1. **Explain the attributes of managed object.2M**

Notes
Managed Object:
Internet Perspective
•object ID unique ID
•and descriptor and name for the object
•syntax used to model the object
•access access privilege to a managed object
•status implementation requirements
•definition textual description of the semantics
of object type
Network Management: Principles and Practice
© Mani Subramanian 2000
3-23
ObjectType:
ObjectID and
Descriptor
circle
Access:
Access
privilege
Defintion :
Semantics-
textualdescription
Status :
Implementaion
requirements
Syntax :
modelofobject
Figure3.9(a)InternetPerspective
Chapter 3
 

1. **Explain MIB. 2M**

* The Management Information Base (MIB) is a conceptual data store that contains a management view of the device being managed. The conceptual data contained in this data store constitutes the management information.
* MIB should not be confused with a real database. It does not contain actual information about a device. It only contains information about the device which is needed by network management system.
* NMS creates a view of various network devices; this view is called the MIB. MIB discusses the semantics of objects i.e. the information about the object modeled.

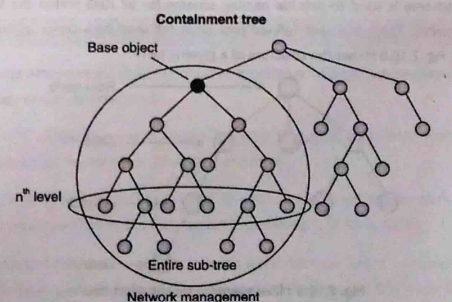
1. **Compare MDB and MIB.2M**

| **Feature** | **MDB** | **MIBs II** |
| --- | --- | --- |
| Definition | Management database Base is a repository of management information | Management Information Base is a virtual database containing network device info |
| Purpose | Store management data locally | Provides easier access to management data through SNMP |
| Structure | Typically organized in a relational database format | Organized as a hierarchical tree structure |
| Data Format | May vary depending on the implementation | Data is structured according to SNMP standards |

1. **Explain sopping and filtering in CMIP.2M**

**Scoping**

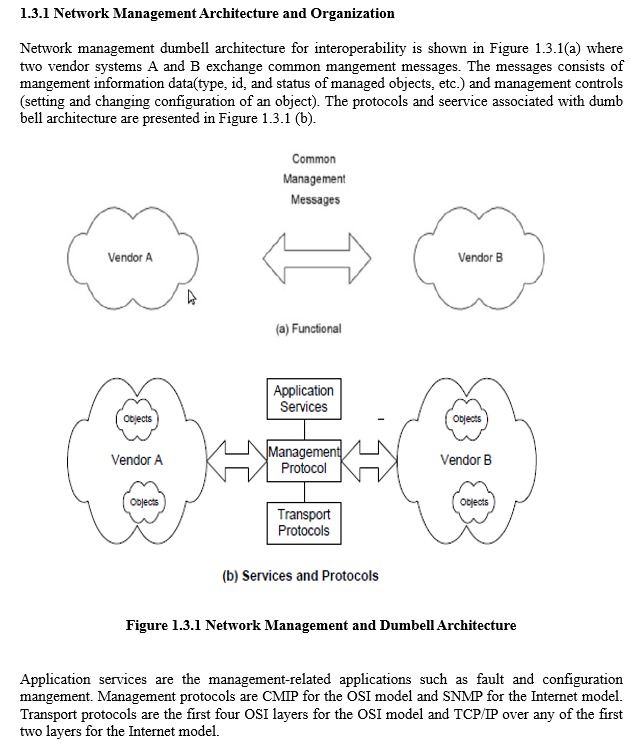
* CMISE applies additional powerful features to distinguish CMIP from SNMP. One of these features is Scoping.
* It selects objects to be operated upon by the NMS. These objects are within the managed object containment tree or Management Information Tree (MIT).
* The objects in the MIT include network devices such as routers and hosts. It also contains the list of events and operations that can be performed upon these network elements.
* Scoping operations can be divided into three categories based on the number and type of nodes on which operations are performed.
  + Base object only : In this case operations are performed only on the base node of management information tree
  + Nth level subordinate object : In this type of scoping, operations are performed on Nth sublevel with respect to the base node.
  + Base object plus all its subordinates : In this scoping mechanism rules are applied to the entire subtree associated with a base object



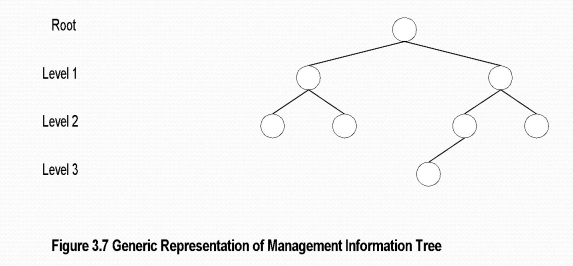
**Filtering**

* Filtering makes it possible to select certain nodes with the management information tree or the containment for applying certain operations.
* Multiple rules can be used for filtering different objects. These rules can be developed for attribute values. Multiple rules can be combined using logical operators.

1. **Explain the Dumbell architecture of network management.2M**



1. **Explain Management Information Tree.2M**

****

* A collection of managed objects and the properties implemented within a system using the schema defined by the information model is referred to as a Management Information Base (MIB).
* In network management it becomes necessary to identify managed devices with some names. Different standards use different naming methodologies. In Internet standard, a scalar structure is used to identify individual network components.
* OSI standard follows a different naming standard owing to its object-oriented methodology.
* The naming scheme for identifying the management objects results in a tree referred to as a Management Information Tree (MIT).

1. **Draw the PDU of CMIP.2M**

**Common Management Information Protocol**

* The CMIP is the communication interface with the CMISE. It generates a PDU for a message. The PDU format generated by CMIP is a modification of the generic ROSE PDU format. The invoke ID field is the PDU identifier and is used in correlating the response. The operation value is determined by the appropriate operation/ notification as in Table.

* For example , the get operation will have an operation value of 3. the next two fiels in the CMIP PDU are the managed object class and the managed object instance. The term base object is used in connection with retrieval using the get commands by specifying a base object. The information field is a group of fields describing operation-specific data.

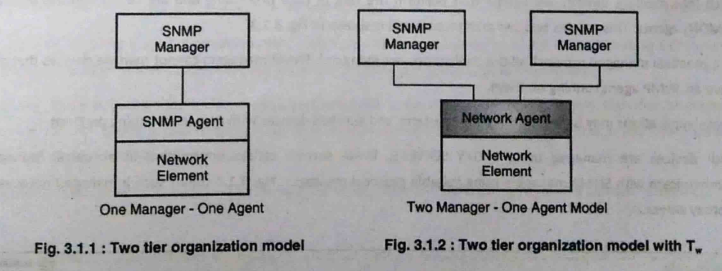


1. **Compare Agent process and Manager process.2M**

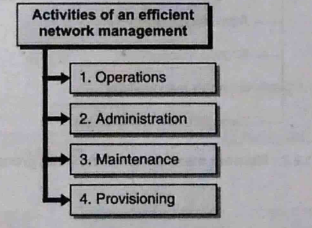
| **Aspect** | **Agent Process** | **Manager Process** |
| --- | --- | --- |
| Role | Runs on managed devices (e.g., routers, switches) | Runs on centralized management system or server |
| Functionality | Collects and stores management data | Collects, analyzes, and manages management data |
| Data Source | Provides information about the device’s status, configuration, and performance | Gathers information from multiple agents for monitoring and control purposes |
| Initiates Communication | Typically passive responding to requests from manager | Actively initiates communication with agents for monitoring and control purposes |
| Examples | SNMP agent on a router <br> SNMP agent on a server | Network management system <br> SNMP manager software |

1. **Explain the two-tier architecture of SNMP. -2M**

* SNMP models generally operate in client/server or more specifically manager/agent mode. Managers can query and change configuration of managed devices by sending suitable protocol messages to agent of managed device.
* The organization model of SNMP tells us how a manager and an agent interact with each other and the hierarchy in which managers and agents are organized in a management network.
* Initial organization of SNMP is a simple two tier model where an agent is a process running on the managed device and manager is a process (program) running in the NMS.
* This organization is shown in figure where both manager and agent are software modules interacting with each other.

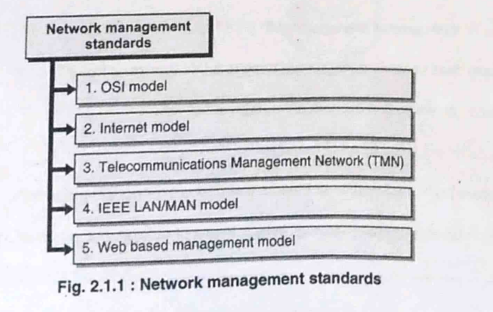


1. **Explain OMAP in network management-5M.**



Network management functions can be broadly summarized as OAMP i.e. Operations Administration Maintenance and Provisioning. These four activities when performed systematically can be called efficient network management.

1. **Operations**: Refers to providing IT services to users of corporate networks. These services are mostly in client/server mode.
2. **Administration:** This activity is responsible for creating overall goals, policies, and procedures for network management. Administration creates formal documents and processes that need to be practiced for efficient network management.
3. **Maintenance:** Maintenance activity is mainly the function of installation and maintenance team. Their responsibility involves repair and installation of facilities and equipment.
4. **Provisioning:** This function refers to network planning and activities which help introduce new services in the network.
5. **Explain network management standards and their features.5M**

****

1. **OSI / CMIP:**

* **International Standard:** Developed by ISO, it serves as a global standard for managing data communications networks, including LANs and WANs.
* **Comprehensive Approach:** Encompasses all seven layers of the OSI model.
* **Object-Oriented:** Utilizes an object-oriented philosophy for device modeling and management.
* **Resource Intensive:** Implementation can be complex, with the CMIP protocol stack consuming significant memory resources.

1. **SNMP / Internet:**

* **Industry Standard:** Established by IETF, initially for Internet management but now widely adopted for WANs and telecommunications.
* **Simplicity and Widely Implemented:** Known for its ease of implementation and widespread acceptance.
* **Manager-Agent Paradigm:** Relies on a manager-agent architecture for communication between network elements.
* **MIB and SMI:** Relies on Management Information Base (MIB) and Structure of Management Information (SMI) for organizing managed objects.

1. **TMN:**

* **Telecom Management Standard:** Developed by ITU-T, focused on managing telecommunications networks.
* **Extends Beyond Network Management:** Addresses service and business management aspects in addition to network management.
* **Based on OSI Framework:** Utilizes OSI CMIP/CMIS specifications as a foundation.

1. **IEEE:**

* **LAN/MAN Management Standard:** Established by IEEE, primarily addressing management of LANs and MANs.
* **Aligned with OSI:** Structured similarly to OSI specifications, particularly focusing on layers 1 (physical) and 2 (data link).
* **Internationally Adopted**: IEEE standards are widely adopted globally for LAN and MAN management.

1. **Web-Based Management:**

* **Utilizes Web Technologies:** Leverages web servers, XML, and HTTP for remote network management.
* **Interoperable Integration:** Based on open standards, enabling integration across heterogeneous environments.
* **Secure and Distributed:** Utilizes HTTP(S) for secure communication and enables distributed applications to behave loosely coupled.

1. **Explain the significance of Trap. Describe the different types of traps5M. Draw the PDU of Trap-2M**

* SNMP is used for managing and monitoring network devices such as routers, switches and servers.
* An SNMP trap is a message that's sent from a network device to an SNMP management system without being solicited by the system.
* The trap is triggered when a specific event or condition occurs on the device, such as a link going down, an authentication or a power failure.
* The SNMP trap message contains information about the event or condition, such as the device and interface where the event occurred, the time the event occurred and the severity of the event.

There are three types of traps— **generic-trap, specific-trap, and time-stamp**, which are application specific.

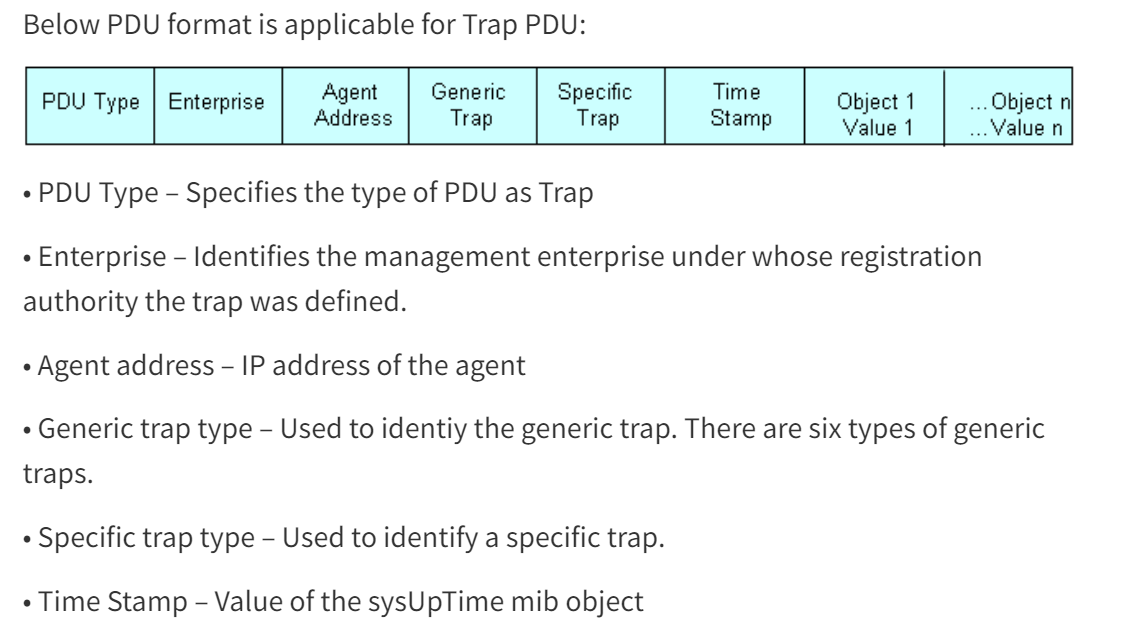
**Generic Trap:**

1. Cold Start: Indicates that the SNMP agent has restarted and is initializing.
2. Warm Start: Indicates that the SNMP agent has restarted without reinitializing.
3. Link Down: Indicates that a network interface has gone offline.
4. Link Up: Indicates that a network interface has come online.
5. Authentication Failure: Indicates a failed attempt to authenticate with the SNMP agent.
6. EGP Neighbor Loss: Indicates the loss of an Exterior Gateway Protocol (EGP) neighbor.

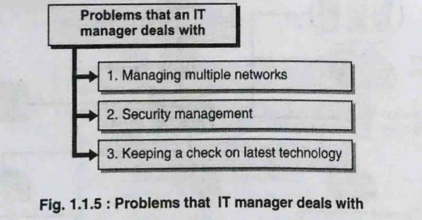
**Specific Traps:** Specific traps, also known as enterprise-specific traps, are custom traps defined by individual vendors or organizations unlike generic traps, which have well-defined codes by SNMP. Organizations can define specific traps to monitor event specific to their network environment.

**Time stamp Trap:** A timestamp trap in SNMP provides exact timing details of network events, aiding administrators in pinpointing issues, correlating events, and analyzing historical data for efficient network management.

**PDU of Trap**



1. PDU Type - Specifies the type of PDU as Trap
2. Enterprise - it contains an object identifier (OID) unique to each enterprise.
3. Agent address: Represents the IP address of the SNMP agent that generated the trap
4. Generic trap type - Used to identiy the generic trap. There are six types of generic traps.
   1. Cold Start
   2. Warm Start
   3. Link Down
   4. Link Up
   5. Authentication Failure
   6. EGP Neighbor Loss
5. Specific trap type - Used to identify a specific trap.
6. Time Stamp - value of system uptime.
7. **Explain the challenges of IT manager.**
8. **Managing multiple network**



* In client/server communication, the network management is no longer a centralized activity.
* Computer and telecommunication networks are slowly merging into a single network and it becomes the responsibility of IT managers to manage multiple networks/services.
* With the explosion of IT services, management of data storage and telecommunication networks now falls under the scope of a network manager.

1. **Security management**

* Along with management of network components, an IT manager must also control and monitor access to information. This involves creating policies as to who accesses the information and whether that access is made by an authentic user.
* Along with information management, the corporate network must be secure against external threats. This is done using components like firewalls and by putting in place proper data access policies.
* Security management in the form of authentication and authorization is another aspect of IT manager's

responsibility.

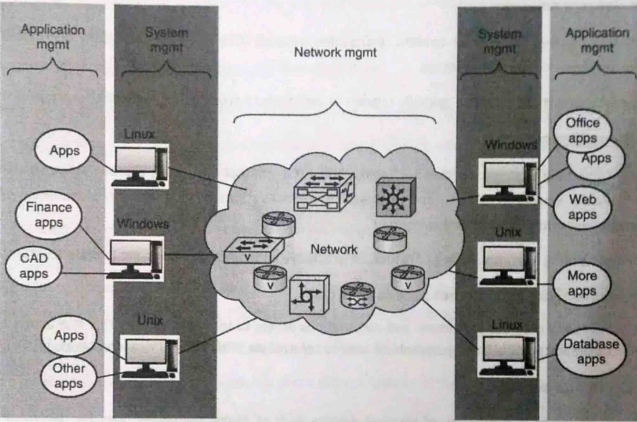
1. **Keeping a check on latest technology**

* Role of an IT manager is also sometimes synonymous with the term CIO (Chief Information Officer). IT managers must keep track of the latest technology and development happening in the field of communications.
* Along with updated information, a manager should also have foresight in predicting future trends while selecting any technology for a corporation. This is needed because that choice will amount into a huge investment for the corporation and the success or failure of the decision may cause a huge monetary setback.

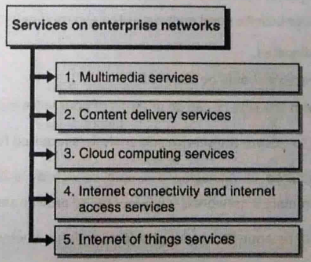
1. **Explain service management in network management.5M**

Management of an enterprise network can be broadly categorized into the following sections:

* Network management
* Systems management
* Application management



1. **Network Management:** Overseeing the operation of the entire network infrastructure, including devices like routers, switches, firewalls, and servers. It includes tasks such as monitoring network performance, configuring devices, managing network traffic, and troubleshooting network issues.
2. **System Management**: System management focuses on the management of individual systems or servers within the network. This includes tasks such as installing and configuring operating systems, managing software applications, monitoring system performance, ensuring system security, and performing backups and recovery procedures.
3. **Application Management:** Application management involves managing the software applications and services running on the network. This includes tasks such as deploying and updating applications, monitoring application performance and availability, ensuring compatibility between different applications, managing licenses, and troubleshooting application-related issues.

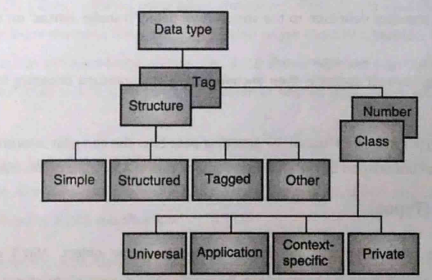
****

1. **Multimedia Service:** Delivering audio, video, and interactive media over the network.
2. **Content Delivery Service:** Distribution of digital content to users.
3. **Cloud Computing Service:** On-demand access to computing resources over the internet.
4. **Internet Connectivity and internet Access:** Providing access to the internet and related devices.
5. **Internet of Things (IoT) Service:**

* Connectivity and communication between internet-enabled devices.
* Internet of things is a network of physical devices such as home appliances, vehicles, electronics, and other equipment with embedded electronics incorporated into them.
* These objects exchange data with each other through various communication technologies and can interoperate within the existing internet infrastructure.

1. **Explain in detail ASN.1-5M**

* ASN.1 is the acronym for Abstract Syntax Notation One, a language for describing structured information; typically, information intended to be conveyed across some interface or communication medium. In network management, information is passed between applications and this information traverses through various layers. There must be a standard way to represent management information efficiently.
* ASN.1 does the task of representing management information in a structured fashion, such that applications can decode it easily.



**ASN.1 Structure (Types)**

Structure represents the type of information that is carried inside an object. It consists of four types of structures:

1. **Simple:** Simple data types are also called atomic or primitive data types. This type is used to represent values and attributes that cannot be further divided into smaller part. As an example, simple data types can involve integers, Bit strings and Octet strings.
2. **Structured:** Structured data types are used to represent complex data that cannot be represented using simple datatypes. These types contain more than one attributes belonging to more than one simple data type.

**Examples of structured data types are:**

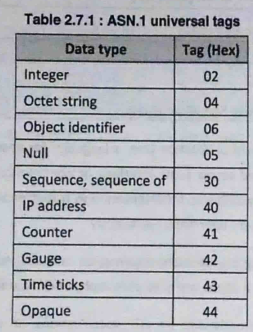
* 1. Sequence: Ordered collection of one or more types.
  2. Set: Unordered collection of one or more types.
  3. Sequence of: Ordered collection of zero or more elements of the same type.
  4. Set of: Unordered collection of zero or more elements of the same type.

1. **Tagged:** Tagged data types are complex data structures that contain other structures. This can be thought of a structure containing another structure.
2. **Other:** This type of data structure is used when there is uncertainty about the type of data. There are two types of values possible are:
   1. Choice: When the supplied data belongs to a set of known data types.
   2. Any: This structure is used when the nature of data to be supplied is unknown.

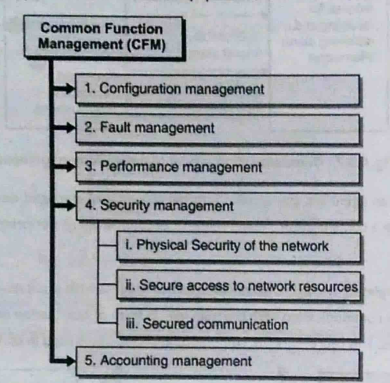
**ASN.1 Tags**

Once the structure of ASN.1 data is defined using types, the nature of this data is identified using ASN.1 'Tags'. ASN.1 There are four types of tags used by ASN.1 module:

1. **Universal:** Defines unique basic data types that can be used in any module, for example, integer, floating points, and strings. These types are also called primitive or atomic types. Table 2.7.1 shows tags used by ASN.1 for encoding universal data types defined by X.208 specification.
2. **Application specific:** These tags have special meaning and encode numbers based on the application being used.
3. **Private**: These tags do not have standard numbers assigned to them, their use and definition is specific to the organization using them.
4. **Context specific:** Context specific tags allow the same data type to be represented with more than one tag number based on the context in which it is used.



**Explain the functional architecture of OSI model in detail.5M**

****

1. **Configuration Management:**

* Involves setting and changing network configurations and component parameters.
* Information stored in a Management Database (MDB).
* Allows provisioning resources and services, as well as monitoring and controlling the state of managed devices.

1. **Fault Management:**

* Includes functions for detecting and isolating network failures.
* Utilizes alarm surveillance to report alarms of varying severity.
* Monitors the network for failures and alerts administrators in case of service or device failures.
* Implements self-healing mechanisms and ticketing systems for fault resolution.

1. **Performance Management:**

* Monitors performance parameters such as traffic statistics and quality of service.
* Applies controls to prevent traffic congestion.
* Tracks traffic statistics and configuration changes for performance analysis.
* Gathers information at all protocol layers for performance monitoring and analysis.

1. **Security Management:**

* Ensures physical security of network components and secure access to network resources.
* Implements mechanisms for authentication, authorization, and encryption.
* Secures communication to prevent tampering of transmitted information.
* Maintains a security database and deploys firewalls to protect against external threats.

1. **Accounting Management:**

* Involves collecting usage information for network resources and generating bills.
* Tracks resource usage based on service parameters.
* Functional accounting of network usage is performed, such as tracking connection time for phone services or packet counts for packet services.

**Explain the Administrative policy of communication model.5M**