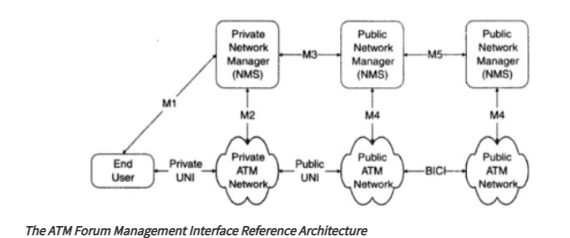
**Question 1. Explain M1,M2 and M4 interface in detail(5M /10M)**

* i. The ATM Forum interface reference architecture identifies a series of management interfaces numbered Ml through M5.
* ii. M1 and M2 are the interfaces between a private NMS and either an end user or a private network, respectively. The end user can be a workstation, ATM switch, or any ATM device. A private ATM network is an enterprise network.
* iii. A private network management system can access its own network-related information in a public network via an M3 interface to the public network management system.
* iv. The public NMS responds to the private NMS via the M3 interface with the relevant information or takes the action requested.
* v. The M4 interface is between the public NMS and the public network. The final interface, M5, is between the NMSs of two service providers. The ATM Forum has not yet specified this interface.
* vi. The ATM framework defines five different M-interfaces for management see Figure 1.



* The ATM Forum Management Model:

i. The Network Management Working Group of the ATM Forum has developed an end-to-end generic management model that encompasses private and public networks and lays out standards for interworking between them.

ii. The model defines gateways between SNMP and CMIP systems, and between standards-based and proprietary systems.

iii. Five key management interfaces are defined in this model, labelled M1-M5.

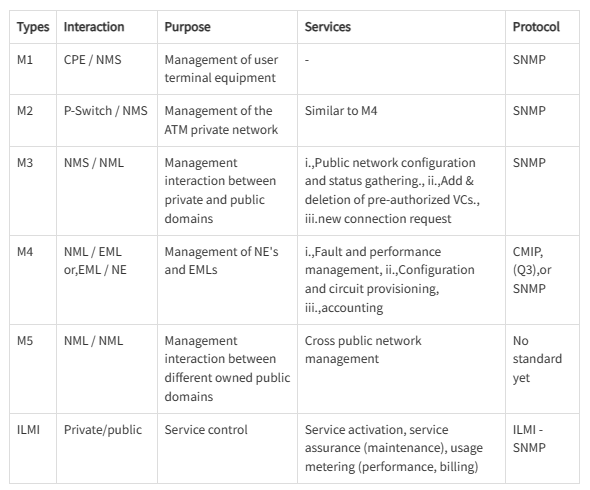
iv. M1 is concerned with the management of the end-user equipment connecting to either private or public switches.

v. M2 undertakes management of private ATM switches and networks. Private ATM network management is addressed through M1 combined with M2. M4 deals with their public ATM switches and networks. M3 is the link between

vi. private and public networks, used for exchanging fault, performance and configuration information.

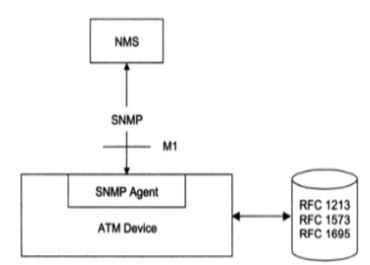
vii. Finally, M5 supports interactions between any two public networks. The definition of these interfaces allows a complete management service, ranging from a global view of the network (M5 management interface) to the management of individual elements (M1 management interface).

viii. In some cases, several management interfaces use the same information from a management information base (MIB) tree, see Table1.



* **M1 Interface: Management of ATM Network Element**

i. The M1 interface is between an SNMP management system and an SNMP agent in an ATM device, as shown in Figure2.



***SNMP ATM Management (M1 Interface)***

ii. Four entities, ifInNUcastPkts, ifOutNUcastPkts, ifOutQLen, and ifspecific have been deprecated. The interfaces (interfaces) and ifMIB (IF MIB) groups under the mgmt. node.

* **M1/M2 Interfaces and the ILMI Implementation:**

i. Interim Local Management Interface (ILMI), which is an implementation of the M I /M2 interfaces, enables the exchange of status, configuration, accounting and control information between any two ATM devices - such as two ATM switches - across a user-to-network interface (UNI).

ii. For ILMI to function, every ATM switch or network terminator and every ATM network that deploys a public or private network UNI must be equipped with a UNI Management Entity (UME) which supports an ILMI MIB.

iii. Two adjacent (or peer) UMEs can communicate using the common attributes provided by the ILMI.

iv. By sending SNMP commands, a UME may obtain or modify (if the object is indeed modifiable) information contained in its ILMI MIB.

v. The ILMI has been deployed by some vendors to perform management tasks across the UNI for some devices. However, since the ILMI provides a solution that is applicable only at the UNI, it cannot support the management tasks that are involved in a network comprising a range of ATM devices.

* **M4 Interface: Public Network Management**

i. The management of public ATM network is primarily the responsibility of network service providers, carriers and Postal Telephone and Telegraph (PTT) companies.

ii. They have the challenge of not only managing the public network, but also keeping up with new technology.

Question 2 :Explain the role of Bilingual manager.(2M)

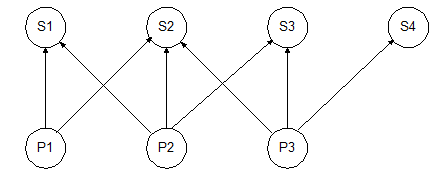


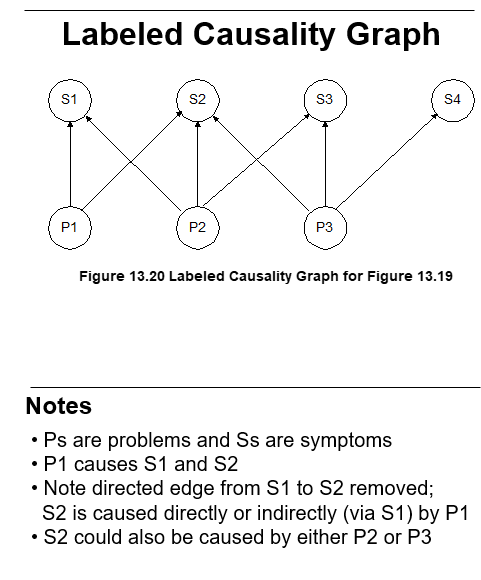
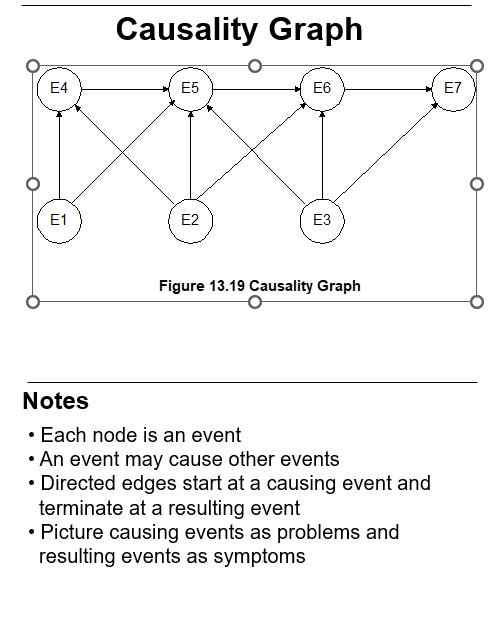
* Bilingual manager is a device that contains modules that can interpret both SNMPv1 as well as SNMPv2 messages.
* These modules are called interpreter modules. Along with the interpreter module bilingual manager has a database that contains information about the versions currently running on various agents.
* The bilingual manager does common functions of network management, this process makes use of the version field in the SNMP message PDU to identify the version of message.
* This arrangement is expensive to implement and maintain. A suitable option for the same is provided by the proxy

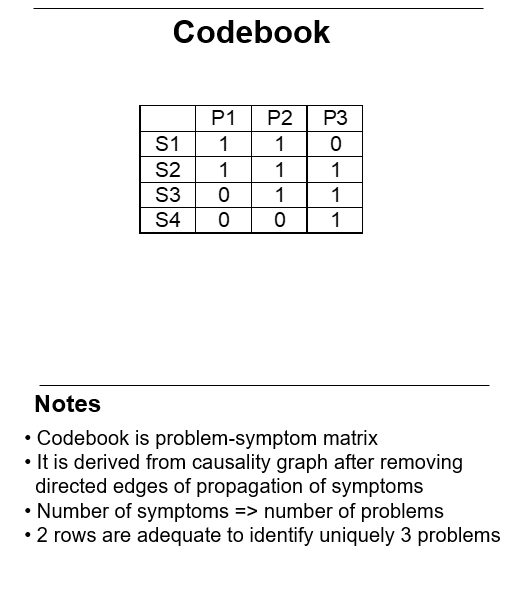
Question 3:-Explain the features of SNMP V3 protocol.(2M)

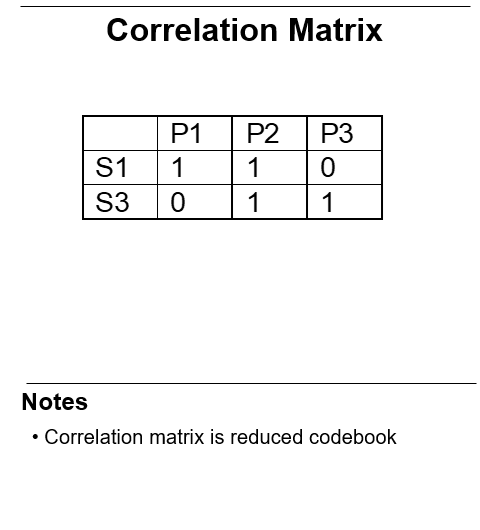
* **Modularization of document**: SNMPv3 features a modularized document structure, which allows for better organization and clarity in defining its specifications. The modularization helps in separating different aspects of the protocol, such as management, security, and operations, making it easier for developers and users to understand and implement.
* **Modularization of architecture**: SNMPv3 architecture is modularized, enabling flexibility and scalability in its deployment. It consists of several components, including SNMP engine, message processing subsystem, security subsystem, access control subsystem, and management information base (MIB) module.
* **SNMP engine:** The SNMP engine is the core component of SNMPv3 responsible for processing SNMP messages, managing SNMP operations, and interacting with the managed devices
* **Security feature:** One of the key features of SNMPv3 is its enhanced security capabilities compared to previous versions. It incorporates various security mechanisms to ensure the confidentiality, integrity, and authenticity of SNMP messages
* **Secure information:** security. SNMP configuration can be done remotely using secure communication links.
* **Access control :** Verifying that the user has access to the objects that are requested.

Question 4:Generate the codebook for the given labeled causality graph (5M).









Question 6:-Define community profile(2M)



MIB view

* + An agent is programmed to view only a subset   
     of managed objects of a network element

Access mode

* + Each community name is assigned an access   
     mode:: read-only and read-write

Community profile: MIB view + access mode

Operations on an object determined by community   
 profile and the access mode of the object

Total of four access privileges

Some objects, such as table and table entry are   
 non-accessible

Question 7:Compare RMON1 and RMON2(2M / 5M)

* RMON1: Ethernet RMON groups (rmon 1 - rmon 9)
* RMON1: Extension: Token ring extension (rmon 10)
* RMON2: Higher layers (3-7) groups (rmon 11 - rmon 20)

Ten groups divided into three categories

* + Statistics groups (rmon 1, 2, 4, 5, 6, and 10))
  + Event reporting groups (rmon 3 and 9)
  + Filter and packet capture groups(romon 7 and 8)

Groups with “2” in the name are enhancements with RMON2

RMON2

* Applicable to Layers 3 and above
* Functions similar to RMON1
* Enhancement to RMON1
* Defined conformance and compliance



RMON 2 groups

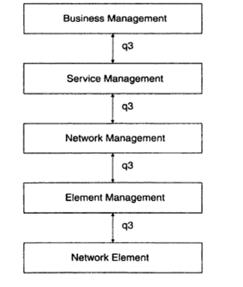


Question:8 Draw the ATM network reference architecture(2M)

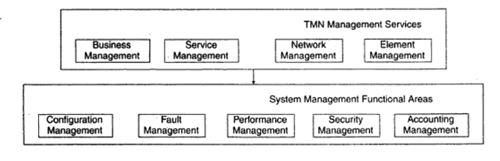


Question 9:Describe TMN layered architecture.(5M)

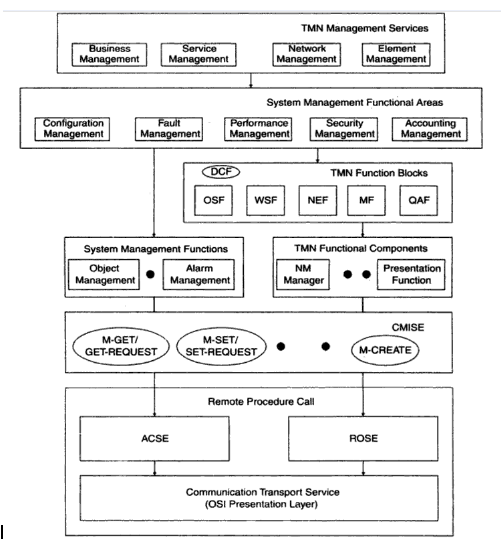
* The TMN services are grouped and presented as TMN layered architecture, as shown in Figure1.
* ii. The lowest layer is the network element layer comprising network elements such as switches, routers, bridges, transmission facilities, etc.
* iii. The next layer, the network element management layer, which manages the network elements.
* iv. The third layer is the network management layer, which manages the network. The network management functions in this layer include bandwidth, performance, and quality of service, end-to-end flow control, and network congestion control.
* v. The network element layer and network element management layer is vendor dependent, whereas the network management layer is not.
* vi. The service management layer is concerned with managing the services provided by a network service provider to customers or to other network service providers.
* vii. They include services such as billing, order processing, complaints, and trouble ticket handling. The top layer is the business management layer. It is concerned with managing the operations of a communications business, including fiscal considerations, human resource needs, project management, and customer needs and satisfaction.
* viii. The TMN reference point between the various service layers is q3. It is the standard interface between the operations system, network element, and mediation functions.



* ix. TMN management services are classified by OSI system management functional area. These areas are the five OSI application functions, configuration management, fault management, performance management, security management, and accounting management.
* x. The TMN management services and the system management functional areas are presented in Figure2.



* xi. The four TMN management services—business, service, network, and element—are at the top of the hierarchy. They invoke the system management functions defined as the five components comprising the system management functional areas: configuration, fault, performance, security, and accounting.
* xii. The management applications in the system functional areas perform either system management functions or TMN functions. The TMN function blocks OSF, WSE NEE ME and QAF consist of TMN functional components such as the NMF and MIB. The data communication function (DCF), although not part of the TMN function blocks, is included for completeness.
* xiii. The system management functions include object management and alarm management. In Figure 3, we could have embedded the system management functions in TMN function blocks and TMN functional components, but we show them separately in order to present a non-OSI environment.
* xiv. Figure3 also shows the OSI primitive services of M-GET, M-SET, and so on. Equivalent SNMP services are GET-REQUEST, SET-REQUEST, and so on. The TMN environment is a distributed environment.
* xv. The applications communicate remotely with the communication transport service by means of the RPC. In the OSI model, the RPC is accomplished with ROSE and ACSE. The former does the remote operation and the latter establishes and releases the application association. In the SNMP management model, the remote operation is accomplished by using the RPC and TCP/IP.

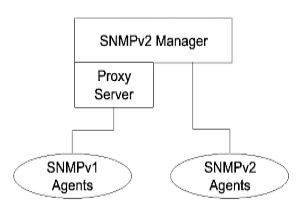


Question 10:What is an SNMP proxy server.(2M)

**Proxy Server:** - i. The SNMPv2 proxy server configuration is shown in Figure12.

ii. The requests to and responses from, as well as traps from, SNMPv2 agents are processed by the SNMPv2 manager with no changes.

iii. A proxy server is implemented as a front-end module to the SNMPv2 manager for communication with SNMPv1 agents.



Question 11:Explain user security model of SNMP V3.(5M)

Based on traditional user name concept

USM primitives across abstract service interfaces

* + Authentication service primitives

Authenticate Outgoing Msg

Authenticate Incoming Msg

* + Privacy Services

Encrypt Data

Decrypt Data



Processing secure incoming message reverse of secure outgoing message

Authentication validation done first by the authentication module

Decryption of the message done then by the privacy module

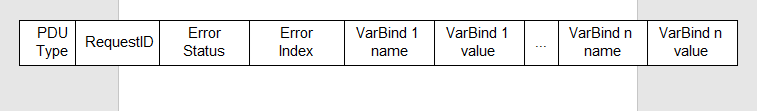


USM invokes privacy module w/ encryption key and scoped PDU

Privacy module returns privacy parameters and encrypted scoped PDU

USM then invokes the authentication module w/authentication key and  
 whole message and receives authenticated whole message

Question 12:Draw and describe SNMP PDU format.(2M)



Question 13:Compare SNMP V2 and SNMP V3(2M)



Question 13:Explain the threats to network management information during transit?(2M)



Any communication networks main concern is having proper and efficient security management. Any network management process has to ensure the following three security concerns :

1. Secure communication
2. Secure access to data
3. Physical security of network devices

These three security concerns shape various policies and procedures instituted under the process of security management. This section talks about such policies and procedures that are implemented to ensure secure communication for all the users.

Along with policies and procedures this section also gives an introduction on the equipments needed to implement these security measures.

Question 14:Explain the TMN information architecture.(2M)



Management of telecommunication networks as a whole relies on communication of proper information between managing entities.

It can be thought of as an information processing application, where the information communicated by various devices has to be understood correctly by the applications. To effectively manage complex networks and support network operator/service provider business processes, it is necessary to exchange management information between management applications implemented in multiple managing and managed systems. Thus, telecommunication management is a distributed application.

The TMN information architecture, in order to promote interoperability, is based on standardized open management paradigms that support the standardized modelling of the information to be communicated.

TMNs information architecture uses an object oriented approach and is based on OSIs Management Information Model. According to this model, entities to be managed are viewed as objects. These objects are described in terms of :

1. Attributes, which are the properties or characteristics of the object.

2. Operations, which are performed upon the object.

3. Behavior, which is exhibited in response to operations.

4. object. the by emitted are which Notifications,

Question 15: Explain Rule based event correlation technique.

* Rule based reasoning is one of the earliest event correlation techniques. RBR makes use of basic principle of if condition.

if (condition)

then (action)

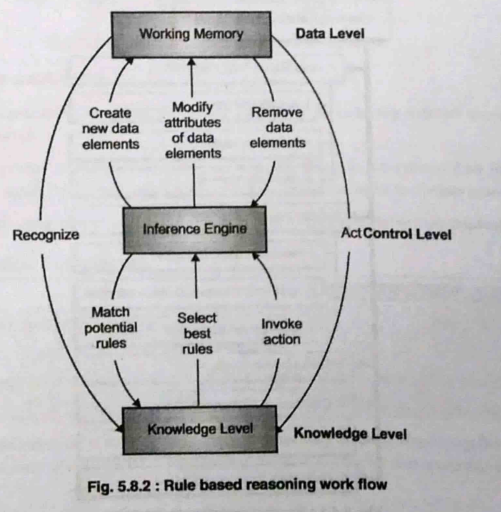
* In this case when an event occurs it is compared to some predefined conditions, if a match is found a corresponding action is performed. The main parts of a typical RBR system are the following :

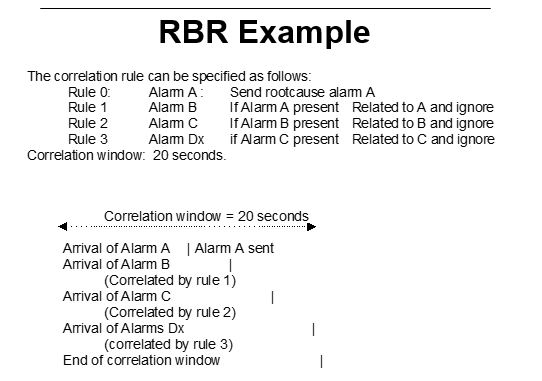
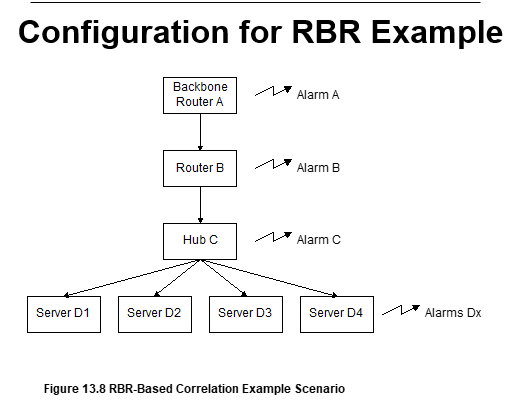
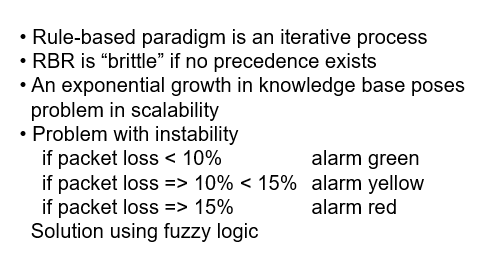
1. **Knowledge base:** It represents knowledge level, it contains the list of conditions and actions that can be used to compare any new event.

(ii) Inference engine: Inference engine works with knowledge base; compares the current state of network with set of rules to determine correct action to be taken for error resolution.

(iii) Working memory: This block contains the current status of the network being monitored. This is stored as a set of memory elements. The state can contain topological state of the network to be monitored.

* Fig. 5.8.2 shows the working of a rule based system used for network management. It consists of the basic components of any RBR system. When a network goes into faulty state, working memory detects the change.
* The inference engine cooperates with the knowledge base and compares the current state with the predefined rules. Based on the comparison, an action is selected.
* The selected action is implemented on the working memory by the knowledge base. This action could initiate another event which is updated in the working memory. This condition match and action process continues till a desired state is achieved in the working memory.
* Rules are made up by experts in the field of management. When any faulty event occurs, a match in the rules has to be exact and it should invoke an exact action.
* If the action is not matched then the system enters a "Brittle" state. In a typical RBR based event correlation there are numerous rules and based on the size of the network the rule base increases exponentially.





Question 5:You are administrating the 24000 workstations in an organization. You are pinging each station periodically. The message size in both direction is 280 byte long. The NMS you are using is on 10 Mbps LAN, which function with 30% efficiency. What would be the frequency of your ping if you were out to exceed 5% overhead. (5M)

Total number of workstations = 24000

Total Message size (both sides) = 280 bytes = 280 - 8 bits

10 Mbps LAN with 30 % efficiency implies total available bandwidth is 3 Mbps (CSMA/CD protocol)

Since, a maximum possible overhead of only 5% is allowed, the available bandwidth for management traffic = 3 x 5/100 = 0.15 Mbps

Time period to complete ping cycle = (280 x 8 x 24000)/ 150000 = 358.4 sec

Ping frequency for each machine = 1/358.4 = 0.00279 Hz