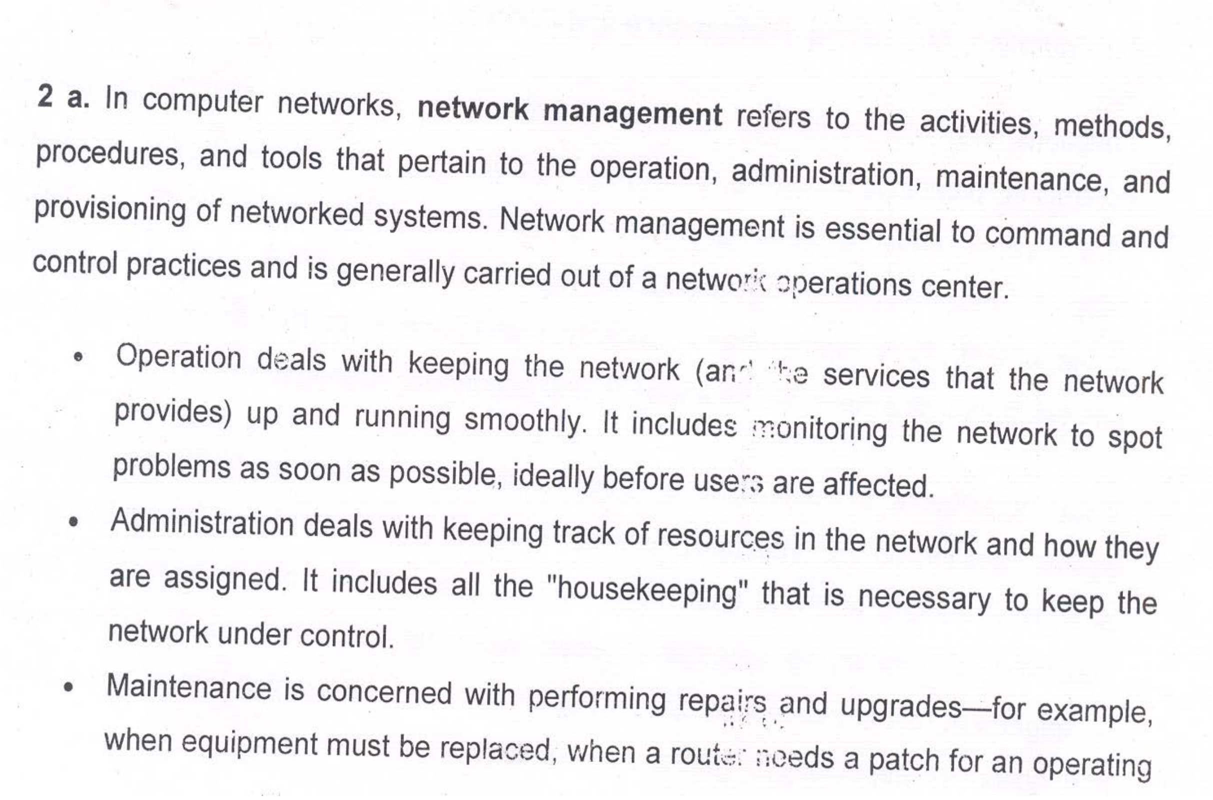
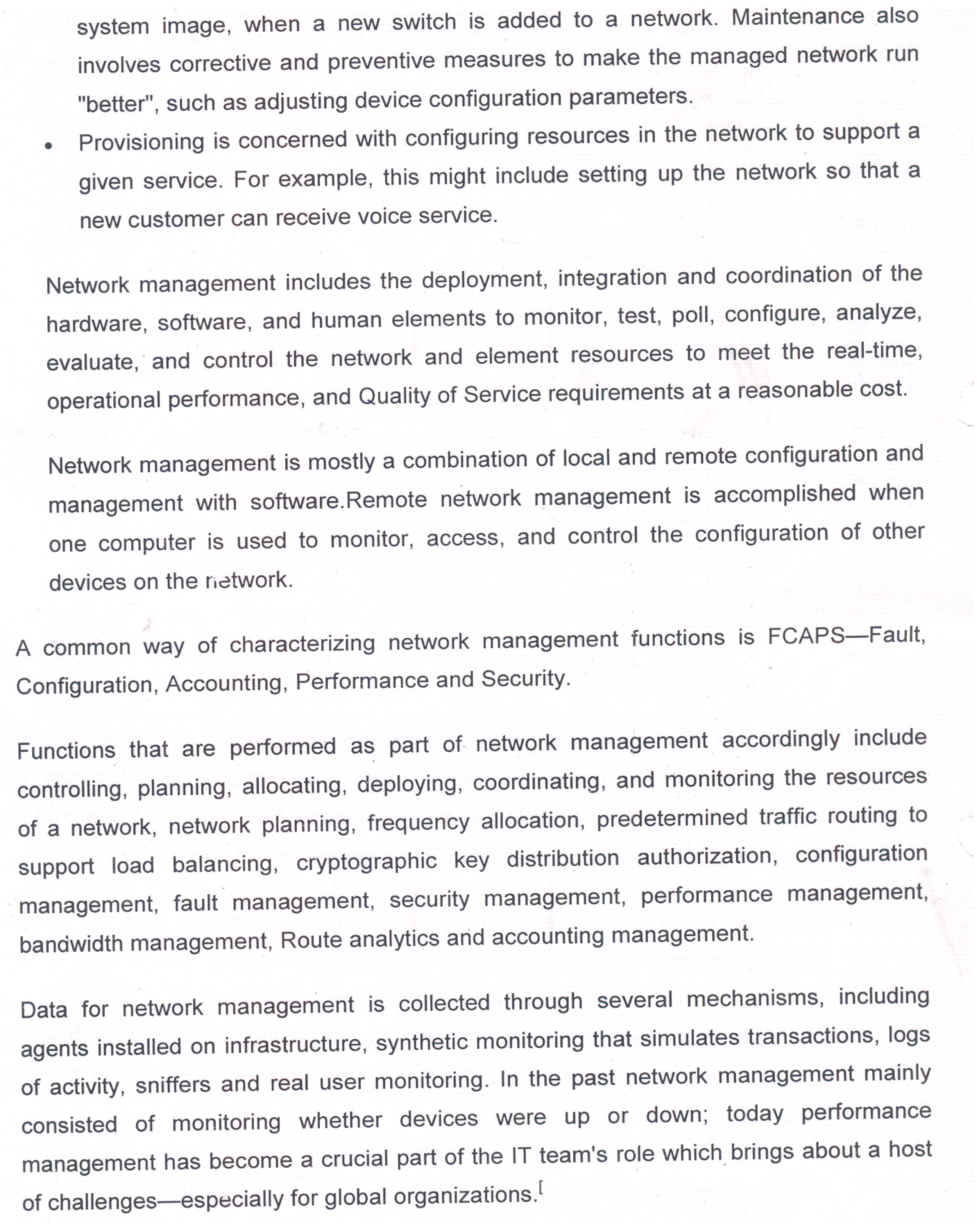
Q.2 a.What do you mean by Network Management? Explain.



2 a. In computer networks, **network management** refers to the activities, methods, procedures, and tools that pertain to the operation, administration, maintenance, and provisioning of networked systems. Network management is essential to command and control practices and is generally carried out of a network operations center.

- Operation deals with keeping the network (and the services that the network provides) up and running smoothly. It includes monitoring the network to spot problems as soon as possible, ideally before users are affected.
- Administration deals with keeping track of resources in the network and how they are assigned. It includes all the "housekeeping" that is necessary to keep the network under control.
- Maintenance is concerned with performing repairs and upgrades—for example, when equipment must be replaced, when a router needs a patch for an operating



system image, when a new switch is added to a network. Maintenance also involves corrective and preventive measures to make the managed network run "better", such as adjusting device configuration parameters.

- Provisioning is concerned with configuring resources in the network to support a given service. For example, this might include setting up the network so that a new customer can receive voice service.

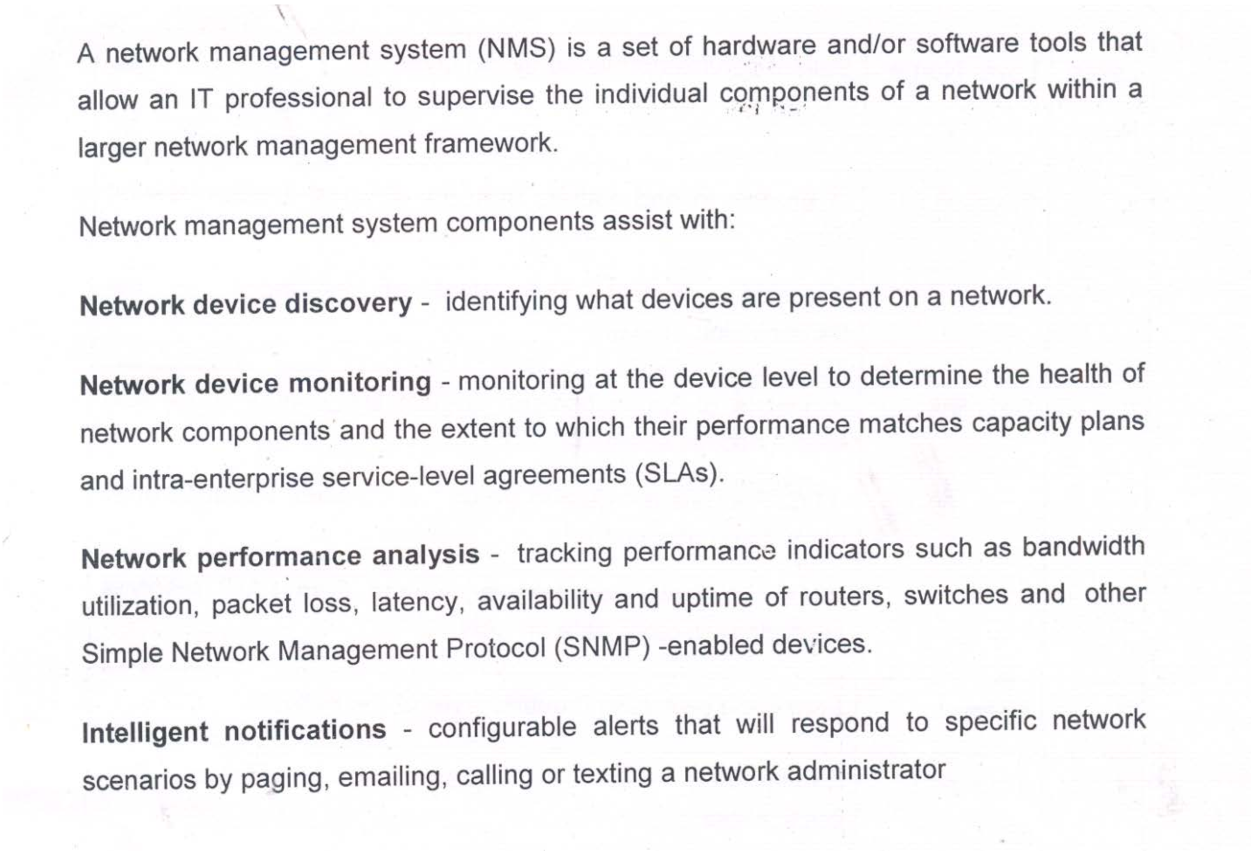
Network management includes the deployment, integration and coordination of the hardware, software, and human elements to monitor, test, poll, configure, analyze, evaluate, and control the network and element resources to meet the real-time, operational performance, and Quality of Service requirements at a reasonable cost.

Network management is mostly a combination of local and remote configuration and management with software.Remote network management is accomplished when one computer is used to monitor, access, and control the configuration of other devices on the network.

A common way of characterizing network management functions is FCAPS—Fault, Configuration, Accounting, Performance and Security.

Functions that are performed as part of network management accordingly include controlling, planning, allocating, deploying, coordinating, and monitoring the resources of a network, network planning, frequency allocation, predetermined traffic routing to support load balancing, cryptographic key distribution authorization, configuration management, fault management, security management, performance management, bandwidth management, Route analytics and accounting management.

Data for network management is collected through several mechanisms, including agents installed on infrastructure, synthetic monitoring that simulates transactions, logs of activity, sniffers and real user monitoring. In the past network management mainly consisted of monitoring whether devices were up or down; today performance management has become a crucial part of the IT team's role which brings about a host of challenges—especially for global organizations.[



A network management system (NMS) is a set of hardware and/or software tools that allow an IT professional to supervise the individual components of a network within a larger network management framework.

Network management system components assist with:

Network device discovery - identifying what devices are present on a network.

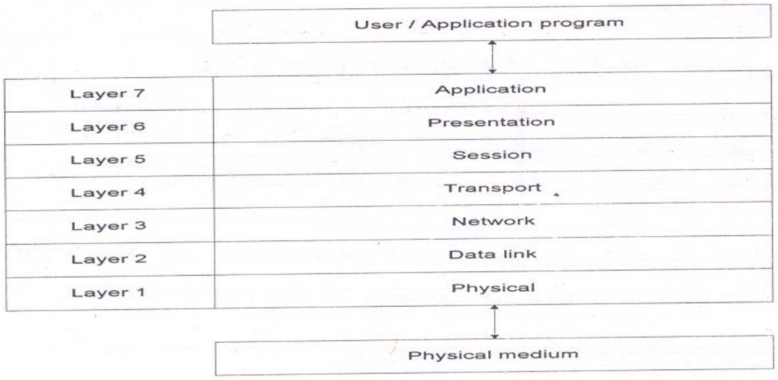
Network device monitoring - monitoring at the device level to determine the health of network components and the extent to which their performance matches capacity plans and intra-enterprise service-level agreements (SLAs).

Network performance analysis - tracking performance indicators such as bandwidth utilization, packet loss, latency, availability and uptime of routers, switches and other Simple Network Management Protocol (SNMP) -enabled devices.

Intelligent notifications - configurable alerts that will respond to specific network scenarios by paging, emailing, calling or texting a network administrator

b. Explain functions of various layers of OSI protocol. Illustrate with the help of a diagram.

2 b.

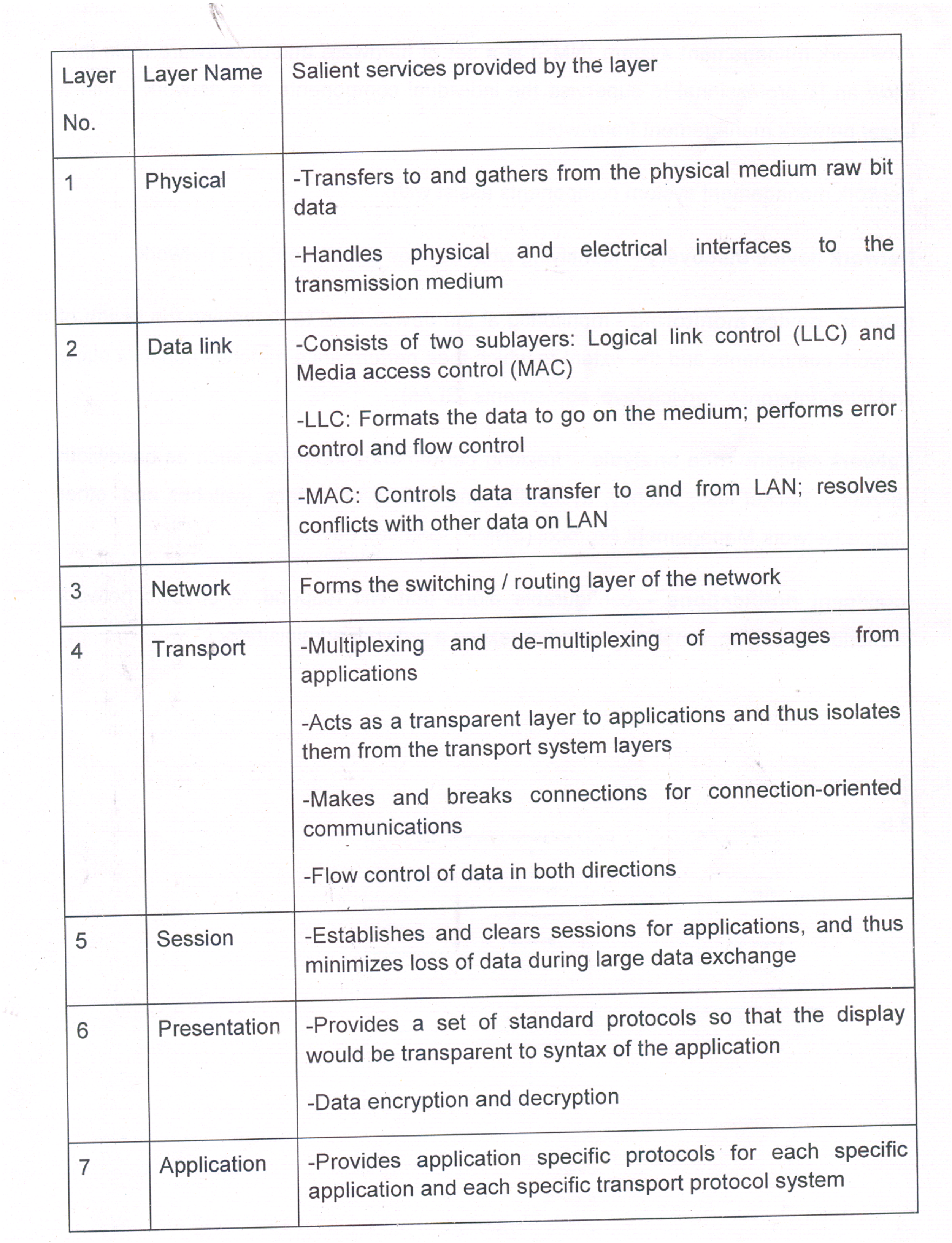


User / Application program

Layer 7	Application
Layer 6	Presentation
Layer 5	Session
Layer 4	Transport
Layer 3	Network
Layer 2	Data link
Layer 1	Physical

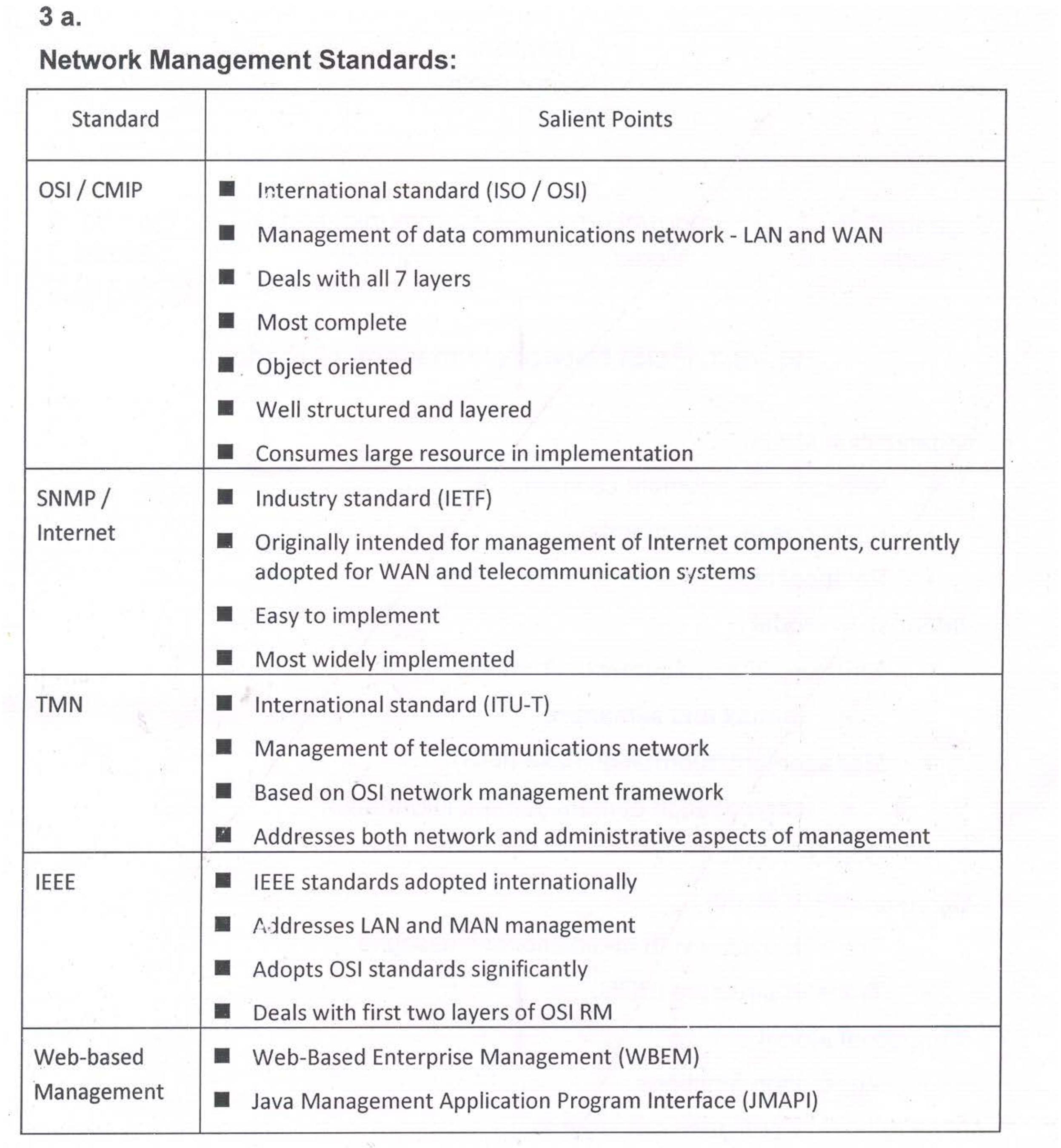
Physical medium

Figure 1.12 OSI Protocol Layers



Layer No.	Layer Name	Salient services provided by the layer
1	Physical	-Transfers to and gathers from the physical medium raw bit data -Handles physical and electrical interfaces to the transmission medium
2	Data link	-Consists of two sublayers: Logical link control (LLC) and Media access control (MAC) -LLC: Formats the data to go on the medium; performs error control and flow control -MAC: Controls data transfer to and from LAN; resolves conflicts with other data on LAN
3	Network	Forms the switching / routing layer of the network
4	Transport	-Multiplexing and de-multiplexing of messages from applications -Acts as a transparent layer to applications and thus isolates them from the transport system layers -Makes and breaks connections for connection-oriented communications -Flow control of data in both directions
5	Session	-Establishes and clears sessions for applications, and thus minimizes loss of data during large data exchange
6	Presentation	-Provides a set of standard protocols so that the display would be transparent to syntax of the application -Data encryption and decryption
7	Application	-Provides application specific protocols for each specific application and each specific transport protocol system

Q.3 a. Explain salient features of various Network Management Standards.



3 a.

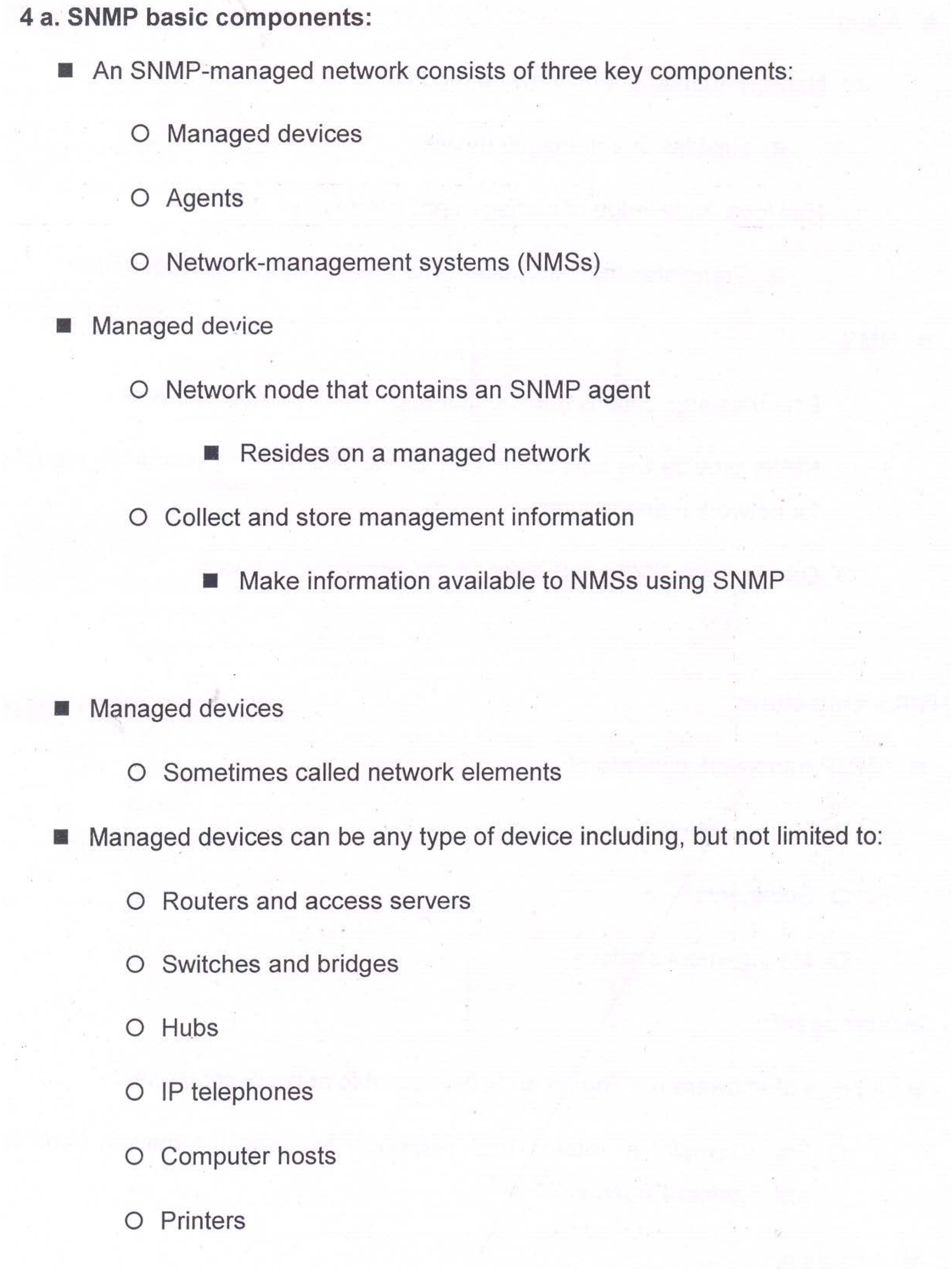
Network Management Standards:

Standard	Salient Points
OSI / CMIP	■ International standard (ISO / OSI) ■ Management of data communications network - LAN and WAN ■ Deals with all 7 layers ■ Most complete ■ Object oriented ■ Well structured and layered ■ Consumes large resource in implementation
SNMP / Internet	■ Industry standard (IETF) ■ Originally intended for management of Internet components, currently adopted for WAN and telecommunication systems ■ Easy to implement ■ Most widely implemented
TMN	■ International standard (ITU-T) ■ Management of telecommunications network ■ Based on OSI network management framework ■ Addresses both network and administrative aspects of management
IEEE	■ IEEE standards adopted internationally ■ Addresses LAN and MAN management ■ Adopts OSI standards significantly ■ Deals with first two layers of OSI RM
Web-based Management	■ Web-Based Enterprise Management (WBEM) ■ Java Management Application Program Interface (JMAPI)

b. Explain the Information model and Functional model of Network Management.

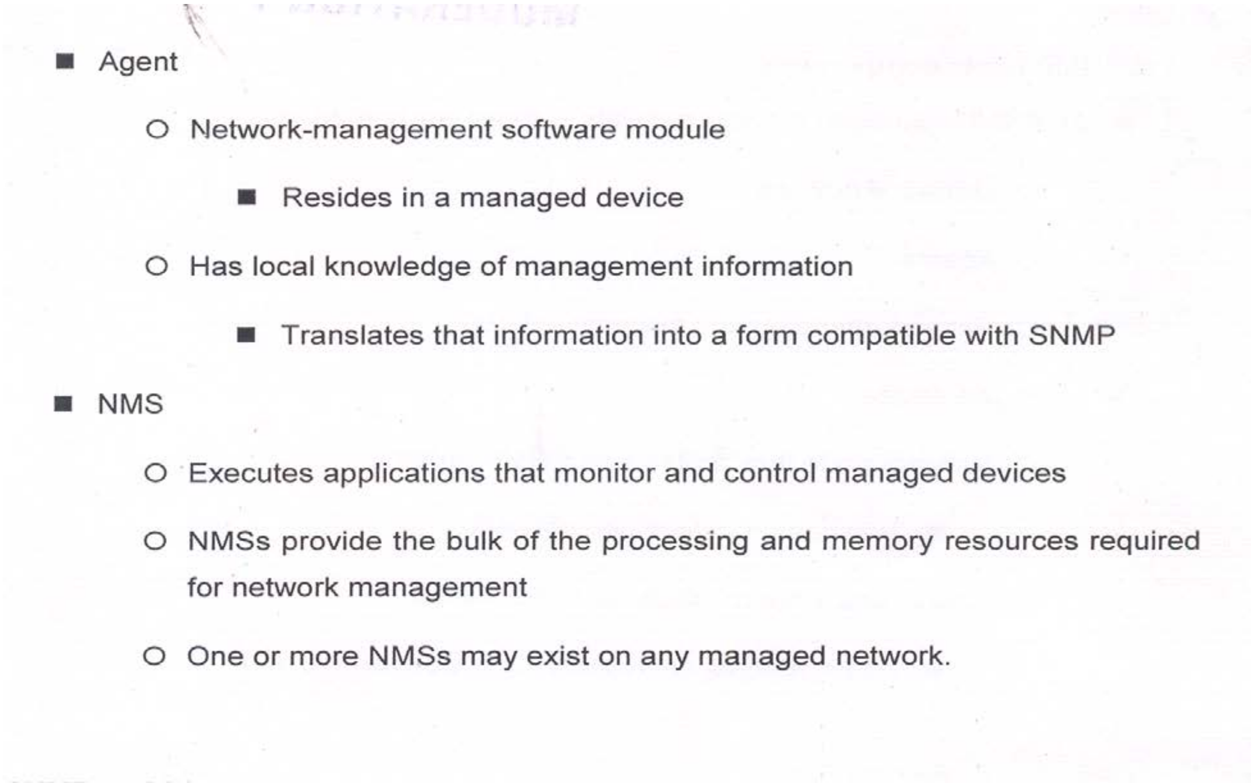
Ans Chapter 3 Page 135-138 and Pg 161-162

Q.4 a. What are the key components of SNMP managed network? Explain.



4 a. SNMP basic components:

- An SNMP-managed network consists of three key components:
  - Managed devices
  - Agents
  - Network-management systems (NMSs)
- Managed device
  - Network node that contains an SNMP agent
    - Resides on a managed network
  - Collect and store management information
    - Make information available to NMSs using SNMP
- Managed devices
  - Sometimes called network elements
- Managed devices can be any type of device including, but not limited to:
  - Routers and access servers
  - Switches and bridges
  - Hubs
  - IP telephones
  - Computer hosts
  - Printers

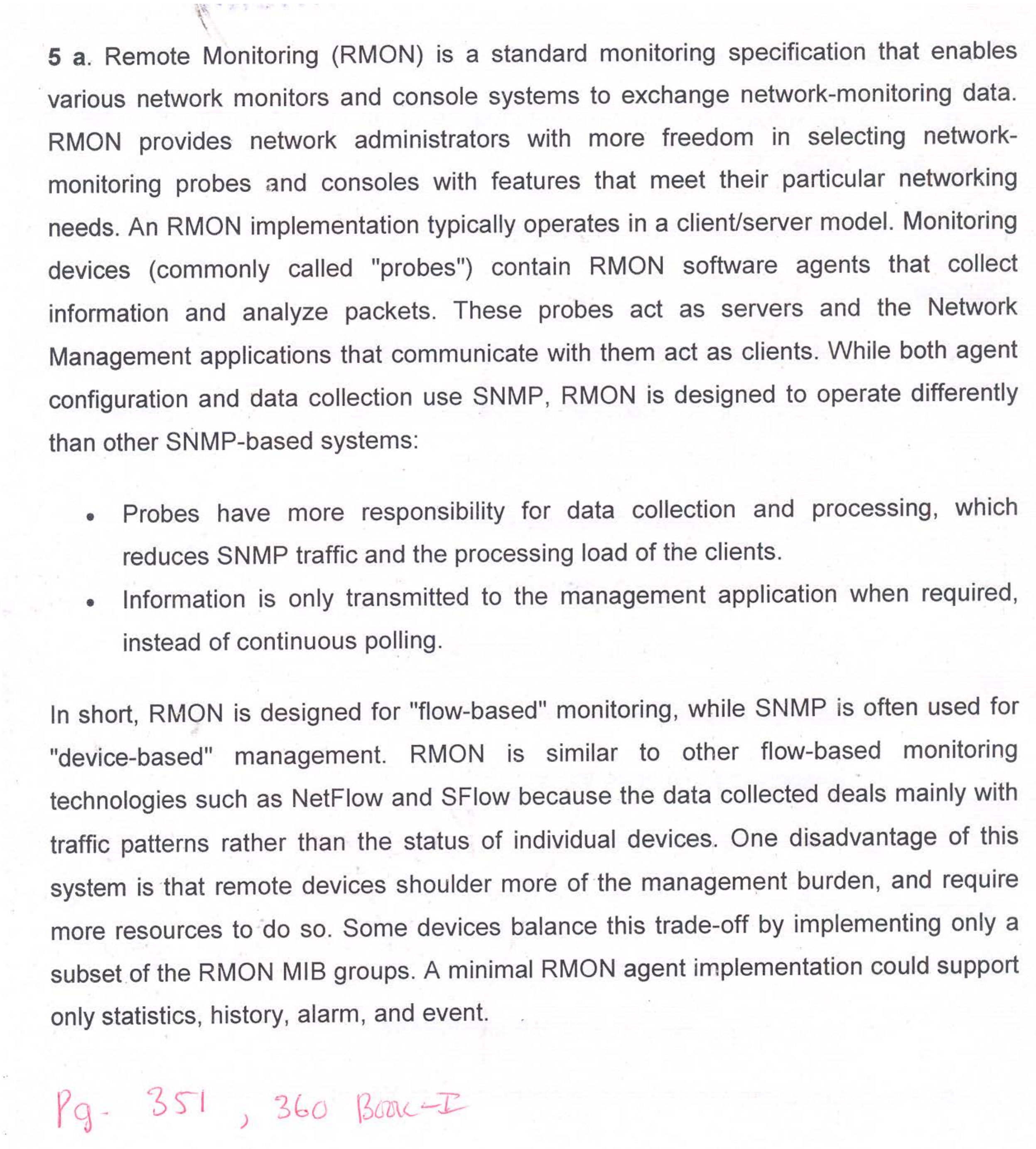


- Agent
  - ○ Network-management software module
    - Resides in a managed device
  - ○ Has local knowledge of management information
    - Translates that information into a form compatible with SNMP
- NMS
  - ○ Executes applications that monitor and control managed devices
  - ○ NMSs provide the bulk of the processing and memory resources required for network management
  - ○ One or more NMSs may exist on any managed network.

b.Explain Management Information Base of SNMPv1.

Ans Page 206-220 of book I

Q.5 a. Compare RMON1 and RMON2. Illustrate your answer by listing various goals and benefits of Remote Monitoring.



5 a. Remote Monitoring (RMON) is a standard monitoring specification that enables various network monitors and console systems to exchange network-monitoring data. RMON provides network administrators with more freedom in selecting network-monitoring probes and consoles with features that meet their particular networking needs. An RMON implementation typically operates in a client/server model. Monitoring devices (commonly called "probes") contain RMON software agents that collect information and analyze packets. These probes act as servers and the Network Management applications that communicate with them act as clients. While both agent configuration and data collection use SNMP, RMON is designed to operate differently than other SNMP-based systems:

- Probes have more responsibility for data collection and processing, which reduces SNMP traffic and the processing load of the clients.
- Information is only transmitted to the management application when required, instead of continuous polling.

In short, RMON is designed for "flow-based" monitoring, while SNMP is often used for "device-based" management. RMON is similar to other flow-based monitoring technologies such as NetFlow and SFlow because the data collected deals mainly with traffic patterns rather than the status of individual devices. One disadvantage of this system is that remote devices shoulder more of the management burden, and require more resources to do so. Some devices balance this trade-off by implementing only a subset of the RMON MIB groups. A minimal RMON agent implementation could support only statistics, history, alarm, and event.

Pg- 351, 360 Book-I

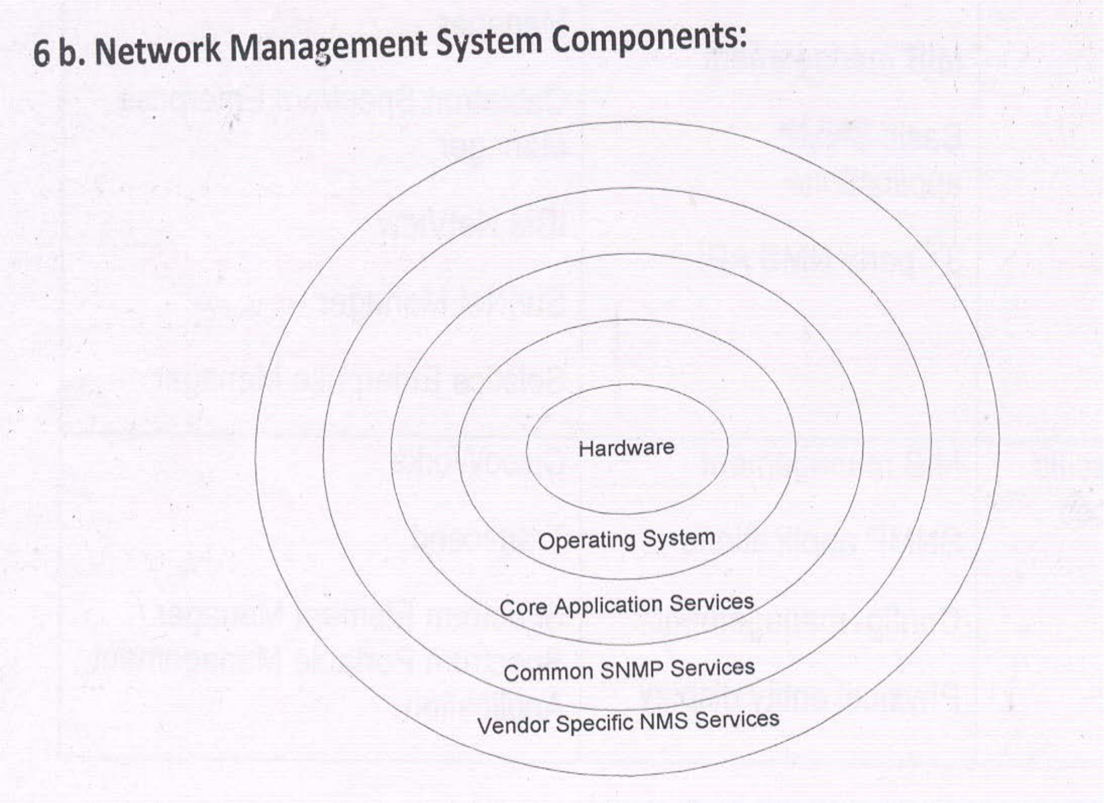
b. Explain SNMP Community Profile and SNMP access policy.

Ans Page 230-234 of book I

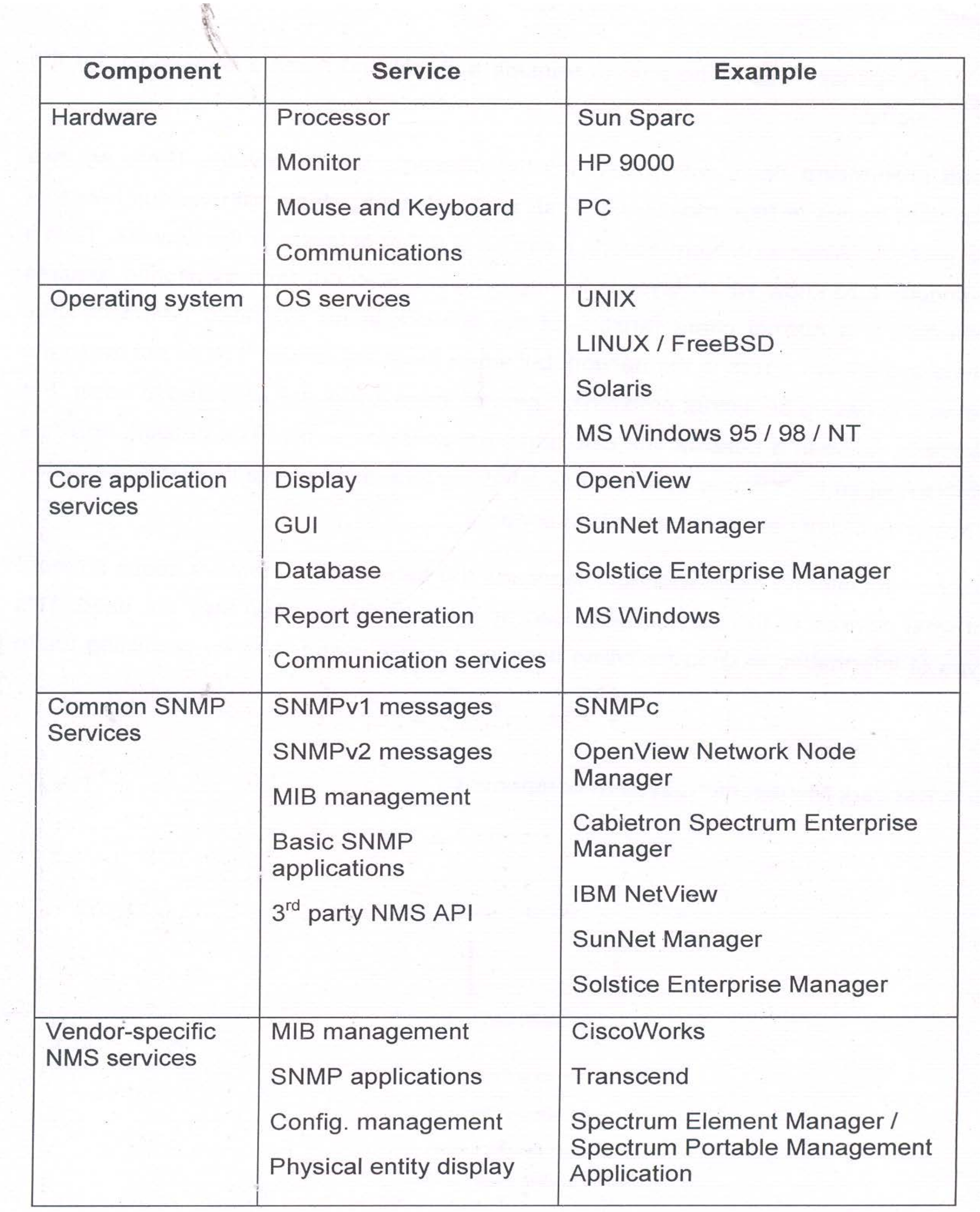
Q.6 a. Explain in detail the concept of Network Management tools.

Ans Page 483-498 of book I

b. Explain briefly the following:
(i) Commercial network management system
(ii) Enterprise management solutions

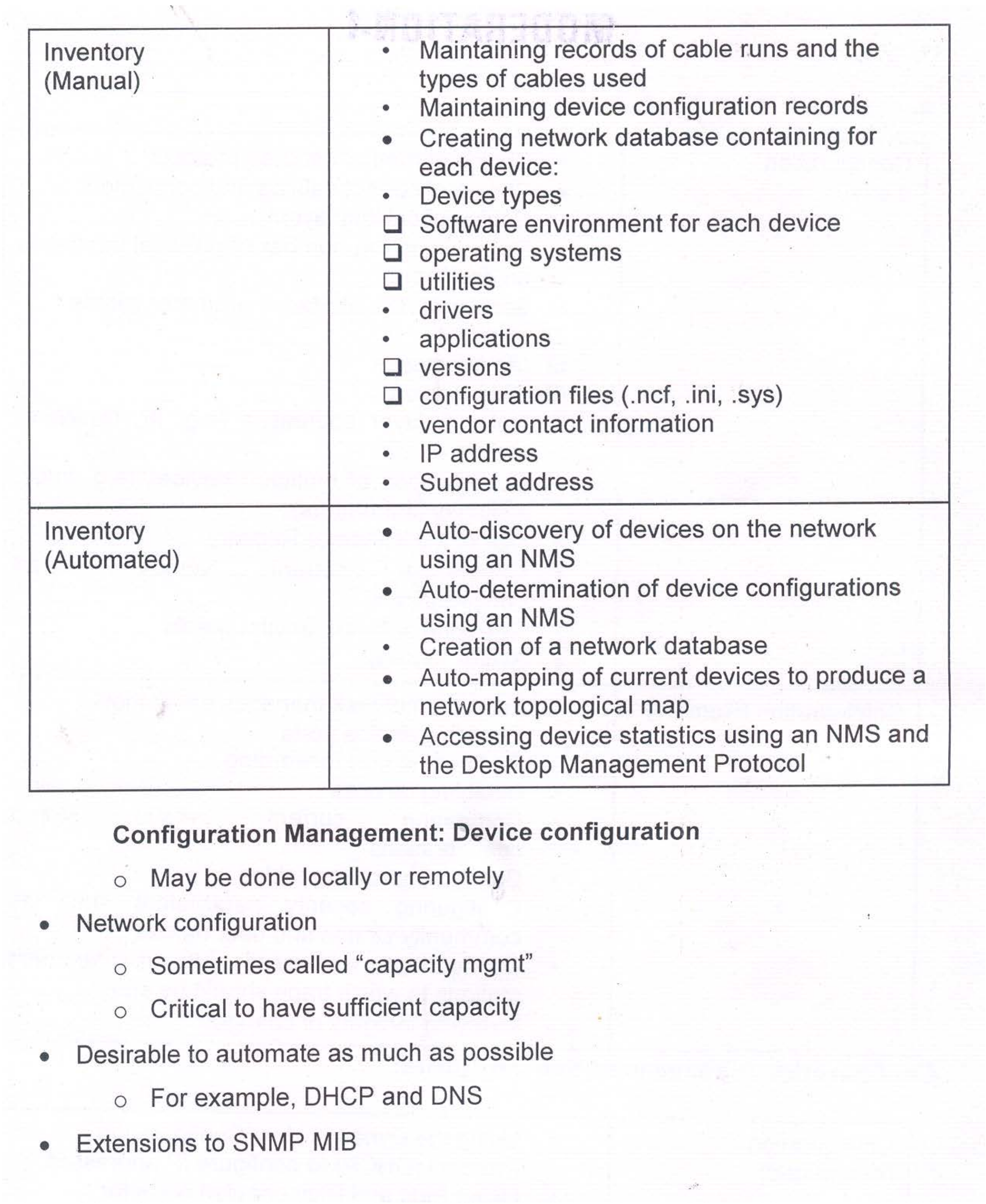


6 b. Network Management System Components:



Component	Service	Example
Hardware	Processor Monitor Mouse and Keyboard Communications	Sun Sparc HP 9000 PC
Operating system	OS services	UNIX LINUX / FreeBSD Solaris MS Windows 95 / 98 / NT
Core application services	Display GUI Database Report generation Communication services	OpenView SunNet Manager Solstice Enterprise Manager MS Windows
Common SNMP Services	SNMPv1 messages SNMPv2 messages MIB management Basic SNMP applications 3rd party NMS API	SNMPc OpenView Network Node Manager Cabietron Spectrum Enterprise Manager IBM NetView SunNet Manager Solstice Enterprise Manager
Vendor-specific NMS services	MIB management SNMP applications Config. management Physical entity display	CiscoWorks Transcend Spectrum Element Manager / Spectrum Portable Management Application

Q.7 a. Explain the significance of Event Correlation Techniques in network management. List various Event Correlation Techniques. Explain any two.



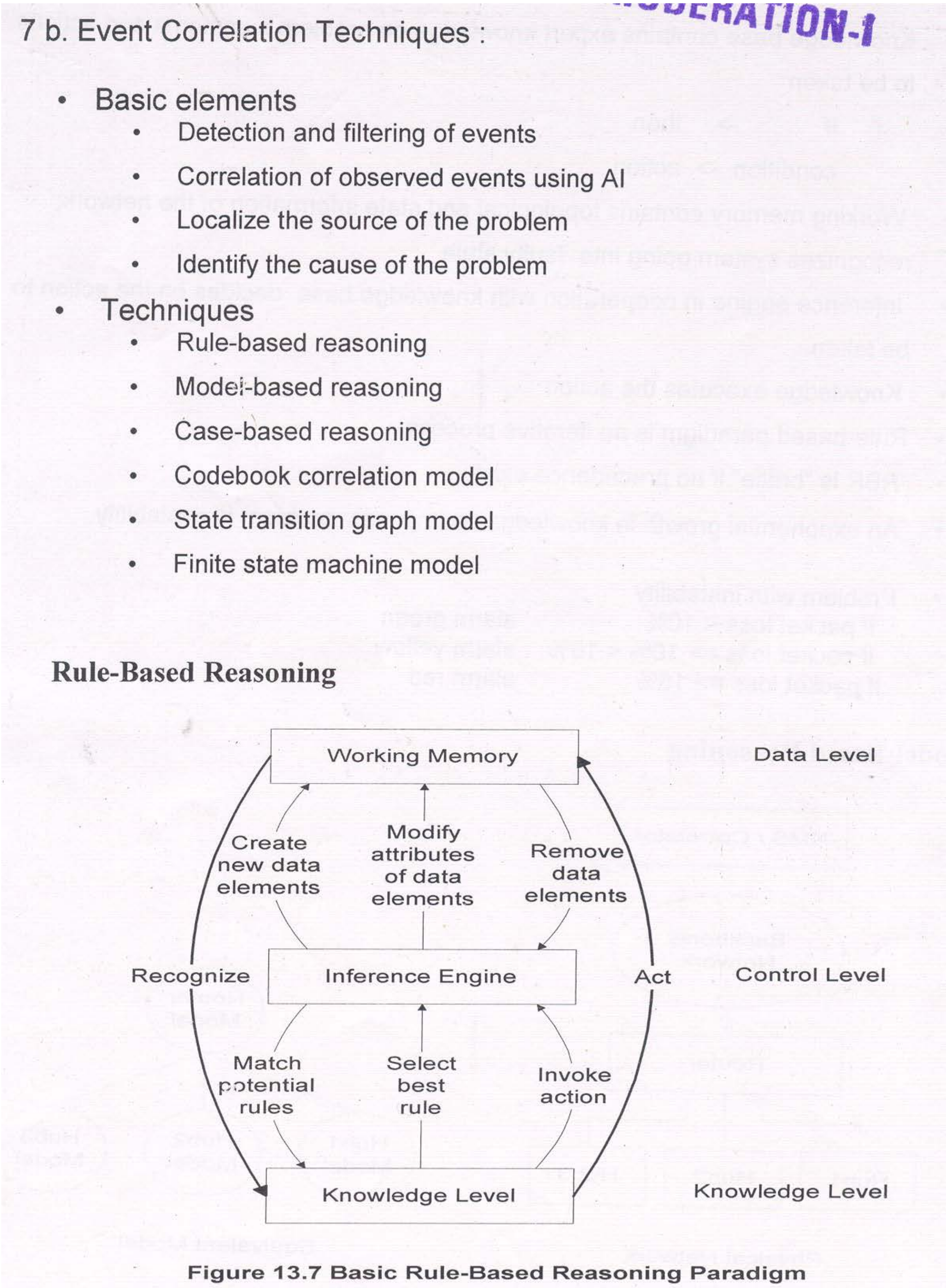
Inventory (Manual)	• Maintaining records of cable runs and the types of cables used • Maintaining device configuration records • Creating network database containing for each device: • Device types □ Software environment for each device □ operating systems □ utilities • drivers • applications □ versions □ configuration files (.ncf, .ini, .sys) • vendor contact information • IP address • Subnet address
Inventory (Automated)	• Auto-discovery of devices on the network using an NMS • Auto-determination of device configurations using an NMS • Creation of a network database • Auto-mapping of current devices to produce a network topological map • Accessing device statistics using an NMS and the Desktop Management Protocol

Configuration Management: Device configuration

- May be done locally or remotely

- Network configuration
  - Sometimes called "capacity mgmt"
  - Critical to have sufficient capacity
- Desirable to automate as much as possible
  - For example, DHCP and DNS
- Extensions to SNMP MIB

b. What do you understand by Configuration Management? Explain.



DERATION-1

7 b. Event Correlation Techniques :

- Basic elements
  - Detection and filtering of events
  - Correlation of observed events using AI
  - Localize the source of the problem
  - Identify the cause of the problem
- Techniques
  - Rule-based reasoning
  - Model-based reasoning
  - Case-based reasoning
  - Codebook correlation model
  - State transition graph model
  - Finite state machine model

Rule-Based Reasoning

Figure 13.7 Basic Rule-Based Reasoning Paradigm

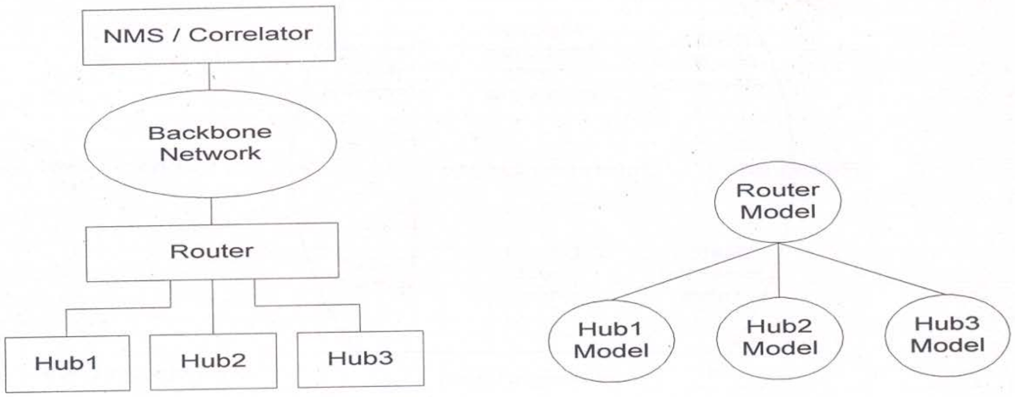
- Knowledge base contains expert knowledge on problem symptoms and actions to be taken

  if -> then

  condition -> action
- Working memory contains topological and state information of the network; recognizes system going into faulty state
- Inference engine in cooperation with knowledge base decides on the action to be taken
- Knowledge executes the action
- Rule-based paradigm is an iterative process
- RBR is "brittle" if no precedence exists
- An exponential growth in knowledge base poses problem in scalability
- Problem with instability

if packet loss < 10%	alarm green
if packet loss => 10% < 15%	alarm yellow
if packet loss => 15%	alarm red

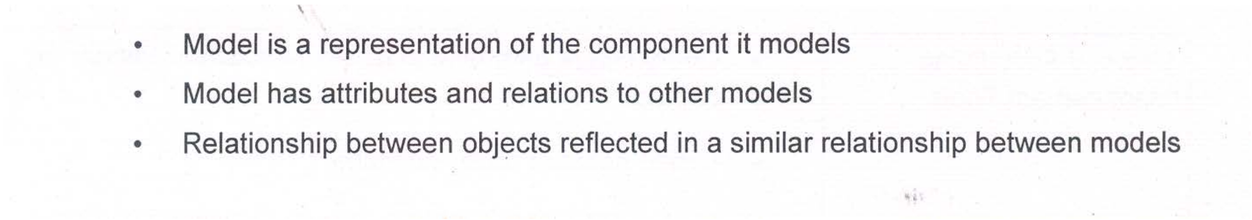
Model-Based Reasoning



Physical Network Equivalent Model

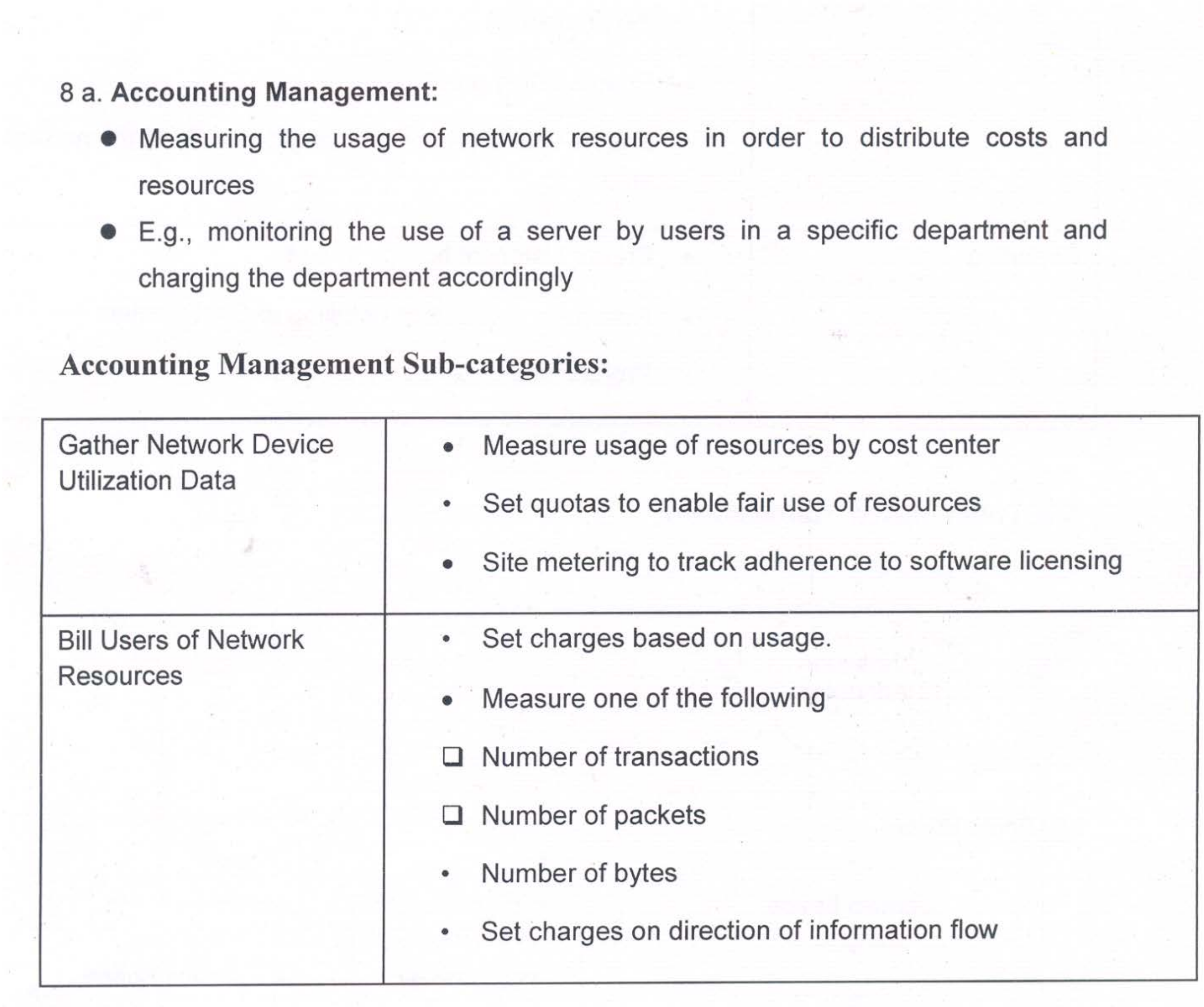
Figure 13.11 Model-Based Reasoning Event Correlator

- Object-oriented model



- Model is a representation of the component it models
- Model has attributes and relations to other models
- Relationship between objects reflected in a similar relationship between models

Q.8 a. What do you understand by Accounting Management? Explain.

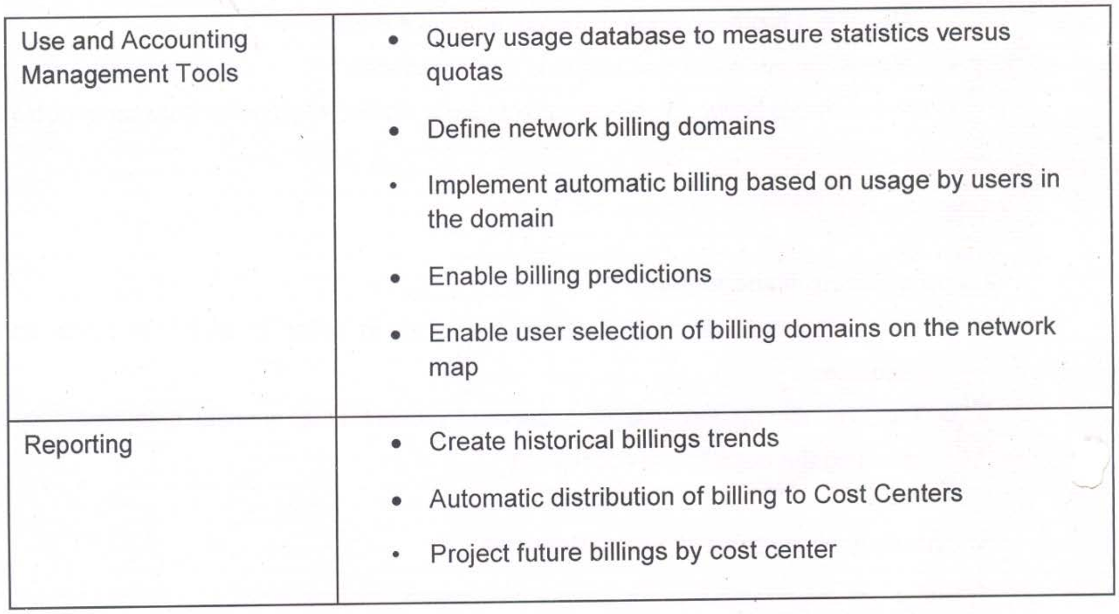


8 a. **Accounting Management:**

- Measuring the usage of network resources in order to distribute costs and resources
- E.g., monitoring the use of a server by users in a specific department and charging the department accordingly

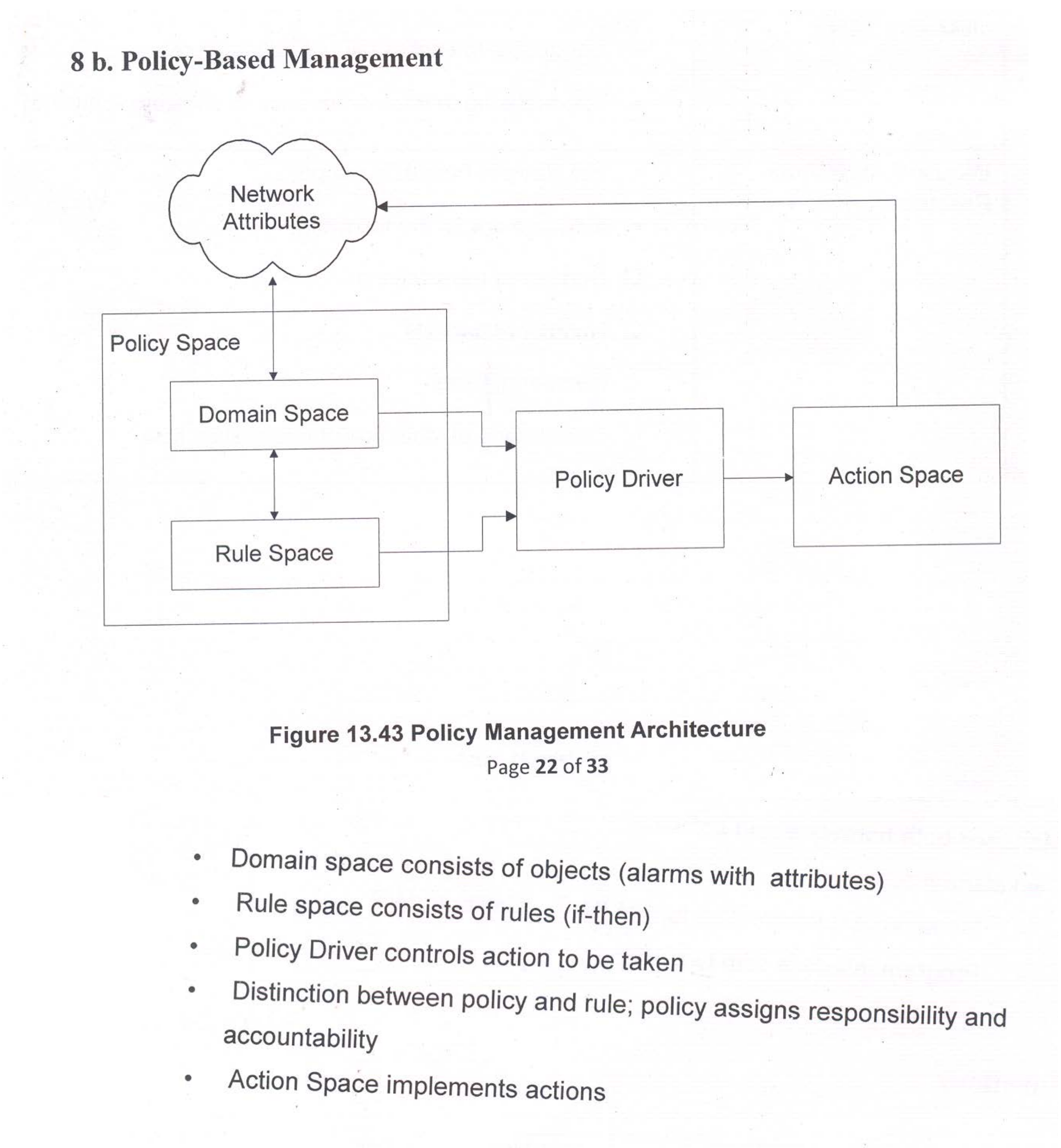
Accounting Management Sub-categories:

Gather Network Device Utilization Data	• Measure usage of resources by cost center • Set quotas to enable fair use of resources • Site metering to track adherence to software licensing
Bill Users of Network Resources	• Set charges based on usage. • Measure one of the following ❑ Number of transactions ❑ Number of packets • Number of bytes • Set charges on direction of information flow



Use and Accounting Management Tools	• Query usage database to measure statistics versus quotas • Define network billing domains • Implement automatic billing based on usage by users in the domain • Enable billing predictions • Enable user selection of billing domains on the network map
Reporting	• Create historical billings trends • Automatic distribution of billing to Cost Centers • Project future billings by cost center

b. Explain Policy-Based Management.



8 b. Policy-Based Management

Figure 13.43 Policy Management Architecture

Page **22** of **33**

- Domain space consists of objects (alarms with attributes)
- Rule space consists of rules (if-then)
- Policy Driver controls action to be taken
- Distinction between policy and rule; policy assigns responsibility and accountability
- Action Space implements actions

Q.9 **a.** Explain the web-based enterprise management. Illustrate with the help of functional diagram.

Ans Page 592-595 of Book I

- Industry standard generated by Desktop Management Task Force (DTMF)
- Started in 1992 to manage PCs
- Manages both hardware and software
- Two standards
  - Management information format (MIF), similar to MIB
  - Program interface with two APIs

DMI Functions

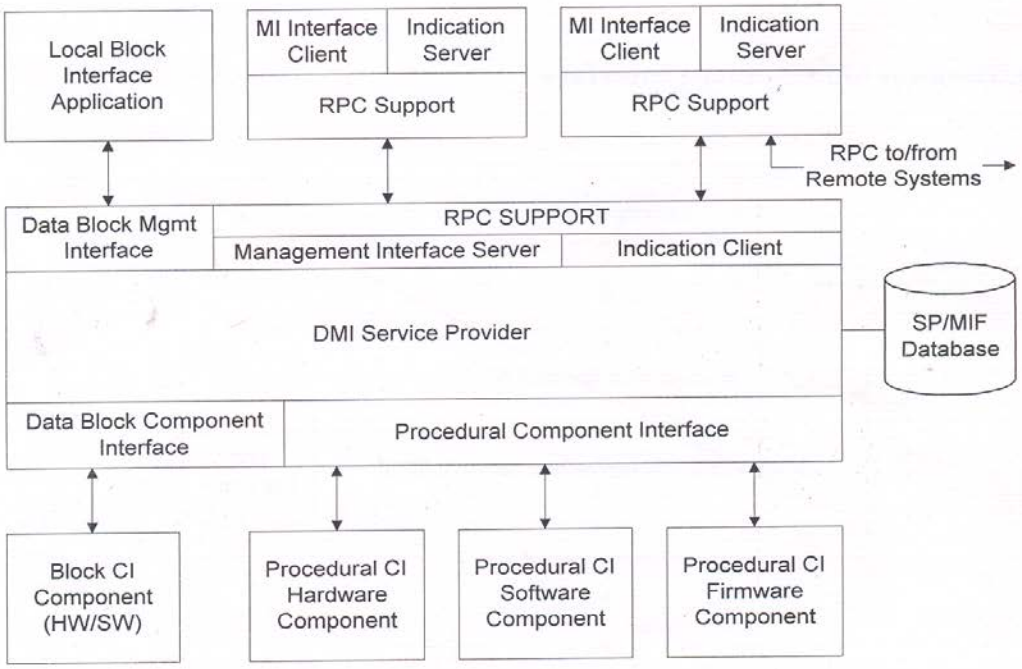
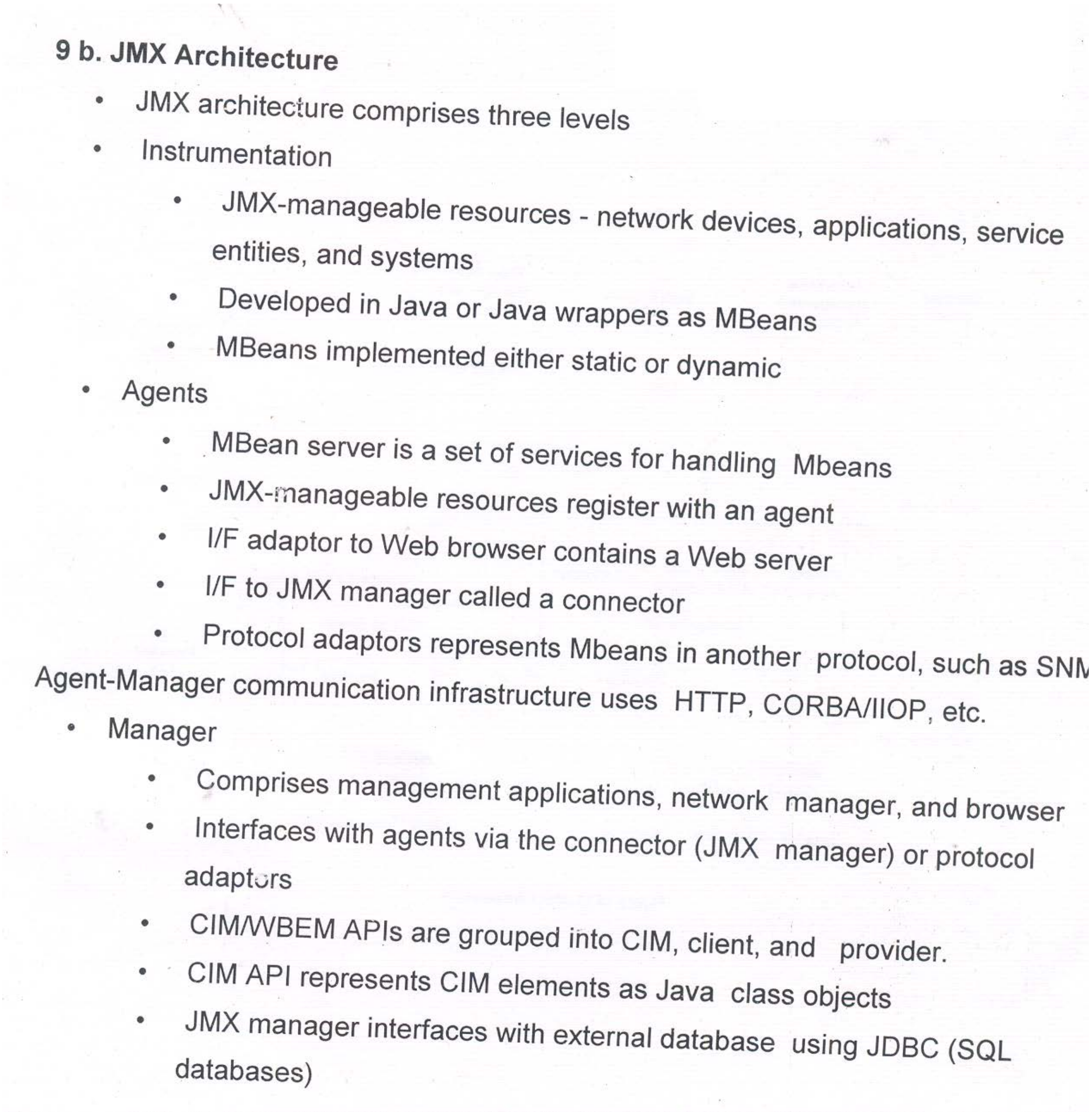

Local Block Interface Application
MI Interface Client
Indication Server
RPC Support
MI Interface Client
Indication Server
RPC Support
RPC to/from Remote Systems
Data Block Mgmt Interface
RPC SUPPORT
Management Interface Server
Indication Client
DMI Service Provider
SP/MIF Database
Data Block Component Interface
Procedural Component Interface
Block CI Component (HW/SW)
Procedural CI Hardware Component
Procedural CI Software Component
Procedural CI Firmware Component

Figure 14.6 DMI Functional Block Diagram

- Architecture has dual representation
  - Version 1 with data block component I/F
  - Version 2 with procedural component I/F

b. Explain the concept of Java Management Extensions. Illustrate your answer by explaining the architecture of Java Management Extensions.



9 b. JMX Architecture

- JMX architecture comprises three levels
- Instrumentation
  - JMX-manageable resources - network devices, applications, service entities, and systems
  - Developed in Java or Java wrappers as MBeans
  - MBeans implemented either static or dynamic
- Agents
  - MBean server is a set of services for handling Mbeans
  - JMX-manageable resources register with an agent
  - I/F adaptor to Web browser contains a Web server
  - I/F to JMX manager called a connector
  - Protocol adaptors represents Mbeans in another protocol, such as SNM

Agent-Manager communication infrastructure uses HTTP, CORBA/IIOP, etc.

- Manager
  - Comprises management applications, network manager, and browser
  - Interfaces with agents via the connector (JMX manager) or protocol adaptors
  - CIM/WBEM APIs are grouped into CIM, client, and provider.
  - CIM API represents CIM elements as Java class objects
  - JMX manager interfaces with external database using JDBC (SQL databases)

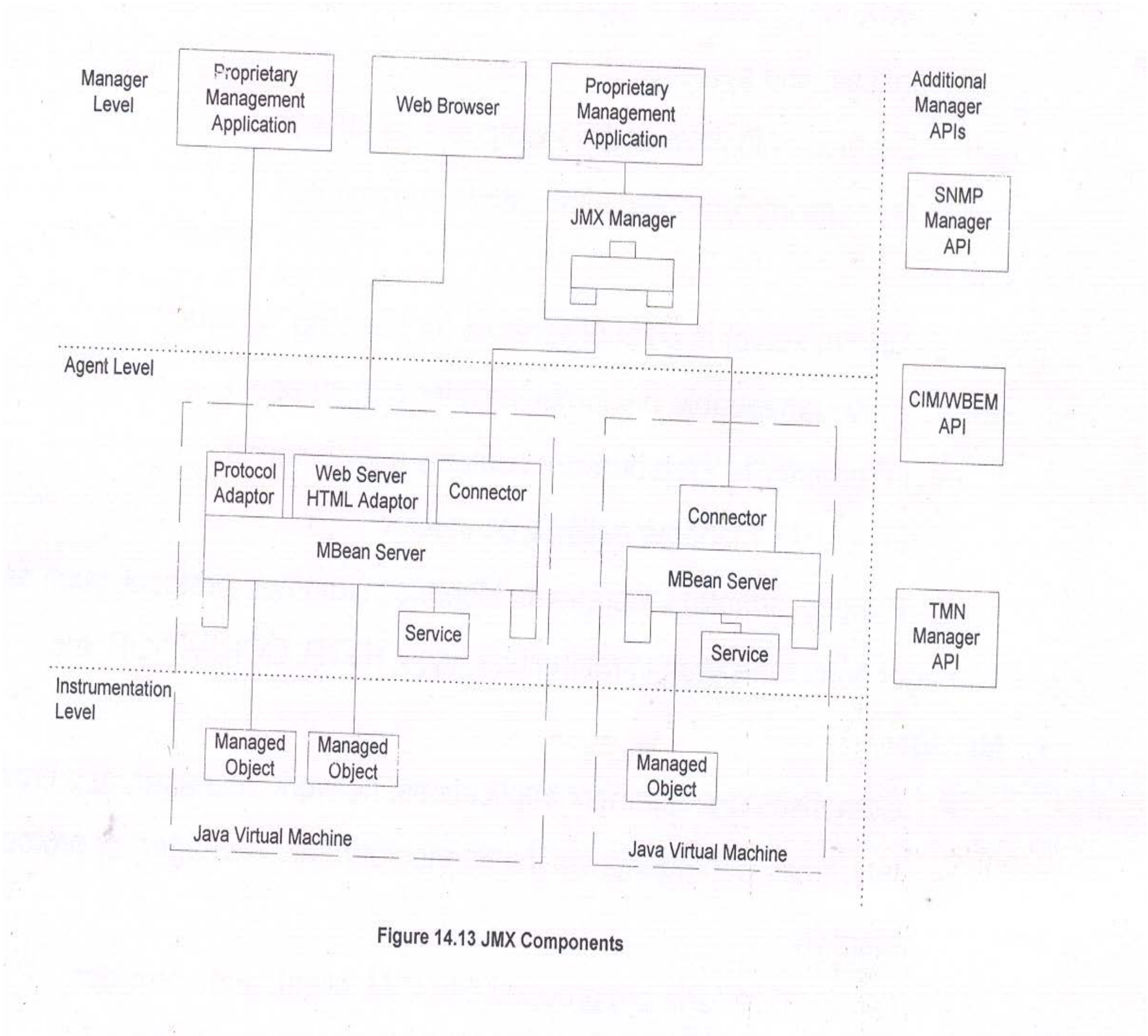


Figure 14.13 JMX Components

Text Book

1. Network Management Principles and Practice, Mani Subramanian, Pearson