Q.2 a. Most of the popular host operating systems come with the TCP/IP Suite and are amenable to SNMP management. The current networks management systems, however, suffer from several limitations. Describe them. (10)

Answer:
The current network management systems need a dedicated NMS monitoring station, which must be on a specific type of platform. Access to an NMS from remote locations is accomplished by using ad hoc schemes such as X-host application in UNIX nased NMS.

Another limit of an SNMP-based NMS is that the values of the managed objects should be defined as scalar values. The OSI-based management protopcol, CMIP, is object oriented. However, it has so far not been successful due to the complexity of specs of managed objects, and thus the enormous memory required to handle CMIP stacks in workstations.

The third limitation is that SNMP-based management is polling based system. In other words, NMS polls each agent as to its status, or for any data that it needs for network management. Only a small set of transactions is initiated by a management agent to an NMS, as alarms.

b. Write the most popular uses of the Internet for home users. (6)

Answer:
The most popular uses of the Internet for home users are:

- Access to remote information: involves interactions between a person and a remote database. Examples: web, on-line newspapers, on-line digital library (e.g., www.acm.org)

- Person-to-person communication. Examples: email, instant messaging, chat rooms, newsgroups, telephone calls, videophone.

o Peer-to-peer communication: eliminate the central database (different from the client/server model). Example: Napster.

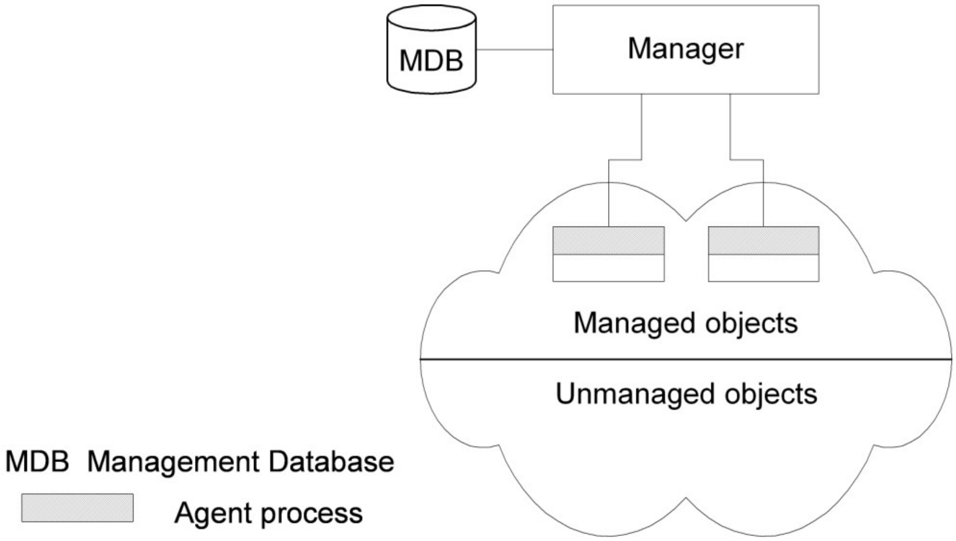
- Interactive entertainment. Examples: video on demand, game playing.

- Electronic commerce: Examples: Home shopping, access to financial institutions (security issues), B2C (e.g., buying online), B2B (manufacturer orders from suppliers), G2C (Tax forms), C2C (Auctions), P2P (File sharing).

B: Business, C: Client, G: Government, P: Peer.

Q.3 a. Describe the components of the 2-tier Network Management Organizational model and their relationship. (8)

Answer:



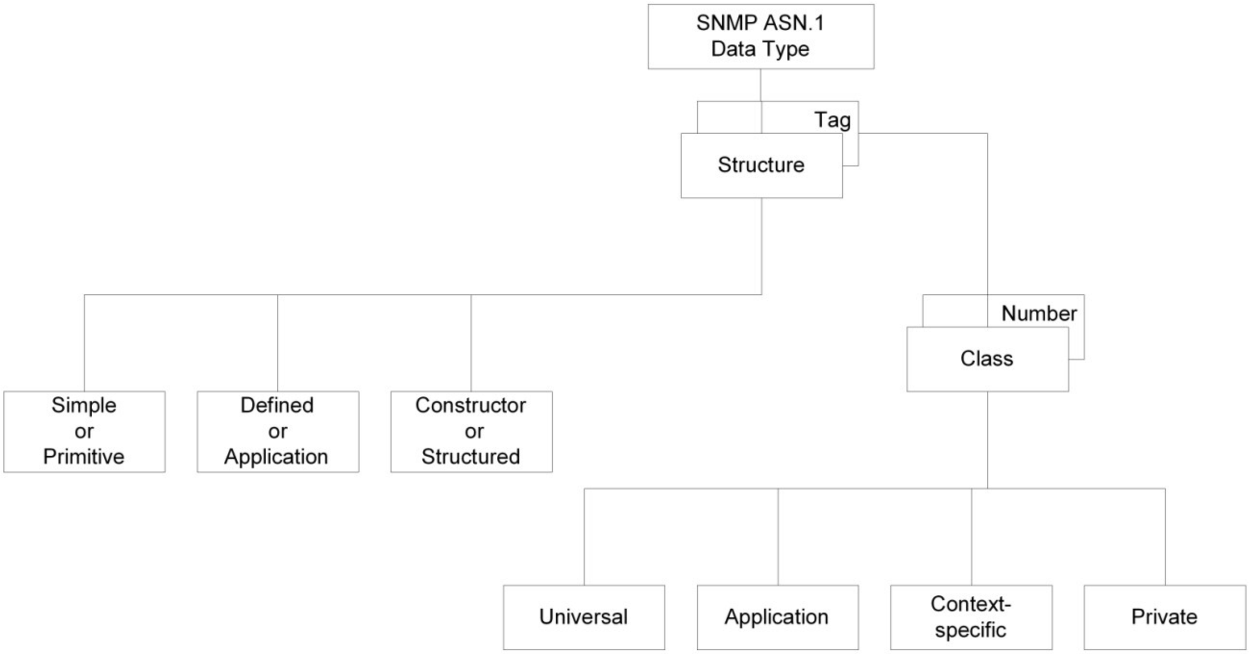
Two-Tier Network Mangement Organization Model

Agent is built into the network element (e.g. managed hub, managed router). A manager can manage multiple elements (e.g 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). The **Manager** manages the managed elements. Sends requests to agents, retrieves management information & stores it in MDB, monitors alarms – unsolicited traps/notifications from agents, houses applications, e.g., CM, FM, and provides user interface, e.g., HPOpenview. The **Agent** gathers information from objects – get, configures parameters of objects – set, responds to managers' requests – response, generates alarms and sends them to managers (unsolicited) – trap, managed object, network element that is managed, e.g., hubs, bridges, etc. houses management agent – process.

b. With the help of a block diagram illustrate SNMP ASN.1 Data Type. (8)

Answer:

Figure below shows the block diagram of SNMP Data Type.



SNMP ASN.1 Data Type

Q.4 a. What are organization responsible for developing Internet Standards? (6)

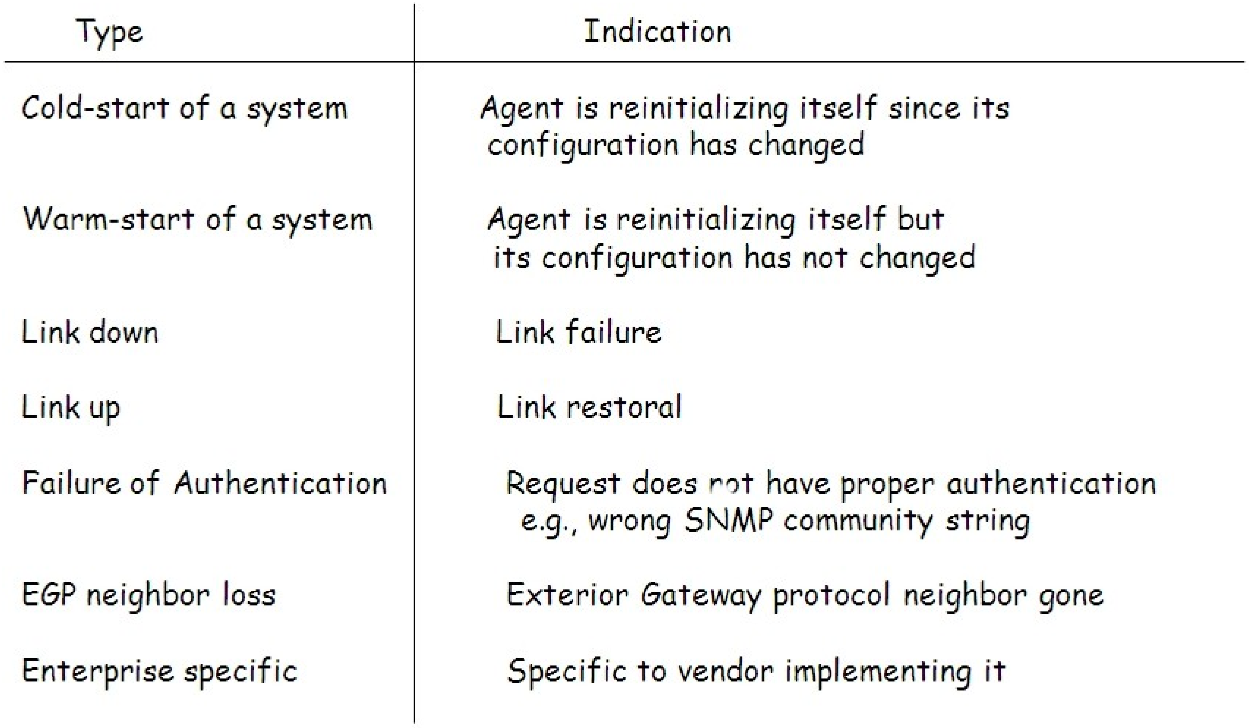
Answer: Refer page 175 of Text Book

b. With the help of suitable diagram explain the two-tier and three-tier organization model of SNMP management. (5+5)

Answer: Refer pages 178-179 of Text Book

Q.5 a. Describe the SNMP traps in the communication model along with the indications. What is the format of a trap? (6+2)

Answer:



Type	Indication
Cold-start of a system	Agent is reinitializing itself since its configuration has changed
Warm-start of a system	Agent is reinitializing itself but its configuration has not changed
Link down	Link failure
Link up	Link restoral
Failure of Authentication	Request does rot have proper authentication e.g., wrong SNMP community string
EGP neighbor loss	Exterior Gateway protocol neighbor gone
Enterprise specific	Specific to vendor implementing it

FORMAT of the GENERIC TRAP:

```
generic-trap    INTEGER {
                 coldStart          (0),
                 warmStart           (1),
                 linkDown             (2),
                 linkUp             (3),
                 authenticationFailure (4),
                 egpNeighborLoss       (5),
                 enterpriseSpecific   (6)
          }
```

b. Describe RMON2 Standard. In addition to existing groups in RMON, what are the 10 groups under which RMON2 objects are divided into? (4+4)

Answer:

RMON2 Standard

RMON2 is an extension of RMON that focuses on higher layers of traffic above the medium access-control(MAC) layer. RMON2 has an emphasis on IP traffic and application-level traffic. RMON2 allows network management applications to monitor packets on all network layers. This is difference from RMON which only allows network monitoring at MAC layer or below. RMON2 is intended to be used by network monitoring applications. It is not intended to be used by human. Each monitored object must have a name, a syntax, an access-level, and an implementation-status. The name is used to identify the a monitored object. The name has an object type and an object instance. Usually, the name is a text string for human to read. The syntax is the structure defined using ASN.1 notation. This abstract structure helps the human to understand the monitored object. The access-level means whether the monitored object can be read, written or both. Implementation-status is the status of the actual object. There are four possible values: mandatory, optional, obsolete, or deprecated.

RMON2 objects are divided into the following 10 groups:

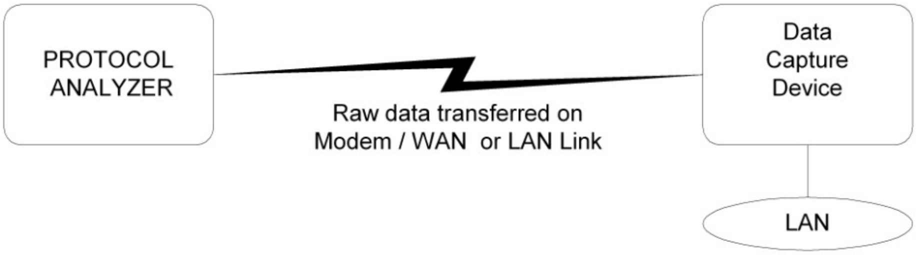
1. protocol directory,
2. protocol distribution,
3. address mapping,
4. network layer host,
5. network layer matrix,
6. application layer host,
7. application layer matrix,
8. user history,
9. probeConfig,
10. rmonConformance

.

Q.6 a. Describe the basic configuration of a protocol analyzer. What are the capabilities of the protocol analyzers that are available in the market? (8)

Answer:

The protocol analyzer is a powerful and versatile network management tool. We will consider it as a test tool in this section, and later on look at its use as a system management tool. It is a tool that analyzes data packets on any transmission line. Although it could be used for the analysis of any line, its primary use is in the LAN environment, which is what we will focus on here. Measurements using the protocol analyzer can be made either locally or remotely. The basic configuration used for a protocol analyzer is shown in Figure below.



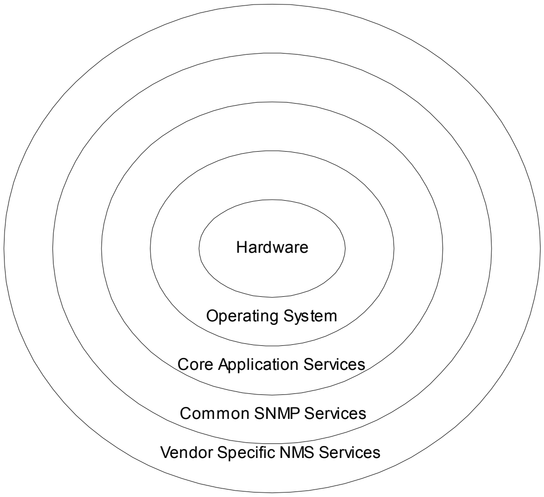
Protocol Analyzer Basic Configuration

It consists of a data capture device that is attached to a LAN. This could be a specialized tool, or either a personal computer or workstation with a network interface card. The captured data are transmitted to the protocol analyzer via a dial-up modem connection, a local or campus network, or a wide area network. The protocol analyzer analyzes the data and presents it to the user on a user-friendly interface.

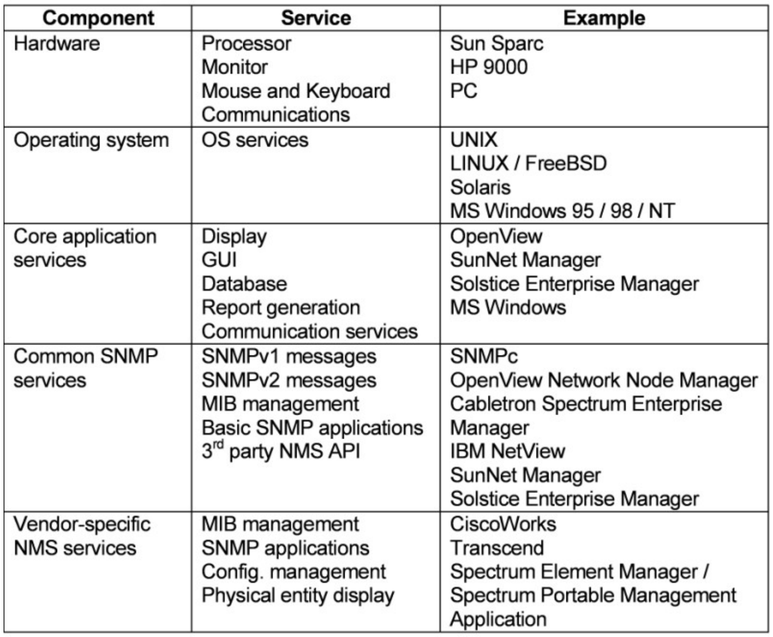
The protocol analyzers that are available in the commercial market are capable of presenting a multitude of results derived from the data. Contents of data packets can be viewed and analyzed at all layers of the OSI reference model. The distribution of various protocols at each layer can be ascertained. At the data link layer, besides the statistical counts, the collision rate can be measured for Ethernet LAN. At the transport layer, port information for different applications and sessions can be obtained. The distribution of application-level protocols provides valuable information on the nature of traffic in the network, which can be used for performance tuning of the network. Numerous commercial and open-source protocol analyzers and sniffers are now available. Sniffer can be used as a stand-alone portable protocol analyzer, as well as on the network HP.

b. What are the 5 NMS components? Illustrate through a diagram as well as a table listing the service provided by each of these with examples. (2+6)

Answer:



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 Cabletron 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. What is a Fault? Discuss the 5 steps involved in fault management. (2+4)

Answer:
Fault is a failure of a network component and it results in loss of connectivity.

Fault management involves a 5-step process:

Step 1. Fault detection
The step involves: Polling and Traps: linkDown, egpNeighborLoss

Step 2. Fault location
The step involves: Detect all components that failed and trace down the tree topology to where the problem starts

Step 3. Restoration of service (has higher priority)

Step 4. Fault isolation
The step involves: Identification of root cause of the problem and Fault isolation by network and SNMP tools to determine source of problem. A Trouble ticket is generated in this process. This step also involves using artificial intelligence as well as correlation techniques.

Step 5. Problem resolution
Here, the Trouble ticket is closed

b. What are the basic guidelines to set up policies and procedures? (1x5)

Answer:
The basic guidelines to set up policies and procedures are as follows:

1. Identify what you are trying to protect.
2. Determine what you are trying to protect it from.
3. Determine how likely the threats are.
4. Implement measures, which will protect your assets in a cost-effective manner.
5. Review the process continuously and make improvements to each item if a weakness is found.

c. What is the purpose of a firewall? Where is it located? What are the benefits of implementing a firewall? (2+1+2)

Answer:
The main purpose of a firewall is to protect a network from external attacks. It monitors and controls traffic into and out of a secure network. It can be implemented in a router, gateway, or special host. A firewall is normally located at the gateway to a network, but it may also be located a host access points.

Implementing a firewall to a network yields numerous benefits. It reduces the risk of access to hosts from external network by filtering insecure services. It can provide controlled access to the network so that only specified hosts or network segments can access some hosts. Because protection from external threats is centralized and transparent, it reduces the annoyance to internal users while controlling the external users.

Q.8 a. Write a description of report management function of network management application. What are the specific planning and management reports? (3+5)

Answer:
We have elected to treat report management as a special category, although it is not assigned a special functionality in the OSI classification. Reports for various application functions—configuration, fault, performance, security, and accounting—could normally be addressed in those sections. The reasons for us to deal with reports as a special category are the following. A well-run network operations center goes unnoticed. Attention is paid normally only when there is a crisis or apparent poor service. It is important to generate, analyze, and distribute various reports to the appropriate groups, even when the network is running smoothly. We can classify such reports into three categories:
(1) planning and management reports,
(2) system reports, and
(3) user reports.

Planning and Management Reports

CATEGORY	REPORTS
Quality of service/service level agreement	Network availability
	Systems availability Problem reports Service response Customer satisfaction
Traffic trends	Traffic patterns
	Analysis of internal traffic volume Analysis of external traffic volume
Technology trends	Current status
	Technology migration projection
Cost of operations	Function
	Use Personnel

Reports on this category include network availability, systems availability, problem reports, service response to problem reports, and customer satisfaction. Trends in traffic should address traffic patterns and volume of traffic in the internal network, as well as external traffic. Information technology is constantly evolving and hence management should be kept apprised of upcoming technology and the plan for migration to new technology. Finally, for budgeting purposes, the cost of operations by function, use, and personnel needs to be presented.

b. What is policy based management? Draw a diagram for the policy based management. (5+3)

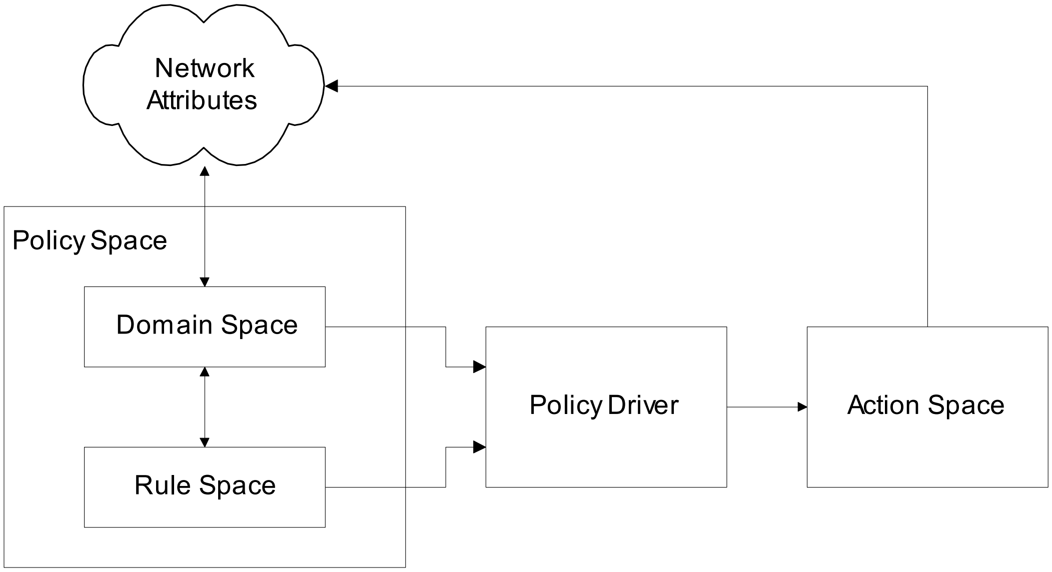
Answer:
Policy-based management is an administrative approach that is used to simplify the management of a given endeavor by establishing policies to deal with situations that are likely to occur.

Policies are operating rules that can be referred to as a way to maintain order, security, consistency, or otherwise furth a goal or mission. For example, a town council might have a policy against hiring the relatives of council members for civic positions. Each time that situation arises, council members can refer to the policy, rather than having to make decisions on a case-by-case basis.

In the computing world, policy-based management is used as an administrative tool throughout an enterprise or network, or on workstations that have multiple users. Policy-based management includes policy-based network management, the use of delineated policies to control access to and priorities for the use of resources. Policy-based management is often used in systems management.

Policy-based management of a multi-user workstation typically includes setting individual policies for such things as access to files or applications, various levels of access (such as "read-only" permission, or permission to update or delete files), the appearance and makeup of individual users' desktops and so on. There are a number of software packages available to automate some elements of policy-based management. In general, the way these work is as follows: business policies are input to the products, and the software communicates to network hardware how to support those policies.

Hers’s the diagram for the policy based management:



Q.9 a. Explain web interface to SNMP management along with a diagram. (8)

Answer:

WEB INTERFACE TO SNMP MANAGEMENT

Two approaches are available.

1) Short-term approach is to add a web interface to an existing management system.

2) To have a web based system with embedded web agents in the network components.

Method1 description:

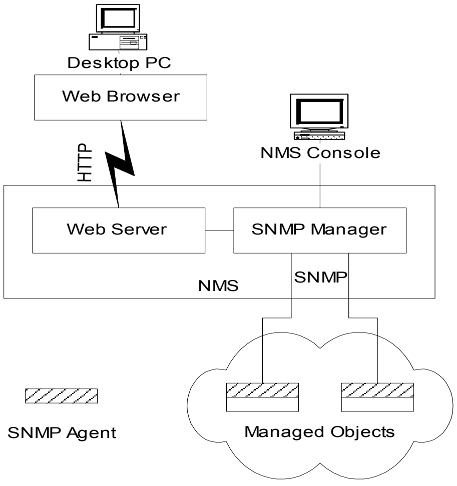


Figure 14.1 SNMP NMS with Web Interface

The most common implementation is to have a web server on an NMS platform with an interface to NMS. The SNMP-NMS implementation I platform and operating system specific and agents are SNMP agents. The protocol between agents and managers is SNMP communication protocol traversing over UDP/IP. The protocol between server and browser is HTTP traversing the internet.

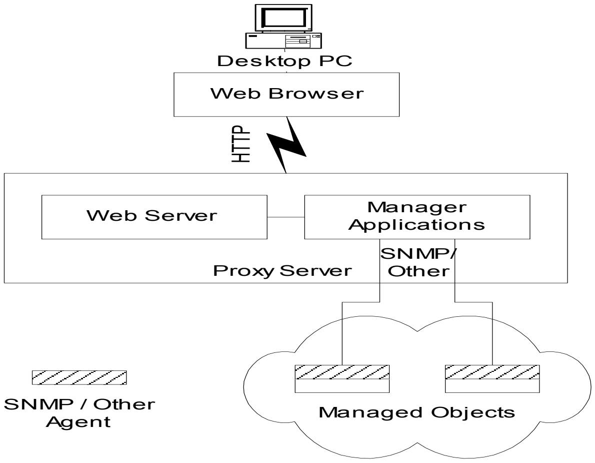


Figure 14.2 Proxy Server with Web Interface

The architecture of proxy server is similar to SNMP NMS with a interface but NMS replaced by a proxy server. The NMS console is eliminated which is a economic advantage. No GUI in manager applications. Another advantage is proxy server can be implemented an any platform and protocol between agents And proxy server can be SNMP are any other protocol.

b. Write short notes on Desktop Management Interface (DMI) with diagrams. (8)

Answer:
The desktop management interface (DMI) is an industry standard generated by DMTF, started in 1992 to develop, support and maintain management standards for Pc systems and products. It is between computer components and application. s/w .The management application is a desktop resident program. The component agents are s/w agents. The components can be s/w(virus checker),h/w(n/w interface card) or firmware (Pentium chip).

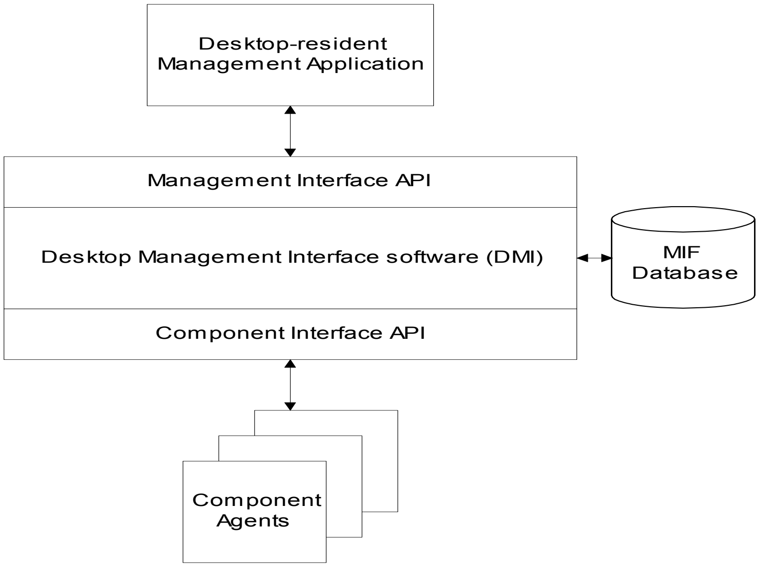

Desktop-resident Management Application
Management Interface API
Desktop Management Interface software (DMI)
Component Interface API
MIF Database
Component Agents

Figure 14.5 DMI Infrastructure

To permit multiple vendors products to be managed by a common application program 2 standards are specified in DMI.

- Management information format (MIF), similar to MIB
- Program interface with two APIs

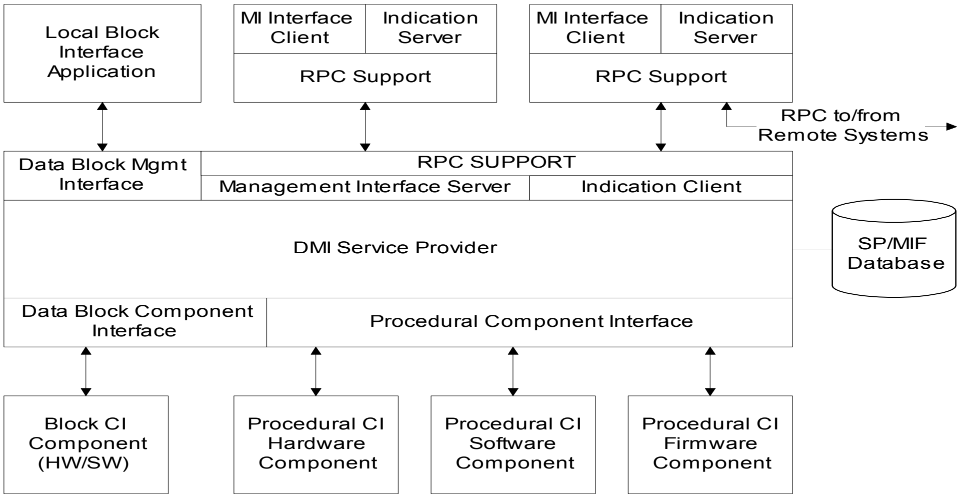

Local Block Interface Application
MI Interface Client
Indication Server
RPC Support
MI Interface Client
Indication Server
RPC Support
RPC to/from Remote Systems
Data Block Mgmt Interface
RPC SUPPORT
Management Interface Server
Indication Client
DMI Service Provider
SP/MIF Database
Data Block Component 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

TEXT BOOK

1. **Network Management Principles and Practice, Mani Subramanian, Pearson Education, 2000**