**Module 4**

1. **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. Notifications, which are emitted by the object.

1. **Explain the need of TMN?**
2. **Efficient Management of Complex Networks:**

**Diverse Elements**: Modern telecommunications networks consist of various types of network elements such as exchanges and transmission systems from multiple vendors. TMN provides a unified management framework to handle this diversity.

**Scalability:** As networks grow in size and complexity, the need for a scalable management system becomes critical. TMN offers a scalable solution that can accommodate expanding network requirements.

1. **Standardized Interfaces and Protocols:**

**Interoperability**: TMN defines standardized interfaces, protocols, and messages which facilitate interoperability between different operations systems (OSs) and telecommunications equipment. This ensures seamless communication and management across diverse systems.

**Generic Models:** By using generic network models and standard interfaces, TMN enables general management of diverse equipment, networks, and services, reducing the need for custom solutions.

1. **Comprehensive Management Functions:**

**Fault Management:** TMN helps in detecting, isolating, and resolving network faults quickly, ensuring high reliability and availability of the telecommunications network.

**Performance Management:** Continuous monitoring and optimization of network performance are essential for delivering high-quality services. TMN provides tools for performance management.

**Security Management:** Effective security management is crucial to protect the network from cyber threats. TMN includes mechanisms for access control, authentication, and other security functions.

1. **Support for Multiple Management Areas:**

**Planning and Installation:** TMN supports the planning and installation of network components, ensuring they are set up correctly and efficiently.

**Operations and Administration**: Daily operations and administrative tasks are streamlined through the TMN’s standardized processes and tools.

**Maintenance and Provisioning**: TMN assists in the maintenance of network elements and the provisioning of new services, ensuring continuous and reliable service delivery.

1. **Automation and Human Intervention:**

**Automated Functions**: TMN enables many management functions to be carried out automatically, reducing the need for human intervention and minimizing the risk of human error.

**Human Operators:** While automation is significant, some functions are still performed by human operators. TMN provides interfaces and tools to support these operators effectively.

1. **Organized Architecture:**

**Framework for Management:** TMN provides a structured architecture that organizes the management functions, making it easier to manage large and complex networks.

**Integration with Other Systems:** The TMN framework allows for integration with other management systems and networks, ensuring a holistic approach to telecommunications management.

1. **Communication and Coordination:**

**Between TMN and Networks:** TMN facilitates communication between itself and the telecommunications networks and services, ensuring coordinated management activities.

**Between TMNs:** TMNs can communicate with each other, enabling coordinated management across different parts of the network or different networks.

1. **Explain TMN Conceptual Model?**

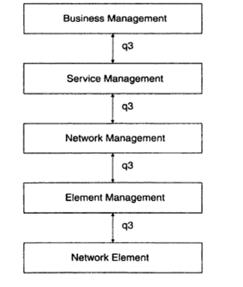
* A TMN can vary in complexity from a very simple connection between an OS and a single piece of telecommunications equipment to a complex network interconnecting many different types of OSs and telecommunications equipment.
* A TMN may provide management functions and other communications both between the Operations Systems (OS) themselves, and between OSs and the various parts of the telecommunications network.
* A TMN may also offer communication between two TMNs of different networks in order to support the management of international and national telecommunications networks.
* A telecommunications network consists of many types of analog and digital telecommunications equipment and associated support equipment, such as transmission systems, switching systems, multiplexes, signalling terminals, front-end processors, mainframes, cluster controllers, file servers, etc.
* When managed, such equipment is generically referred to as network elements (NEs). Fig. 4.1.1 shows the general relationship between a TMN and a telecommunications network which it manages.
* A TMN is conceptually a separate network that interfaces a telecommunications network at several different points to send/receive information to/from it and to control its operations. A TMN may use parts of the telecommunications network to provide its communications.

A diagram of data communication network

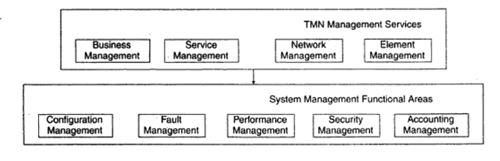
Description automatically generated

1. **Describe TMN layered architecture? TMN Services & Functions**

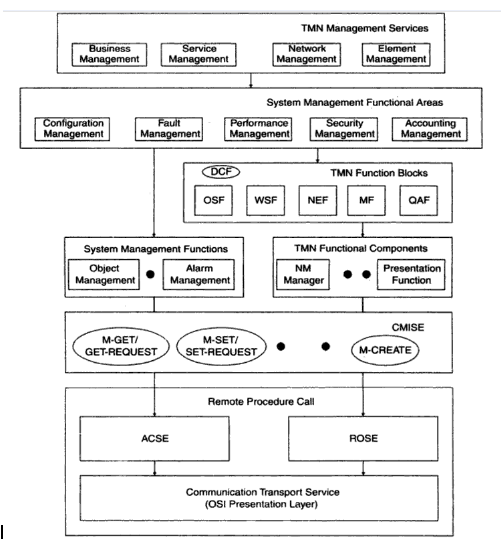
* The TMN services are grouped and presented as TMN layered architecture, as shown in Figure1.
* ii. The lowest layer is the network element layer comprising network elements such as switches, routers, bridges, transmission facilities, etc.
* iii. The next layer, the network element management layer, 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.



**Describe FACPS?**

1. **Fault**

* Fault management is responsible for detection and isolation of problems causing network failure.
* NMS monitoring underlying networks are capable of continuously monitoring network devices and raise an alarm in the event of failure. This failure can be automatically rectified in some cases (self-healing networks). In cases where automatic resolution is not possible a trouble ticket is raised.
* Proper policies and procedures are specified for such fault resolution. SNMP makes use of TRAP messages to generate unsolicited messages for a manager. Whenever a network element fails a suitable TRAP message B generated using SNMP PDU and sent to the manager.

1. **Configuration**

* Configuration management addresses the setting and changing configuration of network parameters and network elements.
* Information about configuration has to be carefully documented and updated as network evolves and new services and devices are added. This becomes essential for a time when network goes under maintenance or upgradation.
* Configuration management maintains a repository of current and running configurations of device.
* In SNMP, SET messages are used by NMS to change configuration of underlying network devices.

1. **Accounting**

* Accounting management administers cost allocation of usage of network.
* Different metrics are established to monitor and measure usage of network resources.
* Traffic data is gathered and used for this analysis. RMON assists SNMP in collecting these statistics.

1. **Performance**

* Performance management is concerned with monitoring performance of networks with respect to certain previously agreed upon parameters. This may include monitoring network bandwidth, latency and jitter statistics.
* Other statistics can also be monitored as per business requirements. These capabilities are embedded into NMS and are essential to NOC for accounting management.

1. **Security**

* Security management can cover a broad range of activities. Some of these aspects are device security, information security and protecting networks from external threats.
* Various techniques like cryptography, firewall implementation and restricting unauthorized access to data is used for implementing security management.
* SNMPv1 security mechanisms are not that strong as it only relies on community names and read write privileges for providing security.
* This is addressed in SNMPv2 by introducing new objects in MIB II structure, but still is inadequate. SNMPv3 addresses security management by introducing a modular approach.

Functional models are also sometimes referred to as 'FCAPS' models. These activities together cover differenttasks that are to be done as a part of network management.

**Module 5**

1. **What are the functional requirement of NMS design?**

* **Scalability:** The NMS must be able to handle the increase in subscribers, network equipment such as servers, routers etc.
* **Heterogeneity:** The NMS software must be versatile to incorporate advancements in network protocols, network devices in a simple manner.
* **Geographic Spread:** The NMS is usually at an isolated place away from the actual network devices and subscribers, hence one must expect the links to have limited bandwidth and the reliability of the link to be low. Also expect the link to be shared by subscriber data and have high latency.
* **Bursty Load:** Network Management is usually done at regular intervals of time, i.e measure traffic throughput every 1 min, while checking for link delay for every second. Such measurements are predictable and expected since we set the intervals, however during network outages i.e. link failures, equipment failures one gets a burst of information which is not predictable and our NMS should be able to handle such traffic.
* **Real-Time Response:** Usually when one expects a network failure, the NMS receives a trap message and NMS is expected to respond. This response can vary depending on the nature of the event, i.e. the NMS can send commands to divert the flow of traffic if a device has gone down or may need to send a page to the network engineer on call to solve the problem.
* **Hardware Provisioning:** One may need extra servers to take on the load if the number of requests to an NMS increases. AWS is an example where we can spin up an extra service to accommodate the extra load and bring that service down when the load reduces. An NMS must be aware of the average load and when the load will increase to spin up a new service of itself.
* **Batch processing:** The NMS is expected to get bulk messages every interval of time and the NMS is expected to process all of these messages irrespective of the load. The NMS must be capable of separating the critical messages from the rest and also have enough processor bandwidth to generate a suitable response for such events.
* **Diverse Users:** NMS is not only handy for network engineers but for a variety of users such as administrators, operators and subscribers. Administrators can use the NMS to perform audits of the entire network, operators use the NMS to monitor the system and bring about changes, while the subscriber can use the system to get information such as billing, network usage and network status. Enterprise customers can use such data to monitor if the ISP is adhering to the agreed upon SLA.
* **Ease of use:** The NMS UI should be both easy to use to the people who prefer a UI and also offer a CLI based schema for engineers to have better control and faster use.
* **Security:** The NMS network must be secure and should identify Denial of service attacks and other malicious activities and must defend against attacks since they have management access to network devices.

1. **What is fault management? Describe 5 steps process in fault management?**

* Service failure or unavailability of any IT service is a common fault with network management. Restoring a service for users is a responsibility of NOC. This involves detection and isolation of problems that caused service failure. In some situations, the network will do this automatically.
* Such networks are called self-healing networks. But in some situations when automatic recovery or healing is not possible, Network Management Systems (NMS) are used to detect failures.
* These failures can be in form of component failure and a NMS raises appropriates alarms and sends notifications to the concerned team. Fault management is a five-step process:

A diagram of fault management process

Description automatically generated

* When a service fails or any device malfunctions an alarm is raised to the network management system.
* The most important part of fault management is service restoration. Root cause analysis of the fault or problem resolution takes a lower priority.
* When a service failure occurs a ticket is generated either automatically (NMS has that option) or manually by an engineer. This ticket contains a detailed description about the problem.
* All the possible available information about service failure events is present in the ticket. This ticket is then assigned to the I & M group for actual maintenance or repair work if necessary.
* Generally, any ticket contains tracking number of the request, affected service, affected user, any SLA that is associated with the disrupted service.
* Once service has been restored and the underlying problem resolved, the ticket is closed.

1. **Fault Detection**

* Fault detection process is generally automated in any complex network management process. There are two techniques to implement fault detection. Polling method and Trap generation.
* An application program sends regular ping commands and waits for response. If a predefined number of ping requests fail, connectivity to that device is declared broken and NMS is informed about the failure.
* To optimize network performance, the number of ping messages and the frequency of ping messages are balanced with data traffic.
* Trap generation is another method where a device upon failure informs the NMS, SNMPv1 makes use of TRAP message to implement fault detection.

1. **Fault Location and Isolation**

* Fault location is an important step in resolving a fault and restoring a service. One thing to notice is that a single fault in the network can affect multiple services at the same time raise multiple different alarms.
* It is important to identify the source of failure to restore services. Fault location is generally implemented by using the network topology as a guide map.
* The origin of the problem could be traced by walking down the topology tree to where the problem starts. Once the source of failure has been located diagnostic tool and procedures are used to resolve the problem.

1. **Service Restoration**

* Upon detection of fault immediate root cause analysis may not be possible sometimes. In many cases service restoration takes a higher priority than root cause analysis.
* This is important because a service not being available may translate into direct monetary loses to the service provider. There can also be indirect losses as a result of non-compliance to SLAs.

1. **Root Cause Analysis and Problem Resolution**

* A single problem in enterprise network can result into large number of faults. It is important to correlate these faults to find a common problem. This is done by analysis the trends in which faults occur.
* Historical tickets are analysed to get deeper understanding of a recurrent problems. Along with this, various event correlation techniques can also be used to observe patterns that cannot be so easily identified. Such analysis is called root cause analysis and help find the root cause of any given faults or group of faults.
* Once the core problem area is identified network administrators can take necessary steps to provide a more permanent solution to the problem. This will involve changing configuration of network elements to optimize the services provided by it.

1. **What is the difference between accounting management and performance management?**

**Performance management**

* The main task of network management systems is to monitor and control the network infrastructure.
* As computer networks increase in size, heterogeneity and complexity, effective management of such networks becomes difficult. An hour of network downtime means an hour of lost business and leads to monetary losses.
* Pro-actively managing the Network's health and performance is indispensable for any business and is something which the administrators of large networks have to implement diligently.
* When it comes to defining network performance management it cannot be restricted to a single activity. Network performance is dependent on a large number of parameters and managing performance many times becomes optimizing these interlinked parameters.
* It is important to note that performance management is not an independent activity;

A diagram of a performance management

Description automatically generated

**Performance Metrics**

* Performance management typically takes help of some metrics from all across the network to optimize network performance.
* These metrics are analyzed and modified at granular level to achieve desired network performance. Some of the commonly used performance metrics are:
  + Network delay
  + Packet losses / errors
  + Response time
  + Throughput
* Many other metrics are used to attune the network to desired performance level. Together they are used to determine levels of network availability and network reliability.
* Response time of a network also depends upon application response time. In a typical client-server network, application response time determines the network response time.

**Data Monitoring**

* Data flow in network is monitored for abnormal behaviour in a network. Various mechanisms are available for implementing traffic monitoring.
* Network management system sets threshold for various parameters which are remotely monitored by RMON probes.
* RMON MIB allows collection of statistics on the local network. In event of a failure or when one of the set thresholds is crossed, alarms are generated. SNMP makes use of Trap messages to inform NMS about a policy violation. NMS has the ability to report these alarms which can be cleared automatically or manually cleared by an operator.

**Problem Isolation**

* Performance management aims to increase reliability of both network and services, for this efficient and timely isolation of problems are important.
* A single break in network connectivity can affect a large number of services using the network.
* Performance management works in close association with fault management to ensure timely resolution of problems. This involves processing performance data to uncover network faults.
* Proactive monitoring is another aspect that helps prevent faults before they occur.

**Performance Statistics**

* Performance Statistics are used in tuning network performance and validating Service Level Agreements (SLA). Statistics are generated by RMON probes placed on the local network.
* RMON allows micro-level monitoring of collected data as they are generally placed on local networks.
* Generating and transmitting large amounts of network statistics can affect network performance. This is overcome by using RMON probes which analyze locally.
* Instead of transmitting raw, unprocessed data to central location, RMON probes only sent statistics that are requested by NMS.
* Various statistics allow measurement of quality of service and improve network performance.
* Apart from QoS, performance statistics bring about improvements in bandwidth, link utilization and traffic utilization in the network.

**Accounting management**

* Accounting management is also termed as billing management; it is one of the least developed functions of network management.
* Accounting Management enables the measurement of the use of network services. Based on this measurement appropriate costs to the service provider and charges to the customer are determined.

**Accounting management includes functions to:**

* 1. **Inform:** users of the cost incurred, or the resources consumed.
  2. **Limit:** Enable accounting limits to be set and associate proper tariff for usage of resources.
  3. **Cost Combine**: Enable combing cost when multiple resources are used.

**Accounting management performs following functions:**

1. **Usage measurement**

* Usage monitoring is performed by different operating systems (OS) and they collect data from different network
* elements, often in real time. This information is used to maintain records of billing activities.

1. **Tariffing/ pricing**

* Tariff to be charged to users is dependent on usage of network services; operation systems correlate the usage of network elements and services with appropriate pricing models.

1. **Collections and finance**

* The Collections and Finance group encompasses functionality to transfer financial data for the TMN for such purposes as administration of customer accounts, informing customers of balances and payment dates and receiving payments.

1. **Enterprise control**

* Enterprise control group support the flow of data needed to exercise diligence over the proper flow of funds within the enterprise and between the enterprise and its owners and creditors.

1. **List and describe event correlation techniques? What is role of event correlation technique for root cause analysis? Describe three scenarios that require event correlation techniques and explain clearly why each one needs it?**

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

if (condition)

then (action)

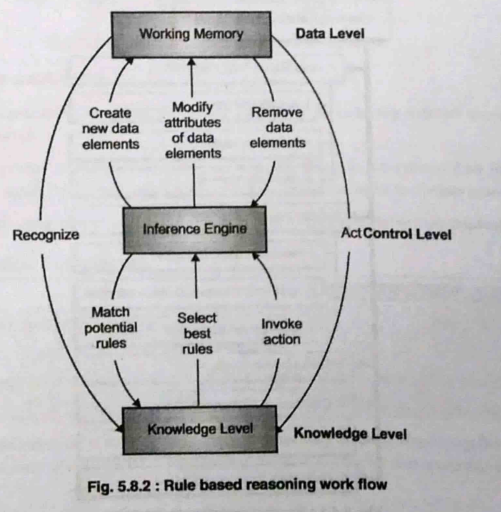
* In this case when an event occurs it is compared to some predefined conditions, if a match is found a corresponding action is performed. The main parts of a typical RBR system are the following :

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.



**A paper with text on it

Description automatically generated**

**A paper with text and words

Description automatically generated**

**A paper with text on it

Description automatically generated**

**Module 6**

**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.

A diagram of a network diagram

Description automatically generated

* 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.

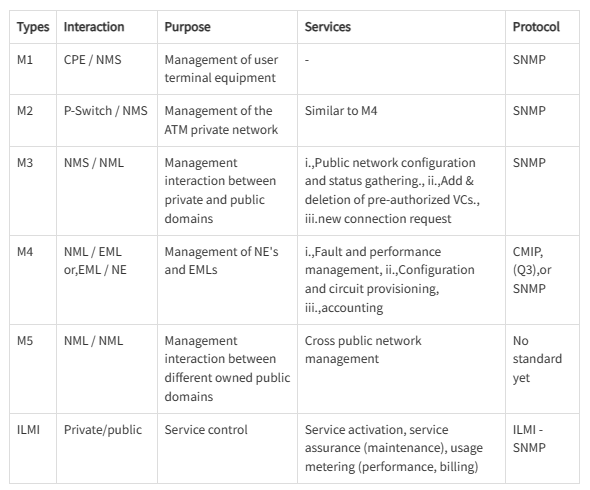
iv. M1 is concerned with the management of the end-user equipment connecting to either private or public switches.

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).

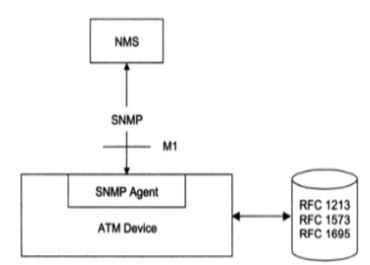
viii. In some cases, several management interfaces use the same information from a management information base (MIB) tree, see Table1.



**What is the role of ilmi and snmp in management**

* **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.

**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)

10 x 30/100 = 3 Mbps

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