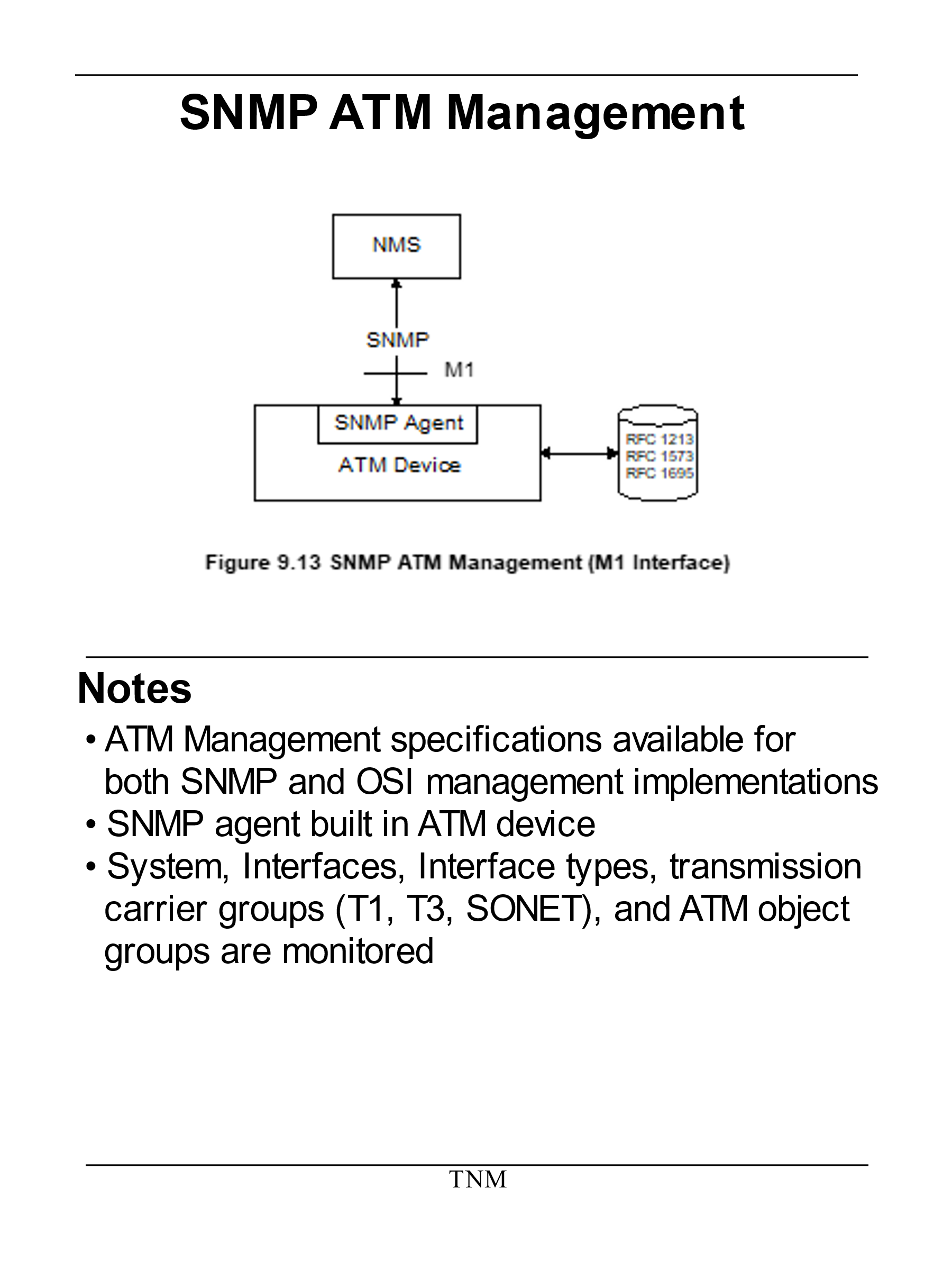
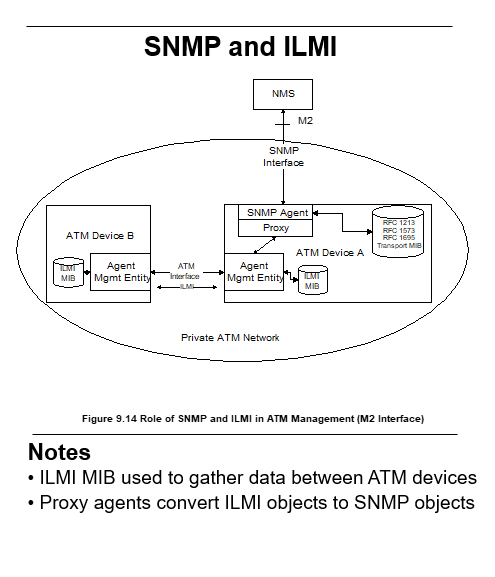
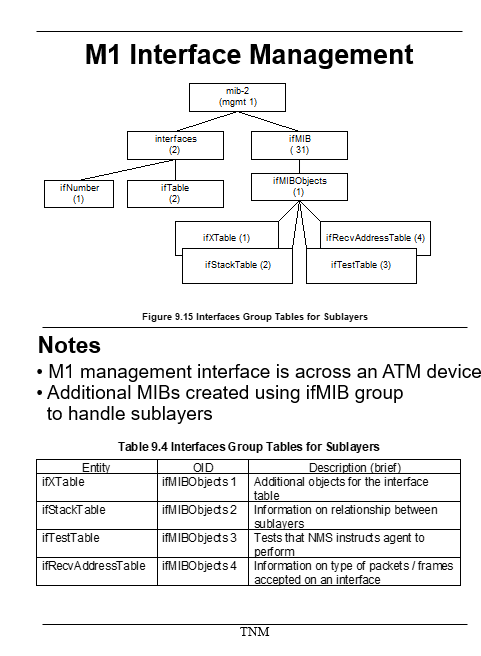
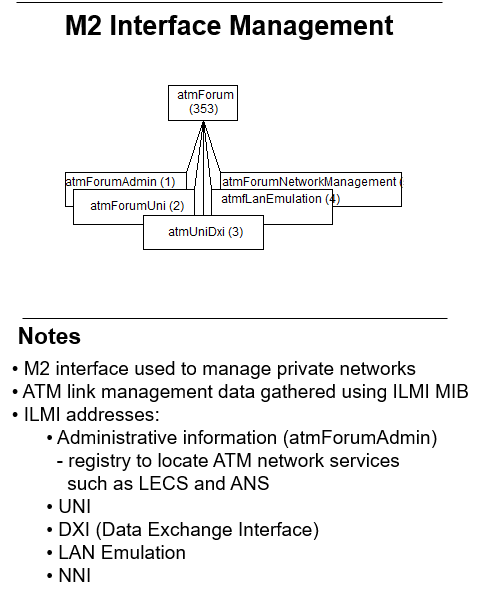
Question 1:Explain M1 and M2 interface in detail



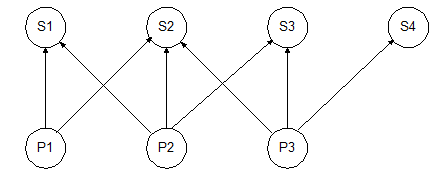


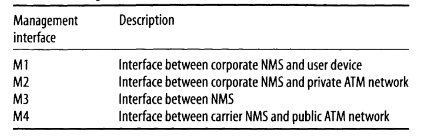
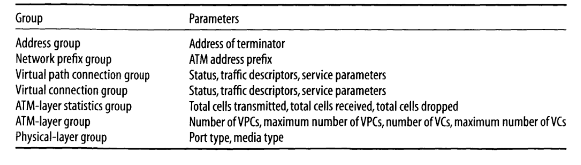




**Question 2:Explain the role of Bilingual manager.**

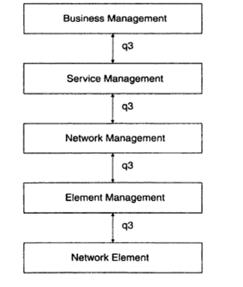
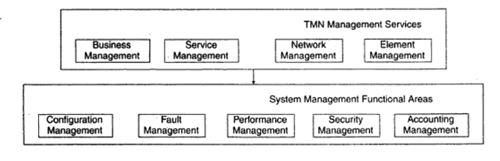
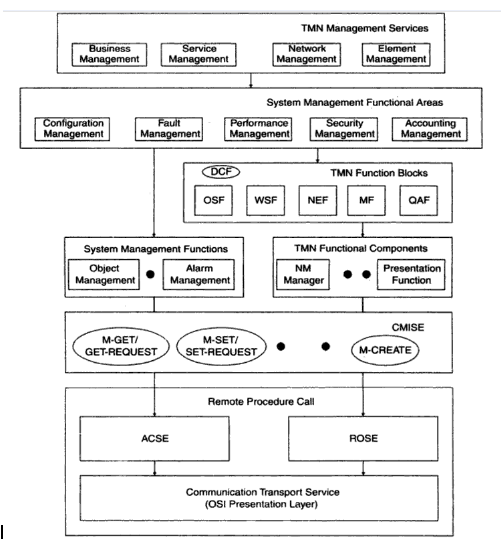
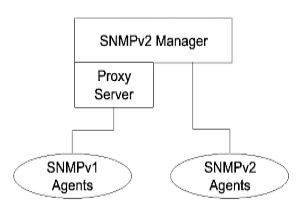
* Explain the features of SNMP V3 protocol.
* Generate the codebook for the given labeled causality graph .



* 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.
* Define community profile
* Compare RMON1 and RMON2
* Draw the ATM network reference architecture
* 
* Explain Rule based event correlation technique.
* Explain fault management? Describe five step process in fault management.
* What is the role of event corelation technique for root cause analysis?
* What is LAN Emulation?
* Explain ATM network management reference architecture.
* 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. Five key management interfaces are defined in this model, labelled M1-M5.
* iii. M1 is concerned with the management of the end-user equipment connecting to either private or public switches. M2 undertakes management of private ATM switches and networks. Private ATM network management is addressed through MI combined with M2. M4 deals with their public ATM switches and networks. M3 is the link between private and public networks, used for exchanging fault, performance and configuration information. 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 inter-face) to the management of individual elements (M1 management interface).
* iv. In some cases, several management interfaces use the same information from a management information base (MIB) tree.
* 
* **M1/M2 Interfaces and the ILMI Implementation:**
* i) The Interim Local Management Interface (ILMI), which is an implementation of the MI /M2 interfaces. ILMI 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 inter-face (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. Two adjacent (or peer) UMEs can communicate using the common attributes provided by the ILMI.
* iii) By sending SNMP commands, a UME may obtain or modify information contained in its ILMI MIB. The ILMI MIB is hierarchically organised (Table2). It contains information concerning each group listed in Table. Also defined are functions that allow retrieval and handling of information in the ILMI MIB.
* iv) 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. Thus, on its own, the ILMI does not provide the capability to manage multi-vendor ATM networks.
* 

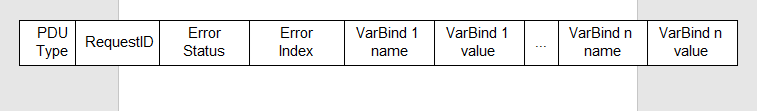


Describe TMN layered architecture.

* 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.
* 
* What is an SNMP proxy server.
* **P 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.
* 
* Explain user security model of SNMP V3.
* **MPv3 Access Control: VACM**
* • The VACM determines whether access to a managed object in a local MIB by a remote principal should be allowed.
* • The VACM makes use of a MIB that defines the access control policy for this agent, and makes it possible for remote configuration to …

|  |  |
| --- | --- |
|  |  |

* • In contrast to SNMP version 1 (SNMPv1) and SNMP version 2 (SNMPv2), SNMP version 3 (SNMPv3) supports authentication and encryption. SNMPv3 uses the user-based security model (USM) for message security and the view-based access control model (VACM) for access control.
* • USM specifies authentication and encryption. VACM specifies access-control …
* Draw and describe SNMP PDU format.



* Compare SNMP V2 and SNMP V3



* Explain the threats to network management information during transit?
* Explain the TMN information architecture.

111