addresses the way information is exchanged between systems (agents/managers)



**Management Message Communication Model**

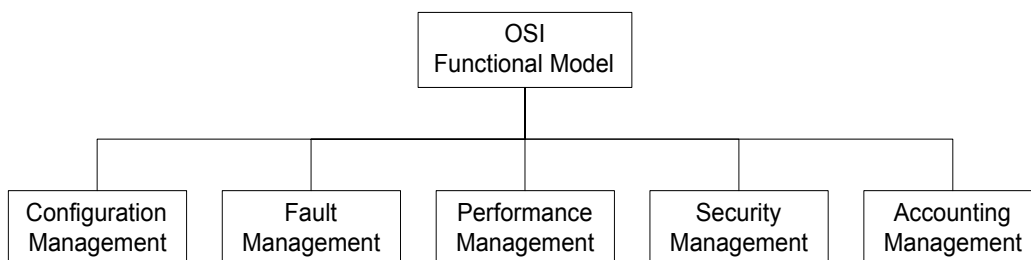
- Transfer Protocols



**Management Communication Transfer Protocols**

### 6.3.4 Functional Model

- Addresses the user-oriented applications
- Formally specified in the OSI model as follows:





### 6.3.4.1 Configuration Management (CM)

- Basic functionality
  - Set and change network configuration and component parameters
  - Set up alarm thresholds
- Network Provisioning
  - Provisioning of network resources: design, installation and maintenance
- Inventory Management
  - Equipment
  - Facilities
  - Database Considerations
- Network Topology
  - Manual
  - Auto-discovery by NMS using
    - Broadcast *ping*
    - ARP table in devices
  - Views
    - Physical
    - Logical (e.g., VLANs)

### 6.3.4.2 Fault Management (FM)

- Summary
  - Detection and isolation of failures in network
  - Trouble ticket administration
- Fault is a failure of a network component
- Results in loss of connectivity
- Fault management involves a 5-step process:
  - Fault detection (trouble ticket generated)
    - Polling
    - Traps: *linkDown*, *egpNeighborLoss*
  - Fault location
    - Detect all components failed and trace down the tree topology to the source
    - Fault isolation by network and SNMP tools
    - Use artificial intelligence / correlation techniques
  - Restoration of service (has higher priority)
  - Identification of root cause of the problem
  - Problem resolution (trouble ticket closed)

### 6.3.4.3 Performance Management (PM)

- Monitor performance of network
- Tools (e.g., analyzers)
- Performance Metrics
  - Macro-level: throughput, response time, availability, reliability
  - Micro-level: bandwidth, utilization, error rate, peak load, average load
- Data Monitoring and Problem Isolation
  - Normal behavior
  - Abnormal behavior (e.g., excessive collisions, high packet loss, etc)
  - Manual and automatic clearing of alarms
- Performance Statistics
  - Traffic statistics
  - Error statistics
  - Used in
    - QoS tracking
    - Performance tuning
    - Validation of SLA (Service Level Agreement)
    - Trend analysis
    - Facility planning
    - Functional accounting

### 6.3.4.4 Security Management (SM)

- Security threats
  - Modification of information
  - Masquerade
  - Message stream modification
  - Disclosure
- Secure communication
  - Integrity protection
  - Authentication validation
- Policies and Procedures
- Resources to prevent security breaches
  - Firewalls (e.g., packet filtering using a TCP/UDP port address)
  - Cryptography (encryption)
  - Authentication (e.g., data integrity & data origin)
  - Authorization (e.g., read, read-write, no-access)

### 6.3.4.5 Accounting Management (AM)

- Functional accounting of network usage
- Least developed
- Usage of resources
- Identification of hidden cost of IT usage

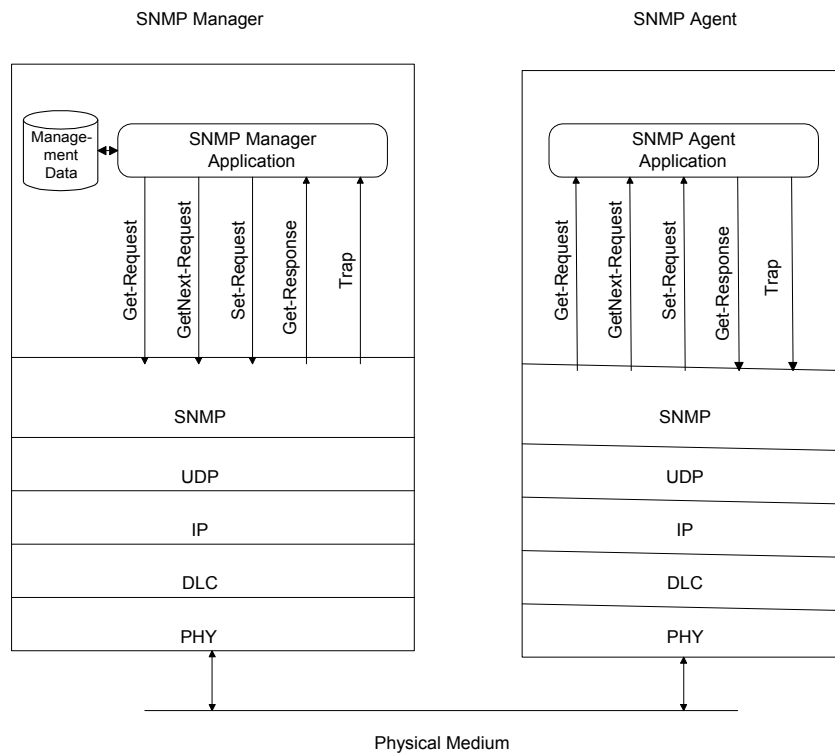
## 6.4 SNMPv1: Communication Model

An SNMP-based Network Management System consists of 3 main elements:

- 
- 
- 

### 6.4.1 SNMP Architecture

- Five SNMP messages, three from manager and two from agent.

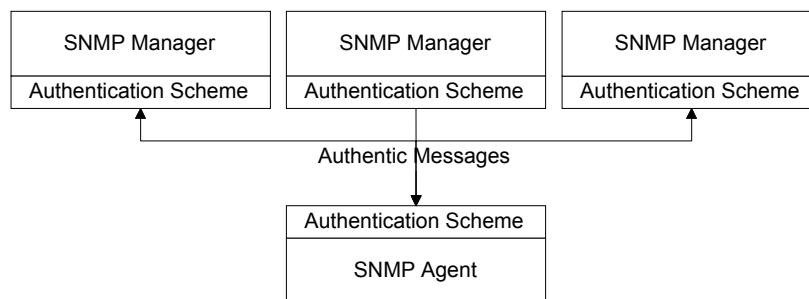


SNMP Network Management Architecture

## 6.4.2 Administrative Model

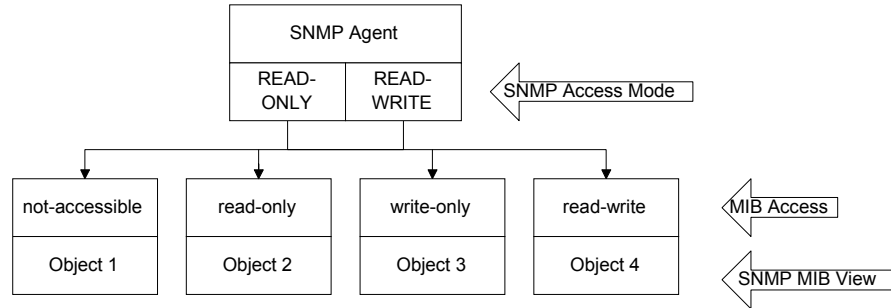
- Based on community profile and policy
- SNMP Entities:
  - SNMP application entities
    - Reside in management stations and network elements
    - Manager and agent
  - SNMP protocol entities
    - Communication processes (PDU handlers)
    - Peer processes that support application entities

### 6.4.2.1 SNMP Community



- Security in SNMPv1 is community-based
- Authentication scheme is a filter module in manager and agent (e.g., common community name)
- Community: Pairing of two application entities
- Community name: String of octets
- Two applications in the same community communicate with each other
- Application could have multiple community names
- Communication is not secured in SNMPv1 - no encryption

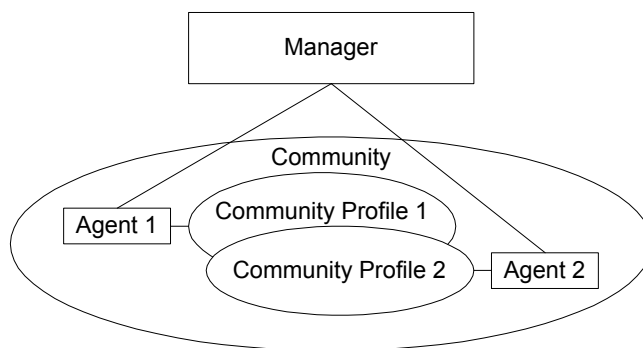
### 6.4.2.2 SNMP Community Profile



- SNMP MIB view
  - An agent is programmed to view only a subset of managed objects of a network element
- SNMP access mode
  - Each community name is assigned an access mode: read-only and read-write
- Community profile: SNMP MIB view + SNMP access mode
- Operations on an object determined by community profile and the access mode of the managed object
- Total of four access privileges
- Some objects, such as table and table entry are non-accessible
- Most objects available for the public community are read-only.

### 6.4.2.3 Access Policy

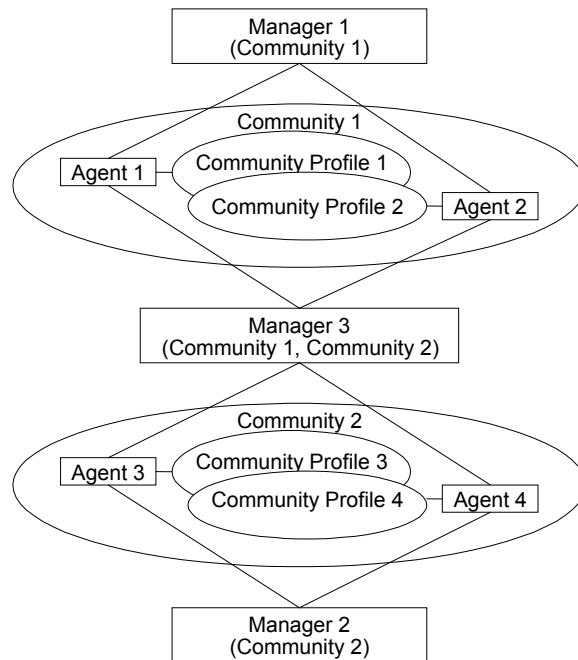
- The SNMP access policy defines the administrative model
- SNMP community paired with SNMP community profile is SNMP access policy



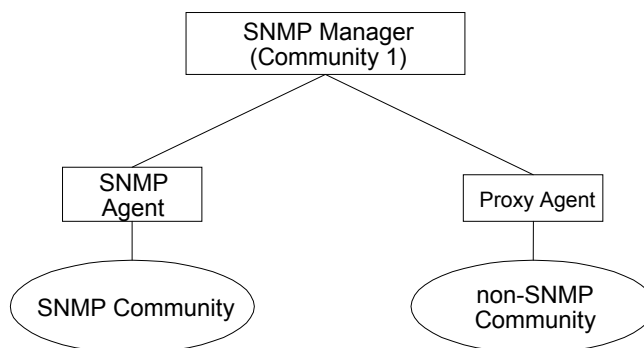
- Manager manages Community 1 and 2 network components via Agents 1 and 2
- Agent 1 has only view of Community Profile 1, e.g. Cisco components
- Agent 2 has only view of Community Profile 2, e.g. 3Com components
- Manager has total view of both Cisco and 3Com components

#### 6.4.2.4 Generalized Administration Model

- Manager 1 manages community 1, manager 2 community 2, and manager 3 (MoM) both communities 1 and 2



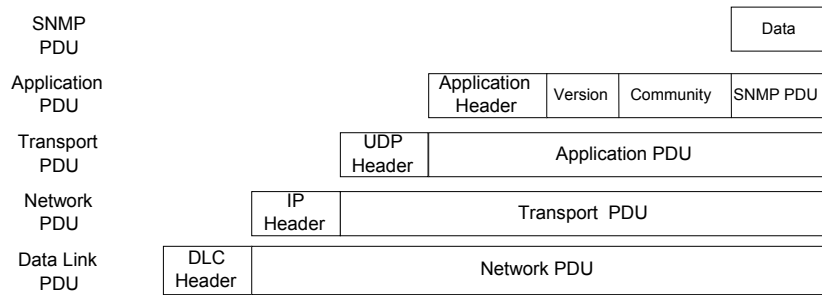
#### 6.4.2.5 Proxy Access Policy



- Proxy agent enables non-SNMP community elements to be managed by an SNMP manager.
- An SNMP MIB is created to handle the non-SNMP objects

## 6.4.3 SNMP Protocol Specifications

### 6.4.3.1 Protocol Entities



**Encapsulated SNMP Message**

- Protocol entities support application entities
- Communication between remote peer processes
- Message consists of
  - Version identifier
  - Community name
  - Protocol Data Unit
- Message encapsulated and transmitted

### 6.4.3.2 Get and Set PDU

PDU Type	RequestID	Error Status	Error Index	VarBind 1 name	VarBind 1 value	...	VarBind n name	VarBind n value
----------	-----------	--------------	-------------	----------------	-----------------	-----	----------------	-----------------

- VarBindList: multiple instances of VarBind pairs
- PDU Type:
 

<b>get-request</b>	<b>[0]</b>
<b>get-next-request</b>	<b>[1]</b>
<b>get-response</b>	<b>[2]</b>
<b>set-request</b>	<b>[3]</b>
<b>trap</b>	<b>[4]</b>
- Error in Response
 

```

      ErrorStatus ::=
      INTEGER {
        noError(0),
        tooBig(1),
        noSuchName(2),
        badValue(3),
        readOnly(4),
        genErr(5) }
      
```
- Error Index: No. of VarBind where the first error occurred

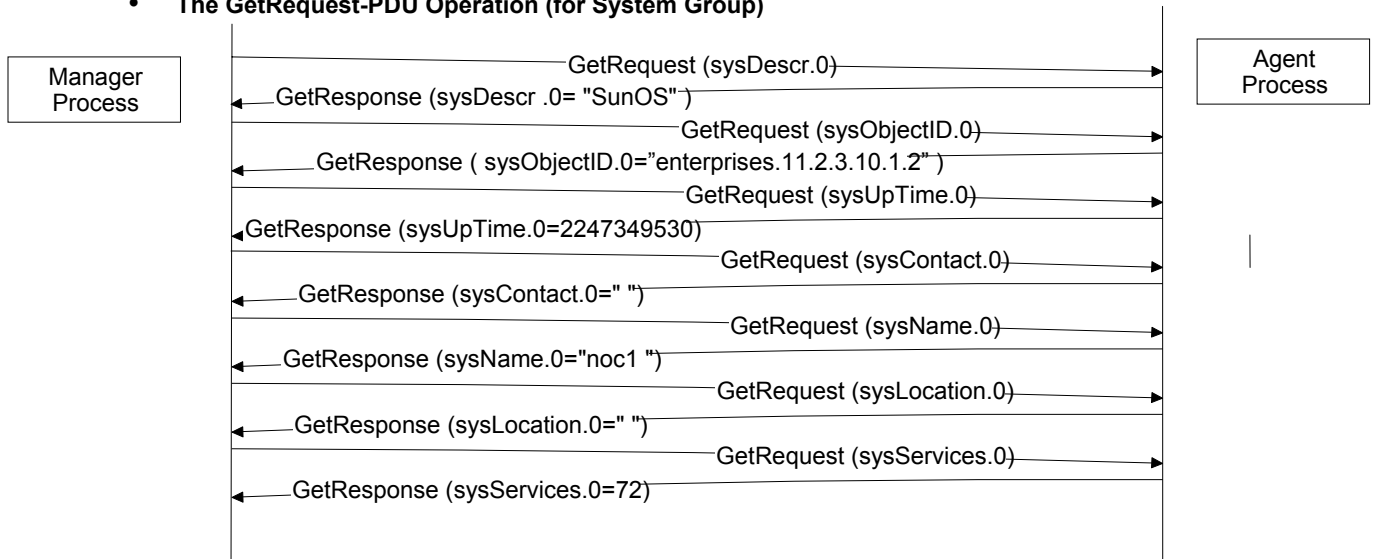
### 6.4.3.3 Trap PDU

PDU Type	Enterprise	Agent Address	Generic Trap Type	Specific Trap Type	Timestamp	VarBind 1 name	VarBind 1 value	...	VarBind n name	VarBind n value
----------	------------	---------------	-------------------	--------------------	-----------	----------------	-----------------	-----	----------------	-----------------

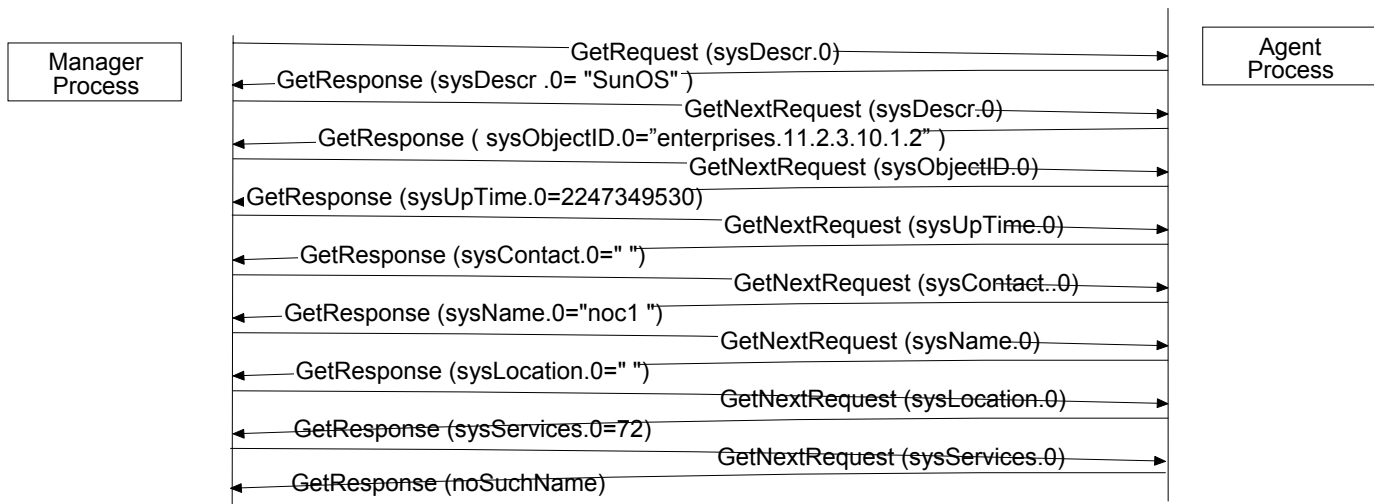
- Enterprise and agent address pertain to the system generating the trap
- Seven generic traps specified by enumerated INTEGER
- The enterprise-specific trap is used by the private organizations to define their device-specific traps. If the Generic Trap type value is 6, the trap is enterprise specific and is defined in a private MIB.
- Timestamp indicates elapsed time since last re-initialization

### 6.4.4 SNMP Operations

- **The GetRequest-PDU Operation (for System Group)**

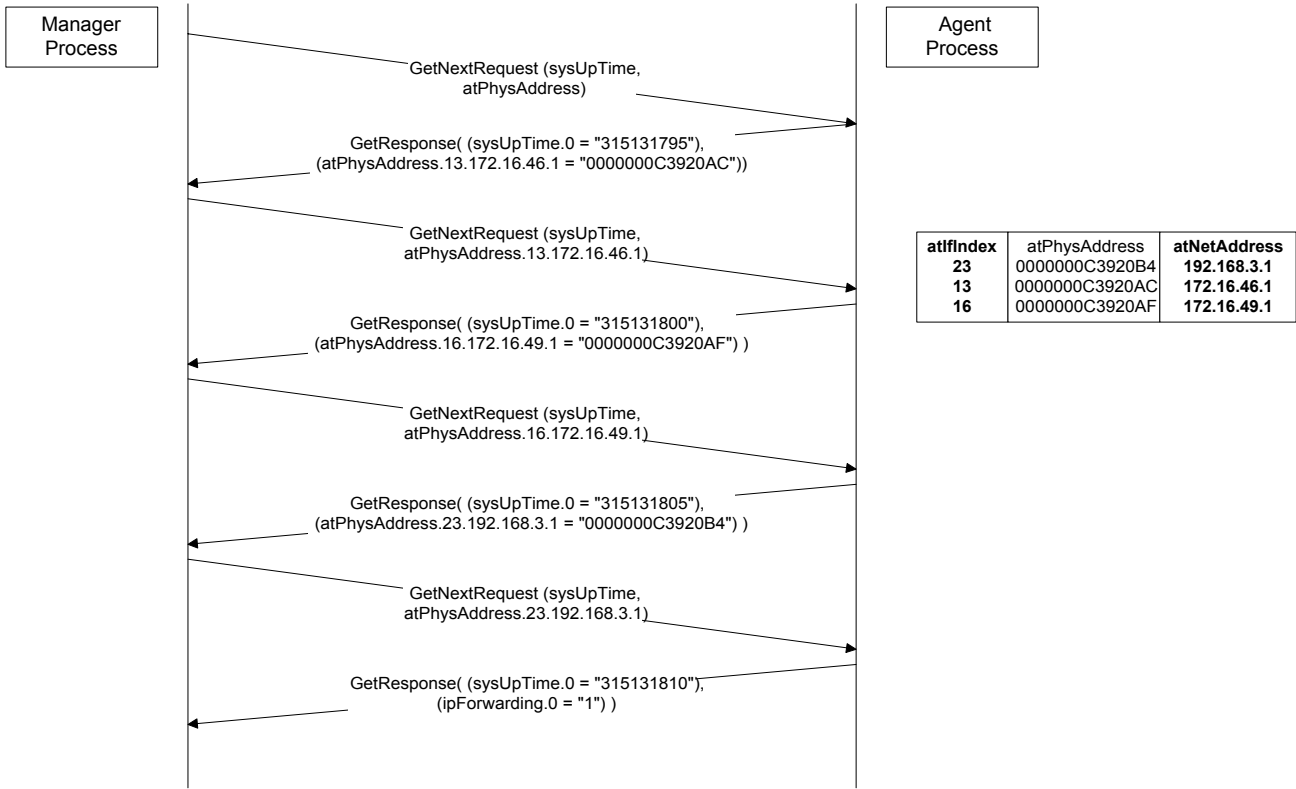


- **The GetNextRequest-PDU Operation (for System Group)**





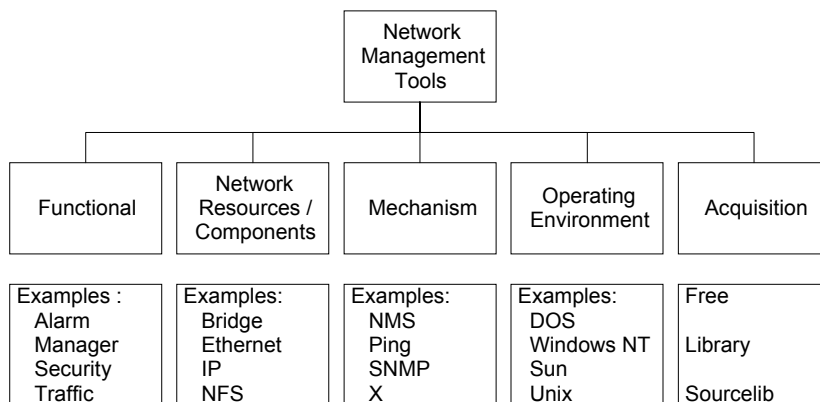
- **GetNextRequest with Indices (faster method)**
  - Uses Lexicographic Order to traverse the MIB subtree
  - A GetNextRequest Example with Indices



GetNextRequest Example with Indices

## 6.5 SNMP Tools & Systems

### 6.5.1 Tools Catalog



NOC Tool Categories (RFC 1470)

## 6.5.2 Network Software Tools

- Status monitoring tools
- Traffic monitoring tools
- Route monitoring tools

### 6.5.2.1 Network Status Monitoring Tools

NAME	OPERATING SYSTEM	DESCRIPTION
ifconfig	UNIX	Obtains and configures networking interface parameters and status
ping	UNIX Windows	Checks the status of node / host
nslookup	UNIX Windows NT	Looks up DNS for name / IP address translation
dig	UNIX	Queries DNS server
host	UNIX	Displays information on Internet hosts / domains

### 6.5.2.2 Network Traffic Monitoring Tools

Name	Operating System	Description
ping	UNIX Windows	Used for measuring roundtrip packet loss
bing	UNIX	Measures point-to-point bandwidth of a link
etherfind	UNIX	Inspects Ethernet packets
snoop	UNIX	Captures and inspects network packets
tcpdump	UNIX	Dumps traffic on a network
getethers	UNIX	Acquires all host addresses of an Ethernet LAN segment
iptrace	UNIX	Measures performance of gateways

### 6.5.2.3 Network Routing Tools

Name	Operating System	Description
netstat	UNIX	Displays the contents of various network related data structures
arp rarp	UNIX, Windows 95/x/00NT	Displays and modifies the Internet-to Ethernet address translation tables
tracert tracert	UNIX Windows	Traces route to a destination with routing delays

### **6.5.3 SNMP MIB Tools**

- SNMP MIB Browsers
- SNMP command-line tools

#### **6.5.3.1 SNMP MIB Browsers**

- User friendly tools
- May have a GUI
- Specify hostname or IP address & request information on a specific MIB object, MIB group or entire MIB
- Response returns object id(s) and value(s)

#### **6.5.3.2 SNMP Command-Line Tools**

- snmpget
- snmpgetnext
- snmpset
- snmptrap
- snmpwalk
- snmpnetstat

## **6.6 References**

1. “Network Management - Principles and Practice” by Mani Subramanian, 2000
2. “TCP/IP Illustrated, Volume 1 - The protocols” by Richard Stevens