Q.2 a. Discuss the OSI protocol architecture in detail. List out, at least one salient service provided by each layer (8)

Answer:

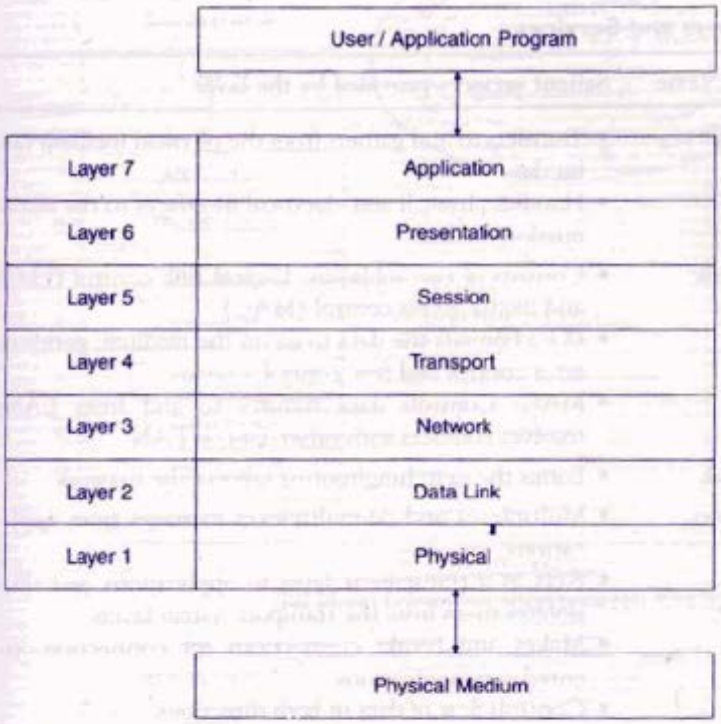

Figure 1.12 The OSI Protocol Layers

cols that is called the Open Systems Interconnection (OSI) Reference Model, published as OSI RM—ISO 7498. This model was developed based on the premise that the different layers of protocol provide different services, and that each layer can communicate with only its own neighboring level. Two systems can communicate on a peer-to-peer level, that is, at the same level of the protocol. The OSI protocol architecture is shown in Figure 1.12. Table 1.1 describes the salient features of and services provided by each of the seven layers. Layers 1 through 4 are the transport system protocol layers; and layers 5, 6, and 7 are application support protocol layers.

OSI protocol architecture truly enables building systems with open interfaces so that networks using systems from different vendors are interoperable. Figure 1.13 expands the basic communication architecture shown in Figure 1.11 to an OSI model. Figure 1.13(a) is a direct end-to-end communication model. The corresponding layers in the two systems communicate on a peer-to-peer protocol interface associated with those layers. In Figure 1.13(b), the end systems communicate by going through an intermediate node/system. Again, notice that the physical media connected to the end systems could be different. The intermediate system is involved only up to the first three layers in the process. Layers 4 through 7 are not involved in the intermediate system. This is analogous to a mail container with letters enclosed in envelopes being transported from one town to another town anywhere in the world. It does not matter what network of intermediate cities (nodes) it goes

Table 1.1 **OSI Layers and Services**

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	• Multiplexes and de-multiplexes 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 • Controls flow 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 application and each transport protocol system

through, a what network of transportation media—surface, air, or water—it takes to get to the destination. The letters in envelopes and the contents of packages are untouched at the transfer points and are handled only by the sender and receiver, that is, user applications.

The message in each layer is contained in message units called protocol data units (PDUs), which consist of two parts—protocol control information (PCI) and user data (UD). PCI contains header information about the layer. UD contains the data that the layer, acting as a service provider, receives from or transmits to the upper layer/service user layer. The PDU communication model between two systems A and Z, including the users at the top and the transmission medium at the bottom of the PDU layers, is shown in Figure 1.14. As you can see in Figure 1.14, the size of the PDU increases as it goes toward lower layers. If the size of the PDU exceeds the maximum size of layers specifications, it is fragmented into multiple packets. Thus, a single application-layer PDU could multiply into several physical PDUs.

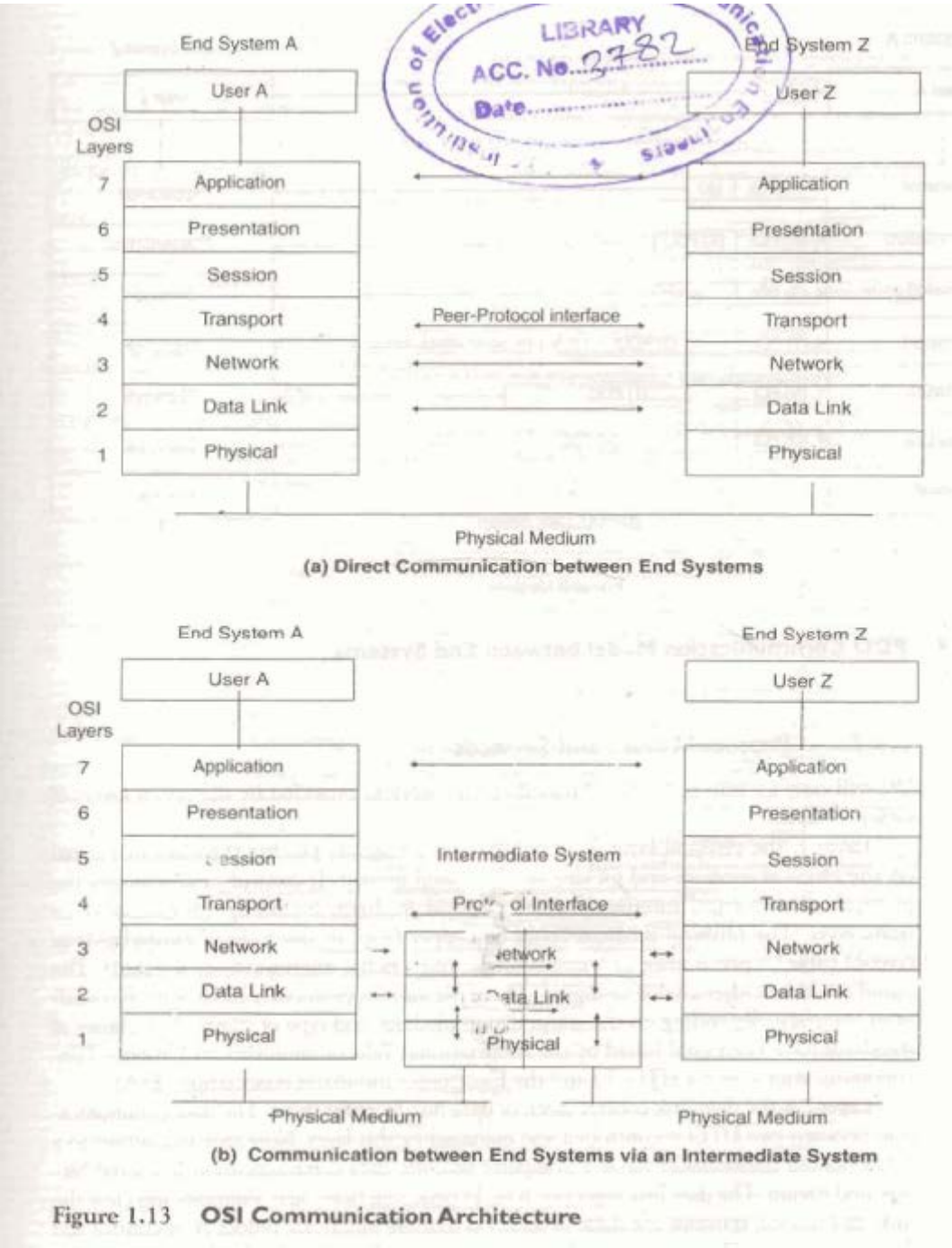

Figure 1.13 OSI Communication Architecture

b. Identify the various network management functions and the groups that perform these functions. Also, explain the interactions among these groups. (8)

Answer:

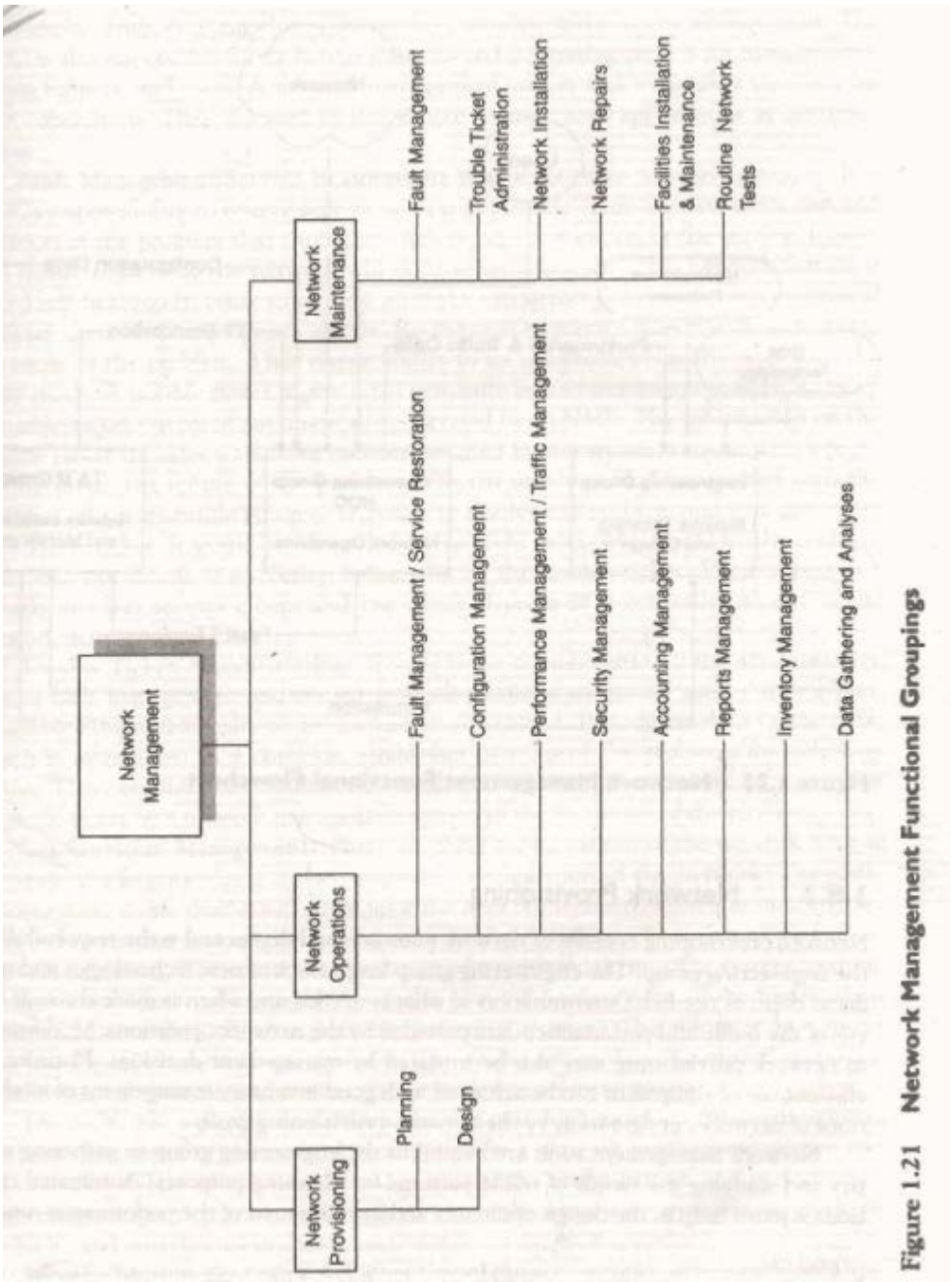

Figure 1.21 Network Management Functional Groupings

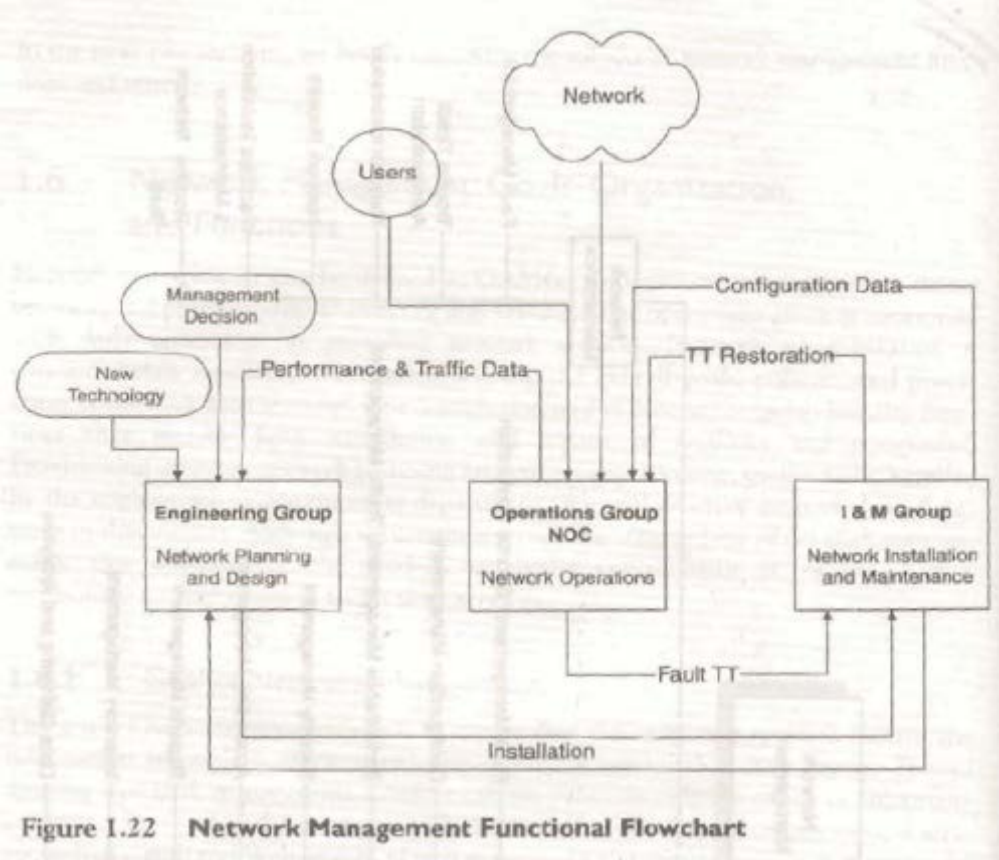

Figure 1.22 **Network Management Functional Flowchart**

Q.3 a. Compare the two-tier network management organizational model with the three-tier network management organizational model. Illustrate your answers with suitable diagrams (8)

Answer:

In the two-tier model network objects consist of network elements such as hosts, hubs, bridges, routers and so on. They can be classified into managed and unmanaged objects or elements. The managed elements have a management process running in them called an agent , which is not present in the unmanaged objects.The managed element is managed by a manager. There is a database present in the manager. The manager queries the agent and receives the management data, processes and stores it in its database. The agent can also send a minimal set of alarm information to the manager unsolicited.

Diagram on p133

2- marks for explanation and 2 marks for diagram

However in a three tier configuration, the intermediate layer acts as both agent and manager. As manager , it collects data from the network elements , processes it and stores the result in it database. As agent it transmits information to th top-level manager. **Diagram on p134**

2- marks for explanation and 2 marks for diagram

b. What is ASN.I and why is it required? With the help of a block diagram , outline the ASN.I data type structure and tag (8)

Answer:

For communication among systems, it is important that a formalized set of rules be agreed upon regarding the structure and meaning of language of communication, that is the syntax and semantics of the language . Because of the variety of sets of application and transport protocols, it is better to choose a syntactical format of language that specifies the management protocol in the application layer , which is transparent to the rest of the protocol layer . A proven format is **Abstract syntax Notation One, ASN.1.** It is a formal language developed jointly by CCITT and ISO fro use with application layers for data transfer between systems. It is also applicable within the system for clearly separating the abstract syntax and the transfer syntax at the presentation layer.

1 for what is ASN.1, 2 marks for why it is needed and 5 for block **diagram(p150)**

Q.4 a. Explain, with the help of a block diagram, a Proxy Server Organization model. List and explain the five protocol messages of SNMPv1 which facilitate the communication of management information among management entities (8)

Answer:

P 180 – the Proxy Server Organization Model.(3 marks)
5 marks for the messages.

The **get-request** message is generated by the management process requesting the value of an object. The value of an object is a scalar variable.

The **get-next-request** is similar to get-request message .An object may have multiple values because of the multiple instances of the object.. This message obtains the value of the next instance of the object.

The **set-request** message is generated by the management process to initilaize or reset the value of an object variable.

The **get-response** message is generated by an agent process. It is generated only on receipt of a get-request, get-next-request or set-request message from a management process. The get-response process involves filling the value of the requested object with any success or error message associated with the response

The other message that the agent generates is trap. A trap is an unsolicited message generated by an agent process without a message or event arriving from the management process. A trap occurs when the agent observes the occurrence of a preset parameter in the agent module.

b. What are the following data types of SNMP ASN.I used for? Also specify the structure of each of the data type.
(i) Gauge (ii) Time-ticks
(iii) Opaque (iv) SEQUENCE (8)

Answer:

i. Gauge- is used a non-negative integer,its value can move either up or down. It is used for data types whose value increases or decreases, such as the number of interfaces that are active in a router or hub. It is a defined data type.

ii. Time-ticks- is a non-negative integer and measures time in units of hundredths of a second. Its value value indicates in hundredths of a second the number of units of time between the current instant and the time it was initialized to 0.It is a defined data type.

iii. Opaque- is an application –wide data type that supports the capability to pass arbitrary ASN.1 syntax.It is used to create data types based on previously defined data types. When it is encoded, it is double wrapped,meaning te TLV for the new definition is wrapped around the tLV of the previously defined type.

iv. SEQUENCE- is a constructor data type. It is used to build a list.

Q.5 a. What are protocol entities? How is communication among these protocol entities is accomplished? Show the structure of encapsulated SNMP message. (8)

Answer:

The peer processes which implement the SNMP, and thus support the SNMP application entities, are called protocol entities. Communication among protocol entities is accomplished using messages encapsulated in UDP datagrams.(1+1)

Explanation of message + diagram of message (6) **p 234**

b. What is Remote Monitoring? Discuss its advantages. (8)

Answer:

8.1 What Is Remote Monitoring?

In Chapter 5 we gave some examples of SNMP messages going across a network between a manager and an agent. We did so with a tool that "sniffs" every packet going across a LAN, opens it, and analyzes it. It is a passive operation and does nothing to the packets, which continue on to their destinations. This approach is called *monitoring* (or probing) *the network*, and the device that performs that function is called a *network monitor* (or probe). We need to make a distinction between the two components of a probe: (1) the physical object that is connected to the transmission medium, and (2) the processor that analyzes the data. If both are at the same place geographically, the probe is local, which is how sniffers used to function. We will discuss this topic further in Chapter 9, when we consider management systems and tools.

The monitored information, gathered and analyzed locally, can be transmitted to a remote network management station. In such a case, remotely monitoring the network with a probe is referred to as Remote Network Monitoring (RMON). Figure 8.1 shows an FDDI backbone network with a local Ethernet LAN. Two remote LANs, one a token ring LAN and another, an FDDI LAN, are connected to the backbone network. The network manage-

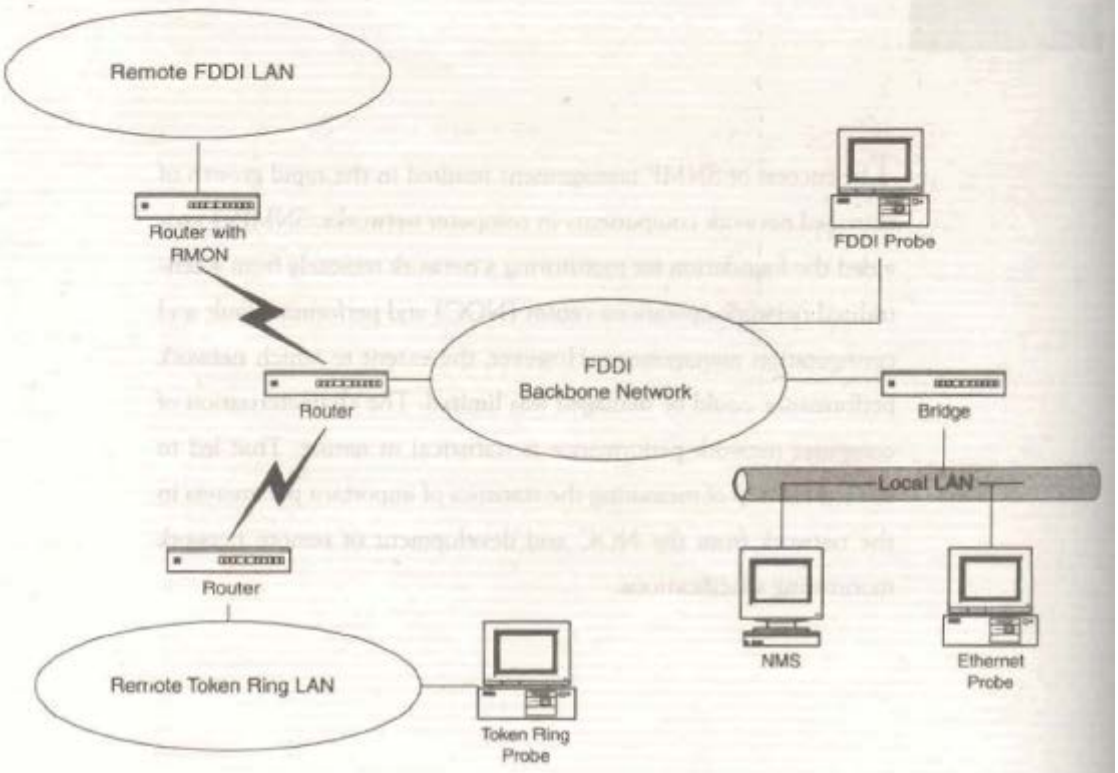

Figure 8.1 Network Configuration with RMONs

ment system (NMS) is on the local Ethernet LAN. Either an Ethernet probe or an RMON is on the Ethernet LAN monitoring the local LAN. The FDDI backbone is monitored by an FDDI probe via the bridge and Ethernet LAN. A token ring probe monitors the token ring LAN. It communicates with the network management system via the routers, the WAN (shown by the lightning bolt symbol of the telecommunications link), and the backbone network. The remote FDDI is monitored by the built-in probe on the router. The FDDI probe communicates with the network management system. All four probes that monitor the four LANs and communicate with the network management system are RMON devices.

The use of RMON devices has several advantages. One advantage is that each RMON device monitors the local network segment and does the necessary analyses. It relays information in both solicited and unsolicited fashion to the network management system. For example, RMON could be locally polling the network elements in a segment. If it detects an abnormal condition, such as heavy packet losses or excessive collisions, it sends an alarm. Because the polling is local, the information is fairly reliable. This example of local monitoring and reporting to a remote network management system significantly reduces SNMP traffic in the network. This reduction is especially true for the segment in which the network management system resides, as all the monitoring traffic would otherwise converge there.

The following case history illustrates another advantage: that RMON reduces the need for agents in the network to be visible at all times to the network management system. A network management system frequently indicated that one of the hubs showed failure, but the hub recovered without any intervention. The performance study of the hub that the LAN was part of, indicated that the LAN would frequently become overloaded with heavy traffic and would experience significant packet loss. The lost packets included the ICMP packets that the NMS was using to poll the hub. The NMS had been set to indicate a node failure if three successive ICMP packets did not receive responses. Increasing the number of packets needed to indicate a failure stopped the failure indication.

Monitoring packets, such as ICMP pings, may get lost in long-distance communication, especially under heavy traffic conditions. Such losses may wrongly be interpreted by the network management system that the managed object is down. RMON pings locally and hence has less chance of losing packets, thus increasing monitoring reliability.

Yet another advantage of local monitoring with RMON is that the individual segments can be monitored almost continuously. This capability provides better statistics and control. Thus a fault can be diagnosed more quickly by the RMON and reported to the network management system. In some situations, a failure may even be prevented by proactive management.

The overall benefits of implementing RMON technology in a network are higher network availability for users and greater productivity for administrators. A study report [CISCO/RMON] indicates significantly increased productivity for network administrators who use RMON in their networks.

Q.6 a. What is a protocol analyzer? Explain the basic configuration used for a protocol analyzer. Use suitable diagram. Name any two popular commercial protocol analyzers. (8)

Answer:

The protocol analyser is a powerful and versatile network management tool. It analyzes data packets on any transmission line.It is primarily used in LAN environment. Protocol analyzer measurements can be made either locally or remotely.(2 marks)

The basic configuration :: - **diagram p 498** (2 marks)

It consists of a data capture device that is attached to a LAN and can be a specialized tool; it can also be 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 LAN or campus network or a WAN. The protocol analyzer analyzes the data and presents the results to the user on a user-friendly interface.(2 marks)

Two popular analyzers – Sniffer, NetMetrix (2 marks)

b. Identify the five functional components of a Network management system. List any one service offered by each of these components along with pictorial representation. (8)

Answer:

The five functional components are

Component Service

i. Hardware – Processor
ii. Operating system- OS service
iii. Core application service – Display/GUI
iv. Common SNMP services- SNMPv1 messages / SNMPv2 messages
v. Vendor –specific NMS services- MIBmanagement

Diagram – p 506

(1/2 marks for identifying component + ½ mark for nay service)

(3 marks for diagram)

Q.7 a. What is a fault? Explain the various steps in fault management. Name any two methods of fault detection. (8)

Answer:

Fault in a network is normally associated with failure of a network component and subsequent loss of connectivity.(1 mark) Fault management process is a five step process

i. Fault detection – The fault should be deteted as quickly as possible by the centralized management system , preferably before or at about the same time as users would notice it.
ii. Fault location- involves identifying here the problem has occurred
iii. Service restoration- has a higher priority than diagnosing the problem and fixing it
iv. Identification of the problem – identifying the root cause, can be a complex process
v. Problem resolution – After source of problem is identified , a trouble ticket is generated. In an automated network , this ticket could be generated automatically by the NMS.(5 marks)

Fault detection is accomplished by using either a polling scheme or generation of traps(2 marks)

b. Differentiate between secret key cryptography and public key cryptography. (8)

Answer:

Secret Key Cryptography. The Caesar cipher was later enhanced by the makers of Ovaltine and distributed as Captain Midnight Secret Decoder rings. Each letter was replaced by another letter n letters later in the alphabet (i.e., key of n). Of course, the sender and the receiver have to agree ahead of time on the secret key for successful communication. It's the same key used for encryption and decryption and is called **secret key cryptography**. The encryption and decryption modules can be implemented in either hardware or software.

An intruder can easily decode the preceding ciphertext. Only a maximum of 26 attempts would be needed to decipher it, as there are 26 letters in the alphabet. In another encryption scheme, the *monoalphabetic cipher*, each letter is replaced uniquely with another letter that is randomly chosen. Now, the maximum number of attempts for the intruder to decipher has been increased to 26! (26! = 26 · 25 · 24 · … 1). However, that many attempts really aren't needed because there are patterns in a language.

Obviously, the key is the key (no pun intended) to the security of messages. Another aspect of the key is the convenience of using it. We will illustrate this point with a scenario involving Ian and Rita (Ian for initiator and Rita for responder) as users at the two ends of a secure communication link. Ian and Rita could share a key—their secret key, for secure communication. However, if Ian wants to communicate with Ted (for third party), they also need to share a secret key. Soon, Ian has to remember one secret key for each person with whom he wants to communicate, which, obviously, is impractical. It's hard enough to remember your own passwords, if you have several of them, and which systems they go with.

Two standard algorithms implement secret key cryptography. They are the Data Encryption Standard (DES) and the International Data Encryption Algorithm (IDEA) [Kaufman C, Perlman R & Speciner M]. Both deal with 64-bit message blocks and create the same size ciphertext. DES uses 56-bit key and IDEA uses a 128-bit key. DES is designed for efficient hardware implementation and consequently performs poorly if implemented in software. In contrast, IDEA functions efficiently in software implementations.

Both DES and IDEA are based on the same principle of encryption. The bits in the plaintext block are rearranged several times, using a predetermined algorithm and the secret key. During decryption, the process is repeated in reverse for DES. Decryption is a bit more complicated for IDEA.

A message that is longer than the block length is divided into 64-bit message blocks. Any one of several algorithms is used to break up the message. One of the more popular ones is the cipher block chaining (CBC) method. Recall that we used it with the USM in SNMPv3 in Chapter 7. There, we used CBC to break up the message and then used DES to encrypt it. Performing such an operation on the message, even on identical plaintext blocks, would result in dissimilar ciphertext blocks.

Public Key Cryptography. In private key cryptography each pair of users must have a secret key. Public key cryptography [Diffe W & Hellman M; Kaufman C, Perlman R, & Speciner M] overcomes the difficulty of having too many cryptography keys. The secret key cryptography is symmetric in that the same key is used for both encryption and decryption, but public key cryptography is asymmetric with a *public key* and a *private key*, which are different. Let us return to our Ian, Rita, and Ted scenario to illustrate. In Figure 13.34, the public key is Ian's; it is the key that Rita, Ted, and everybody else (with whom Ian wants to communicate) knows and uses to encrypt messages that they send to Ian. The private key, which only Ian knows, is the key that he uses to decrypt the messages. This scheme ensures secure communication between Ian and the other communicators on a one-to-one basis. Rita's message to Ian can be read only by Ian and not by anyone else who has his public key because the public key cannot be used to decrypt the message.

We can compare the use of asymmetric public and private keys in cryptography to a mailbox with two openings: a mail slot for dropping off mail and a collection door for

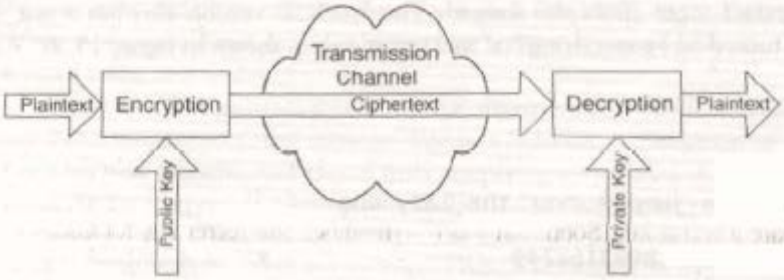

Figure 13.34 Public Key Cryptographic Communication

removing mail. Suppose that it is a private mailbox in a club that restricts access to members only. All members can open the mail slot with a public key provided by the club's administration to drop off their mail, possibly containing comments on a sensitive issue about the club. A member's mail cannot be accessed by other members because only the administrator with a private key can open the collection door and access the mail of all the members. Of course, this asymmetric example has more to do with access than cryptography. But, you get the idea!

The Diffe–Hellman public key algorithm is the oldest public key algorithm. It is a hybrid of secret and public key. The commonly used public key cryptography algorithm is called RSA, after its inventors [Rivest RL, Shamir A, & Adleman L]. It does both encryption and decryption, as well as digital signatures. Both the message length and the key length are variable. The commonly used key length is 512 bits. The block size of the plaintext, which is variable, should be less than the key size. The ciphertext is always the length of the key. RSA is less efficient than either of the secret key algorithms, DES or IDEA. Hence, in practice, RSA is used to encrypt the secret key. The message is then transmitted in one of the secret key algorithms.

Q.8 a. What is the function of planning and management reports in report management activity of network management? List the various categories of the planning and management reports with an example from each of the category (8)

Answer:

Planning and management reports keep upper management apprised of status of network and system operations. They also help in planning and budgeting the capital and operational expenses.(2 marks)

Categories and example, **p 575** (1 mark for each category and ½ mark for example)

b. What is Service level management? Identify the characteristics associated with services (8)

Answer:

Service level management is defined as the process of

i. Identifying services and characteristics associated with them
ii. Negotiating a service level agreement
iii. Deploying agents to monitor and control network, system and application component performance and
iv. Producing service level reports (4 marks)

Characteristics associated with services are

i. service parameters
ii. Service levels
iii. Component parameters
iv. Component-to-service mappings (4 marks)

Q.9 a. What is Windows Management Instrumentation (WMI)? Explain the WMI architecture in detail, with the help of an example. (8)

Answer:

WMI is the infrastructure implemented by Microsoft to support the WBEM CIM and Microsoft –specific extensions to it.

P596, 597

b. What is Embedded Web-based management? What are the benefits of Embedded Web-based management? (8)

Answer:

14.3 Embedded Web-Based Management

In embedded Web-based management (WBM), Web servers are embedded in the managed objects. Each managed object is assigned a Web address. The management application receives management information from the agents and displays it by means of a Web browser, as shown in Figure 14.3.

Web servers are more intelligent than SNMP agents, which mostly read counters and pass information to the manager or respond to a ping. SNMP agents can send unsolicited basic traps to the manager. However, a Web agent could be sophisticated. For example, it could gather RMON information. Communication between an agent and the manager application is HTTP. For small offices, whose management requirements are minimal, the browser could monitor the Web agents directly, without any management application software. Thus embedded Web agents in network elements greatly simplify network management for network administrators.

Another benefit of embedded WBM is that we can take advantage of portable tools to write the Web agent. For example, the Web agent and server could be written in Java, an interpretive programming language with built-in Web-enabled capabilities. The Java virtual machine (Java interpreter) is available for a variety of platforms. The browser also is portable. The two most popular browsers, Netscape Navigator™ and Microsoft's Internet Explorer™, are also available on multiplatforms. The numerous benefits of using Java for Web-based management applications have been enumerated [Hyde D].

Commercial network products with built-in Web agents are now available, but they are based on proprietary protocols. For example, Hewlett-Packard produces Web-based

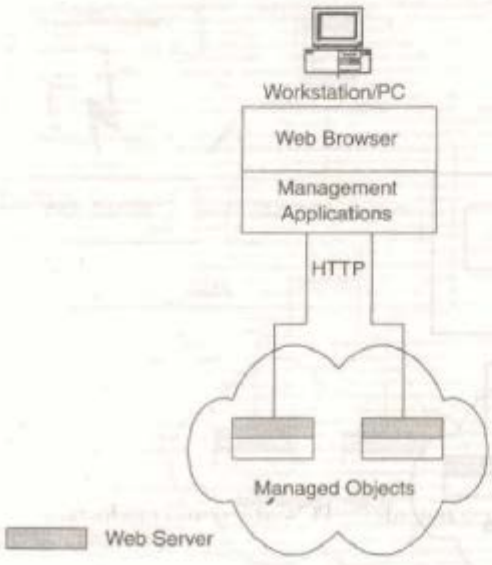

Figure 14.3 An Embedded WBM Configuration

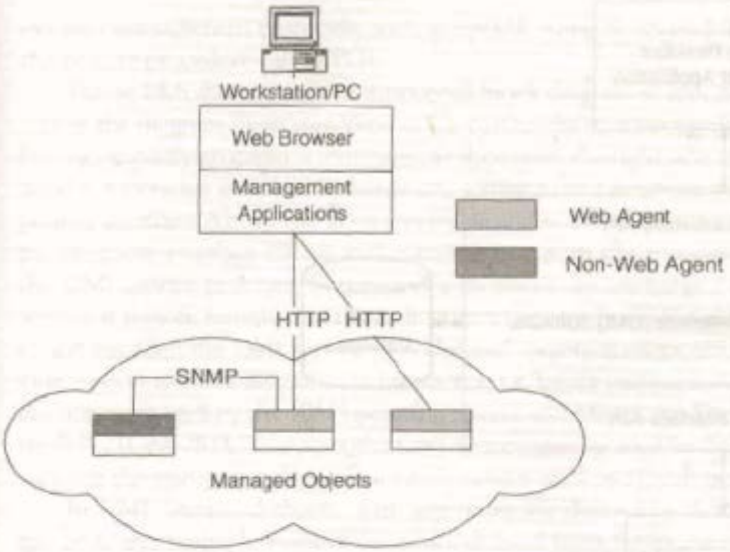

Figure 14.4 The Hewlett-Packard Embedded Agent Configuration

management agents in hubs and switches. Figure 14.4 shows the configuration of both Web and non-Web agents. Web agents function and provide data much the same as RMON does. Communication to the manager application/Web browser, called the HP AdvanceStack Assistant™, is via the HTTP transport protocol. As shown in Figure 14.4, non-Web agents (an SNMP agent is shown) are managed by a Web-agent. This method is especially beneficial for two reasons. First, a network element without a Web agent can be managed in a Web-based management environment. Second, the configuration enables remote probing of switched LANs. As we pointed out in Chapter 8, an expensive means of measuring network statistics is to have a LAN probe in each LAN segment. The Web agent provides an alternative method of measuring statistics. As shown in Figure 14.4, a limited set of statistical data on a non-Web managed device is collected through the Web server and transmitted to the management application. It is limited in that no packet capturing is done.

TEXT BOOK

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