**Module - 1**

1. **Define Network Management? Why do we need network management?**

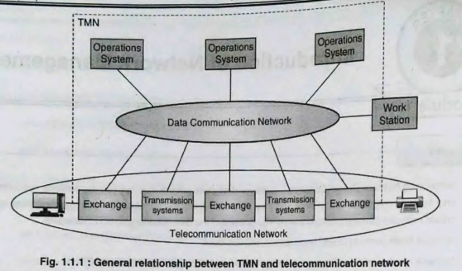
* Network management in telecommunications refers to the set of activities, methods, procedures, and tools required to operate, administer, maintain, and provision networked systems. This field is essential for ensuring that telecommunication networks function efficiently, reliably, and securely. Effective network management is critical for supporting the diverse and complex nature of modern telecommunications, which includes a mix of analog, digital, public, private, switching systems, transmission systems, and telecommunication software.

**Telecommunications Management Network (TMN)**

* The concept of TMN, as defined by ITU-T recommendation M.3010, refers to a network within the telecommunication network that is responsible for the management and upkeep of telecommunication systems. TMN is designed to interface with the telecommunication network at various points to collect and process information about the network's status.

**Functions and Structure of TMN.**

* **Separate Network:** TMN is conceptually a separate network that interfaces with the primary telecommunications network at multiple points to manage the network without interfering with user data transmission.
* **Operations Systems (OS):** These are programs operating at the application layer of the OSI model, performing most management functions. These functions can be automated or handled by human operators. OS facilitates the exchange of management information across the network.
* **Integration of Networks:** With the advent of advanced communication systems and the internet, traditional distinctions between voice and data networks have blurred. Modern data networks now handle real-time voice communications and other services, increasing user satisfaction but also complicating network management.

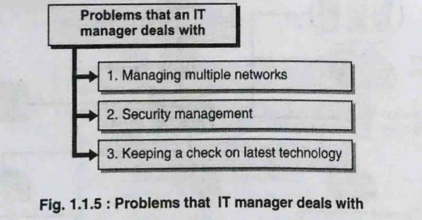
****

**Need of Network Management:**

* **Reliability and Availability:** Effective network management ensures that network services are consistently available and reliable, minimizing the risk of downtime and service interruptions that can impact business operations and user experience.
* **Performance Optimization:** By continuously monitoring and analyzing network performance, administrators can identify and address bottlenecks, optimize traffic flow, and ensure that the network meets performance expectations.
* **Security:** Network management plays a vital role in protecting the network from security threats by implementing robust security measures, monitoring for suspicious activities, and responding to incidents swiftly.
* **Efficiency:** Automation of routine tasks such as configuration updates, monitoring, and reporting reduces manual intervention, increasing operational efficiency and allowing administrators to focus on more strategic tasks.
* **Troubleshooting and Maintenance:** Network management tools and processes enable quick identification and resolution of issues, reducing the time required for troubleshooting and maintenance and improving overall network reliability.
* **Cost Management:** By optimizing resource utilization and tracking network usage, network management helps organizations control operational costs and make informed decisions about infrastructure investments.
* **Scalability:** As networks grow and become more complex, effective network management ensures that the infrastructure can scale efficiently, accommodating increasing numbers of devices and connections without compromising performance or security.

1. **Explain the challenges of IT manager.**

* Managing a corporate network is challenging due to its size and diversity. Corporate networks include various elements like routers, firewalls, load-balancers, access switches, and workstations, necessitating automatic network management tools.
* Network management involves overseeing network components and traffic flow. Breakdowns can lead to service loss and revenue impact. It also includes implementing policies and procedures for network use.



1. **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. **What is OMAP in network management?**

A diagram of a network management

Description automatically generated

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.

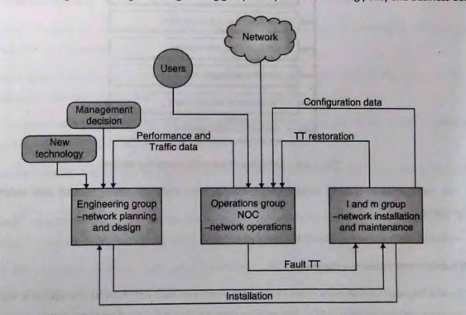
1. **Operations**: Refers to providing IT services to users of corporate networks. These services are mostly in client/server mode.
2. **Administration:** This activity is responsible for creating overall goals, policies, and procedures for network management. Administration creates formal documents 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. **State goals of network management?**

* Goal of network management is to ensure that users of the network receive IT services at an agreed level of QoS and to oversee the interoperability of networking devices.
* To meet this requirement, management should establish policies by creating a Service Level Agreement (SLA) for the users. This SLA will vary depending upon the type of services.
* SLA is more stringent for critical services which may need to run uninterrupted 24 x 7. Network management will not only involve technical aspects but also business aspects where policy decisions have to be taken with an intention of making profit.

1. Network provisioning
2. Network operations
3. Network Installation and Maintenance (I&M)



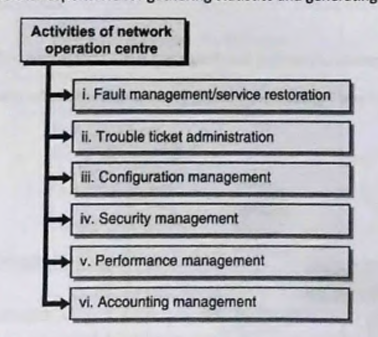
* From a business administration point of view, network management involves strategic and tactical planning of engineering, operations and maintenance of network and network services for current and future needs at a minimum overall cost.
* Network management consists of three major groups that take care of overall network management activities.
* Fig shows a list of activities performed by individual groups. Although these activities are assigned to a specific group, actual tasks pertaining to these activities are carried out by teams as per company's policies and organization's structure for managing operations.
* Network provisioning is primarily related to planning and designing of corporate networks. These activities are taken care of by an engineering group. Monitoring and administration of activities falls under Network Operations Centre (NOC) while the actual tasks of maintenance repair and installation is carried out by I & M team.



* Fig. 1.2.3 shows functional relations between activities of various network management groups. Engineering group is responsible for policy decisions, formulating business strategies along with planning and design of network management. NOC is a core group that performs various task of handling complaints and tickets raised for any service related issues.
* All network management groups rely on other two groups for various information and input. This is represented in Fig. 1.2.3 where the engineering group takes policy decisions based on inputs provided by NOC and I & M. NOC handles incoming service requests from users and delegate maintenance or repair related tasks to I & M.

**Various Functions of Network Management:**

* + - **Network Provisioning:**
* Network provisioning consists of planning and design and is the core responsibility of the engineering group. engineering group is responsible for taking policy and business decisions.
* This involves keeping track of current technology trends and selecting appropriate option for designing corporate networks.
* These decisions are based on thorough analysis of traffic patterns and requirements for a particular corporate network.
* Along with procurement of new equipment, efficient use of available resources is also a task assigned to engineering group. This is achieved through inventory management.
* Another set of responsibilities involve creating policies and procedures for various practices performed by NOC and I&M. Tracing and analysis is done using automated tools. These tools form a part of network management system and help tune network performance automatically.
  + - **Network Operation Centre (NOC):**
* This is the heart of network management functions where most of the core managing activities are performed.
* NOC is concerned with daily activities of network and providing network services.
* Some of the functions of NOC
* NOC is responsible for gathering statistics and generating reports for management.
* This traffic analysis is done using network management tools and systems which help automate different processes.



1. **Fault management / service restoration**

* Service failure or unavailability of any IT service is a common fault with network management. Restoring services for users is a responsibility of NOC. This involves detection and isolation of problems that cause 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 the form of component failure and NMS raises appropriate alarms and sends notifications to the concerned team. 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 on 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 and any SLA that is associated with the disrupted service.
* Once service has been restored and the underlying problem is resolved, the ticket is closed.

1. **Trouble Ticket Administration**

* Trouble ticket administration is the administrative part of network management system which is used to keep track of all problems in a network management system.
* Ticket is a single docket of information about a fault that occurs in the network. It is kept open until it is resolved.
* Generation of trouble tickets are performed automatically or manually and they are stored in a database. These can later be reviewed for analysis and for finding patterns or trends in a particular service fault.

1. **Configuration management**

* Network configuration management is the process of organizing and maintaining information about all components of a computer network.
* When a network needs repair, modification, expansion or upgrade, the administrator refers to the network configuration management database.
* This database contains location and network addresses of all hardware devices as well as information about programs, versions and updates installed in the network components.
* There are three types of configurations, 'static configuration' (permanent configuration), this is the configuration from which the network would start if it is started from an idle status.
* Second configuration is 'current configuration'. This is the configuration on which the network is currently running. It is not necessary that the current running configuration is the same as static configuration.
* Third type of configuration is the 'planned configuration', this refers to the configuration to which the network will be upgraded in future.

1. **Security management**

* Security management can cover a wide range of aspects which includes physically securing network components as well as securing access to information.
* Security database is maintained by NOC for access to the network and network information. Other aspects of security management involve maintaining firewalls and using cryptography for encrypting user information while using public networks.

1. **Performance management**

* For optimum performance, NOC maintains up to date information about the network. Data gathered is used to tune the network for optimum performance.
* The network statistics include data on traffic, network availability and network delay. Traffic data is made available in various formats where it can be evaluated based on its nature example web traffic, voice traffic, email and network management traffic. Traffic statistics are helpful in predicting trends and planning future needs.
* Performance data available on delay and availability can be used for tuning the network to increase reliability and improve response time.

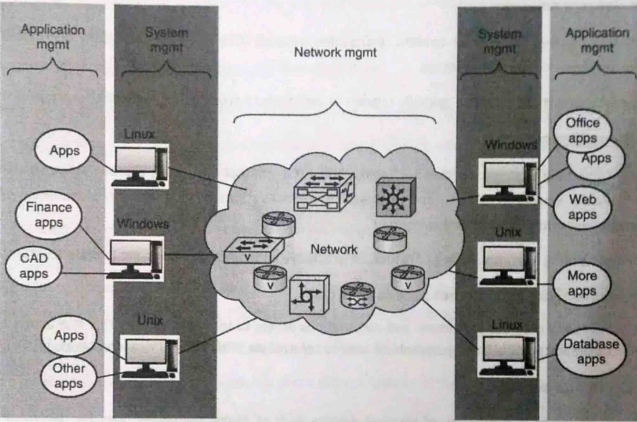
1. **Accounting Management**

* NOC decides the cost and allocates the use of the network.
* Metrics are established to measure the usage of these e-resources and services.
  + - **Installation and Maintenance (I & M):**
* I & M takes care of all maintenance and repair work that is carried out under the process of network management. This group takes orders and directives from NOC to perform any physical maintenance such as installation of components and ping troubles of network operations.
* Tickets generated for any service breakdown or maintenance is handed over to (I & M) for resolution.

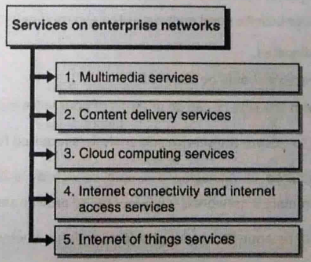
1. **Explain service management in network management**

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 services**

* Multimedia is content that uses a combination of different content forms such as text, audio, images, animations, video, and interactive content.

1. **Content delivery services**

* A content delivery network or content distribution network (CDN) is a geographically distributed network of proxy servers and their data centres.
* The goal is to distribute service spatially relative to end-users to provide high availability and performance.

1. **Cloud computing services**

* Cloud computing is an Information Technology (IT) paradigm that enables ubiquitous access to shared pools ofconfigurable system resources and higher-level services that can be rapidly provisioned with minimalmanagement effort, often over the internet.
* Cloud computing relies on sharing of resources to achieve coherence and economy of scale, similar to a utility.

1. **Internet connectivity and internet access services**

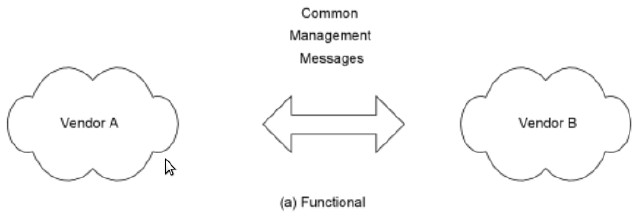
* Internet connectivity provides individuals and corporations access to internet services. This also allows organizations having offices separated over large geographical area to connect via VPN (Virtual Private Networks).

1. **Internet of things services**

* The Internet of Things (IoT) connects physical devices like home appliances, vehicles, and electronics through embedded electronics, allowing them to exchange data and work together via the internet. As IoT evolves, various services are hosted on it.
* For example, managing a Voice over Internet Protocol (VoIP) service involves allocating numbers, updating directories, and troubleshooting issues like poor voice quality or service interruptions. Network management systems handle these tasks to ensure service reliability and performance.

1. **List and describe network management architecture? Dumbbell architecture?**

* Network Management Systems (NMS) are essential for monitoring and managing network components, providing real-time updates and alerts. Corporate networks often include diverse components from different vendors, requiring interoperable NMS solutions. Standards like Internet and OSI facilitate this interoperability. Newer NMS, offer automatic fault diagnosis and correction. ITU Recommendation outlines the 3 key components of network management architecture.
* **Functional components**
* This component defines functions which can be performed by network management architecture. Five functions that are defined; these are fault management, security, accounting, performance management and configuration management.
* **Information component**
* A classical view of network management architecture consists of a network management system whichcommunicates with an agent which in turn will communicate with the managed devices.
* These devices are called managed devices and the NMS creates a view or image of these managed devices basedusing information provided by the agent.
* Information component specifies the type and structure of information that can be collected to create arepresentation of managed devices. This image is called information model.
* **Communication component**
* This component is responsible for providing reliable communication between entities of network management architecture. This level defines various protocols that are used for establishing reliable communication between different network components.



A diagram of a process

Description automatically generated

* Network management **dumbbell architecture** for interoperability is shown in above Fig. Here, components from vendor A and vendor B exchange information with each other.
* This information is generally of two types, 'management information data' which contains device type, status and current running configuration.
* Other type of information conveyed consists of 'management control information' e.g. change in setting or configuration. It shows the functional relation between components from two separate vendors.
* Protocols and services associated with dumbbell architecture are presented in Fig.
* Application related services are the management-related applications such as fault and configuration management. Management protocols are CMIP for the OSI model and SNMP for the Internet model. Transport protocols are the first four OSI layers for the OSI model and TCP/IP over any of the first two layers for the Internet model
* Management protocols used for networks are CMIP (Common Management Information Protocol) and SNMP (Simple Network Management Protocol).

A diagram of a network agent

Description automatically generated

* Above fig shows a hierarchical model for network management, different agents manage a set of components which then provide the status report to a NMS.
* This update can be periodic as well as based on polling mechanism or Query sent by the NMS.
* The same hierarchical architecture can then extended to have interoperability between network management systems from different vendors.

A diagram of a network agent

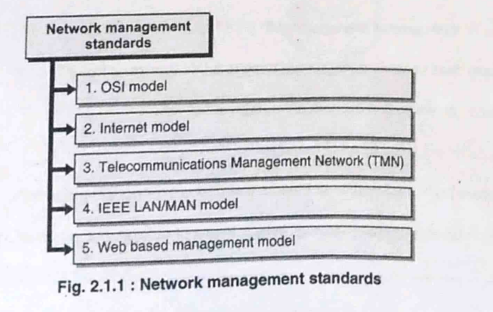
Description automatically generated

**Figure 1.3.3 Network Management Interoperability**

* This architecture is shown in Fig. 1.3.3 where two NMSs connected to two different network exchange control and status information.

**Module 2**

1. **Explain network management standards and their features.(if for 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.

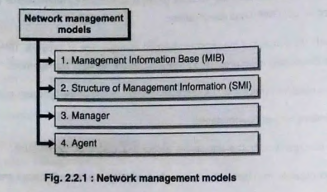
1. **IEEE:**

* **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 network management models? Explain MIB.**

****

1. **Management Information Base (MIB)**

* 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 modelled.

1. **Structure of Management Information (SMI**)

* SMI is responsible for the general rules for naming objects (hardware and system, non-physical such as programs, and administrative information), objects types, and show how to encode objects and values. In case of network management, SMI state the syntax used for naming objects.
* It declares how an object should be named while creating a Model. SMI is a protocol that states these rules.
* However, we must understand that SMI only state the rules; it does not state how many objects are managed in an entity or which object uses which type.
* SMI is a collection of general rules to name objects and to list their types. The association of an object with the type is not done by SMI.

1. **Manager**

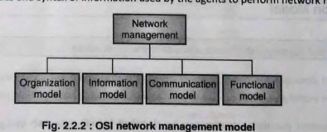
* The manager is the brain of network management and it administers and conducts Operations and Management tasks (O&M) for the managed devices.
* Manager refers to the application that performs the task of network management.

1. **Agent**

* Agent is software that resides in managed devices, and it facilitates communication and management tasks between manager and managed devices.
* Agent is the mediator between the managed device and the manger. The agent keeps performance information in a database. The manager has access to the values in the database.

**OSI Model/ OSI network management model**

OSI model is one the most structured and well-defined model for network management. All the four components mentioned below are present and well defined in OSI model for network management.



1. **Organization model**

* Organization model describes the components of network management system, their functions and their infrastructure. It defines the terms agent, object and manager.
* Different standards have different definitions incorporated under organization model. SNMP, the internet standard has an organization model similar to OSI model.
* In contrast, IEEE standard for LAN and WAN deals only with layer 1 and layer 2 and does not have a well defined structure of organization.

1. **Information model**

* Information model defines the structure and organization of management information. Information model specifies the semantics and syntax of information used by the agents to perform network management.
* This information is stored in the form of Management Information Base (MIB) and Structure of Management Information (SMI). MIB is a conceptual database and does not store actual information about a device; instead it is only a list of attributes about which information is available.
* The actual information about the managed device is available with a different database (i.e. part of configuration management).

1. **Communication model**

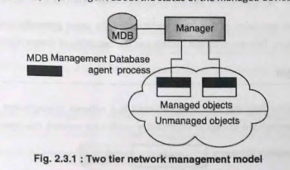
* The third model in OSI is the communication model. This model is responsible for successful communication between managed devices and managing devices.
* Its role is specifying structured protocols for communication requirements. This component has three subcomponents which are:

1. Management application process that performs function in application layer.
2. Layer Management for communication between protocols at different layers.
3. Layer Operation for communications within a protocol layer.
4. **Functional model**

* The functional component defines various activities performed by network management systems. These functions are grouped in different categories.
* Functions are configuration, fault, performance, security and accounting. These are defined as system management functions in OSI.
* The reason for such a grouping was to facilitate rapid and consistent progress within each category in individual groups, and not to segregate NMSs for each area.
* Functions from one area will be influenced by others, and a system may be implemented with n functions from different areas to meet the business objectives and market needs.

1. **Describe two-tier and three-tier network management organization model.**

**Two-tier Model:**

****

* Organization model describes the components of network management and their relationships. Fig. 2.3.1 shows a two-tier model. This model gives a conceptual understanding of network management process.
* In network management paradigm, devices can be classified broadly into two categories, managed devices and managing devices.
* Managed devices are generally network components that are used to carry telecommunication and voice data namely hub, switches, routers and data servers. If devices have the capability to communicate with managing devices (manager) they are called managed devices, else, they are simple unmanaged devices with no communication capability with the management network.
* The managed devices have a process (application) running on them which facilitates communication with management network, this process is called an agent process (agent can also be a separate device with the sole responsibility of monitoring managed devices).
* This agent works as a mediator between management network and managed device. Fig. 2.3.1 shows that the manager (managing device) can query the agent about the status of the managed device.
* Also, the agent can send some alarm to the manager in case of some failure or fault with the managed device. The manager receives management data (status/ data other than communication data) from the agent and takes necessary action. This data is stored in Management Database (MDB).

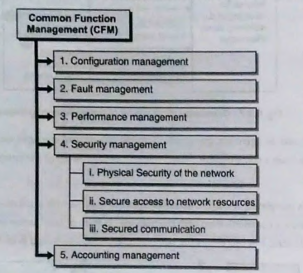
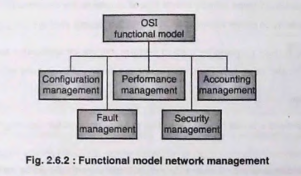
**Three-tier Model:**

**A diagram of a cloud

Description automatically generated**

* Fig. 2.3.2 shows a three tier management model where a large number of devices needs to be managed by a single manager. This three tier model is an extension of two tier network management model.
* Here an intermediate device acts as a manager/agent and store status and data related to various managed devices within its scope of monitoring. This data is then sent to a manager which resides in an intermediate device. This manager can use the data for statistical analysis.
* The above two models represent the interaction of network managers with local devices and with other managers. In case the managed network is spread over a geographically wide area for example a corporation with local offices spread over different cities, there is a need for a distributed network management process.
* This process involves communication between various Managers as well as communication between agents running different types of network management systems.

1. **Explain the functional architecture of OSI model in detail.**

****

1. **Configuration management**

* It includes functions that allow a management system to provision resources and services, monitor, and control the state of various managed devices within the network.
* It addresses the functions related to changing the configuration of various network components.
* Information related settings and configurations of managed devices are stored in Management Database (MDB).
* This information can be retrieved by managers and can be used to change the configuration of managed devices.
* Configuration management is responsible for setting various parameters in network components.
* In case of a failure, component management performs the task of informing the team responsible for provisioning that service failure has occurred. Such failure are recorded and maintained in a database which can later be reviewed for analysis.

1. **Fault management**

* Fault management includes functions that address alarm surveillance, testing and fault isolation. (Alarm surveillance, as the name implies, allows reporting alarms with different levels of severity along with the possible causes of alarms.) It also provides a summary of the alarms that are outstanding and permits the manager to retrieve the alarm information.
* NMS implements fault management by constantly monitoring the network for any service or device failures. In case of failure, an alert is displayed in the application.
* Service must be restored as soon as possible. This may involve changing some configuration. In several failure situations, the network could automatically detect the problem and perform troubleshooting procedures for restoration of service.
* Such networks are called self-healing networks. In case the self-healing feature cannot resolve the issue, there will be a ticketing system in place that will issue a trouble ticket, which is carefully reviewed and followed up until service is not restored.
* NMS has the capability of tracking any pending trouble tickets and raises periodic alarms in case some issues are left unresolved. A record of all such tickets are maintained in the database which can be used later for analysis of patterns in which fault occur.

1. **Performance management**

* It includes functions to monitor performance parameters such as number of bad messages, collecting traffic statistics, and applying control to prevent traffic congestion. It ensures quality of service.
* Threshold values may be assigned for the parameters, and when the threshold is exceeded, events may be generated to inform the management system.
* Up-to-date information of traffic statistics should be maintained by NOC for performance analysis. Along with traffic statistics, any updates in the configuration changes must be updated with a database in NOC.
* The data gathering feature may also be used to perform analysis on application specific traffic like email traffic, web browsing traffic and voice calls. Performance data on delay and availability will help improve response time.

1. **Security management**

* Security management defines a broad range of activities to be performed for securing the network. This involves the following aspects:

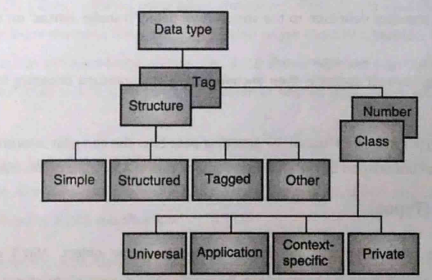
1. **Physical security:** Protecting network component from physical damage.
2. **Secure access:** Providing access to information and network resources only to authenticated users. Also making sure the privilege levels for accessing information are well defined.
3. **Secured communication:**
   * This feature of communication deals with securing the transmitted information. Management information along with telecommunication data should be securely transmitted over the network.
   * Secured communication prevents tampering of information.
   * Security database is maintained by NOC for access to the network and network resources. Any unauthorized access will raise an alarm through NMS.
   * Another mechanism implemented by security management is deploying firewalls to network from external threats. Any intrusion or attempt to override security procedures are recorded by NMS systems.
4. **Accounting management**

* It includes collecting usage information for the resources used in providing a service and then generating a bill.
* It is to be expected that while collecting, the usage information and reporting on the values is subject to standardization, the billing process is are considered outside the scope of standardization.

1. **Explain in detail ASN.1? Formal and semi Formal Notations?**

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.



* Before ASN.1, specific bits and bytes in protocol messages had fixed meanings, complicating data interpretation. ASN.1 allows complex information to be structured using simpler data types, such as representing a student object with attributes like name, age, and registration number.

A white paper with black text

Description automatically generated

* ASN.1 uses two main concepts: abstract syntax and transfer syntax. Abstract syntax defines data structures using object-oriented principles, while transfer syntax deals with encoding these structures for transmission. The data generated using abstract syntax is then encoded using any standard encoding format defined by transfer syntax.
* The Basic Encoding Rule (BER) is a common encoding format for ASN.1 data, ensuring that encoded information is machine-readable.

**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:**

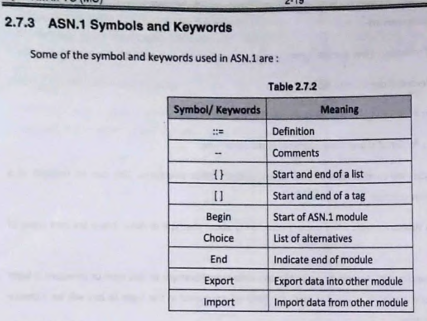
* 1. Sequence: Ordered collection of one or more types.
  2. Set: Unordered collection of one or more types.
  3. Sequence of: Ordered collection of zero or more elements of the same type.
  4. Set of: Unordered collection of zero or more elements of the same type.

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. Ex. Login to a website using phone number and emal id.
   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.



1. **What encoding mechanisms are used for ASN.1?**

ASN.1 transfer syntax makes use of Basic Encoding Rules (B.E.R.) technique to transfer ASN.1 data. International standard defines a set of Distinguished Encoding Rules (DER) and a set of Canonical Encoding Rules (CER) both make use of Basic Encoding Rules (BER) with some constraints. These encoding rules are applied to data types defined by ASN.1 notation.

**Basic Encoding Rules (BER)**

* Basic encoding rules is the preferred encoding rule used by ASN.1; other rules may be used depending upon the type of data to be transferred.
* Basic encoding rules give the sender of an encoding various choices as to how data values may be encoded.
* The canonical and distinguished encoding rules select just one encoding from those allowed by the basic encoding rules, eliminating all of the sender's options.
* Encoding of data consists of four components which are:

A diagram of components of coding

Description automatically generated

* Octets (Bytes) are used to represent different contents of data enable error free encoding/decoding.

1. **Identifier octets**

* Identifier octets are used to identify the type of data being encoded. These types are the ones specified by ASN.1 notation. Identification is done using 'Tag Number' specified by ASN.1 universal tags.
* Identifier octet is made up of 1 byte. Each bit in this octet is used to provide different information about data and its class.
* It consists of three sections :
  + Bits 8-7 are encoded to represent class of tag show in Table 2.8.1.
  + Bit 6 (P/C) can be a 0 or 1. Where a 0 indicates primitive data types and 1 indicates constructed data type.
  + Bits 5-1 encode tag number of data in binary. (Bit 5 is MSB)



1. **Length octet**

* Length octet can be 1 or more bytes depending on length of data. It is used to indicate length of encoded data.
* This one byte of length octet has to take into consideration that data length can be any value. This is achieved by assigning specific meaning to MSB (bit 8) of length field.
* If length of data can be expressed using 7 bits (between 1 to 127 bytes) MSB is assigned a value 0.
* Remaining 7 bits are used to indicate the length of the data field. In case the length of data exceeds 127 it cannot be expressed using 7 bits; in such a case MSB is assigned a value 1.
* Remaining 7 bits of length field is used to indicate the 'number of bytes' needed to express the length of the data field. These octets will follow the length field and will be used to identify length of data field.

1. **Content octet**

* Content octet can have a length of 0 bytes of more depending on the amount of data being carried.
* It contains binary equivalent of data and is followed by end of content octets (optional).

1. **Describe all CMISE services in following categories:**

**(i) Management association services**

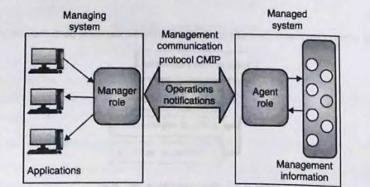
**(ii) Management notification services**

OSI network management scheme bundles the network management protocols into a single set called Common Management Information Service Element (CMISE).

It is used to exchange management information between the manager and agent. Basic operation of OSI network management systems is represented by Fig. 2.10.1. CMISE is specified into two parts:

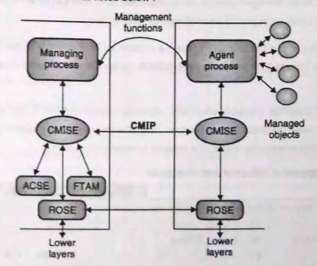
**1. CMIS:** Common Management Information Service

**2. CMIP:** Common Management Information Protocol

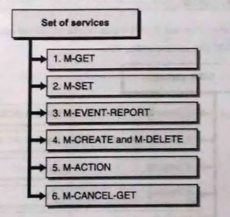


**Common Management Information Service**

* Common Management Information Service (CMIS) provides a way to manage network based on OSI network management principle.
* CMIS acts as a user interface and provides a set of functions or methods that can be used to perform operations on managed objects (network devices) or receive notifications from them.



**Figure 4 : OSI system Architecture CMIS/CMIP**



* **M-GET:** This can be used to retrieve attributes of network and system resources, for example number of bytes (octets) processed by the switch/router, port status, system name etc.
* **M-SET:** M-SET service can be used to modify the attributes of an object.
* **M-EVENT-REPORT:** This function can be used to report an occurrence of any significant activity for example excessive transmissions happening through a port, or a device going offline.
* **M-CREATE and M-DELETE:** This service allows the manager to request for creating or deleting a particular instance of an object (A single managed element can be represented by multiple objects). M-CREATE/ M-DELETE allow
* creation/deletion of such objects as per the need of management system.
* **M-ACTION:** This service allows the manager to issue a request for performing any operation on the object (These operations are different from M-SET). For example M-ACTION can be used for activating a protocol at any layer of the OSI model.
* **M-CANCEL-GET:** This service is used to abort any previously requested M-GET. This is used to prevent multiple transmissions of the same request. These services help the manager to perform activities defined by the communication model and information model of a network management system.

1. **With respect ISO/OSI network management describe following terms :**
2. **ACSE**
3. **ROSE**
4. **Scoping and Filtering**
5. **Linked Replies**
6. **CMIS/CMIP**
7. **GDMO**

**What is Management Information Tree (MIT) ?**

**What is CMIP ?**

**What is scoping and Filtering in CMIP/CMIS network management standard?**

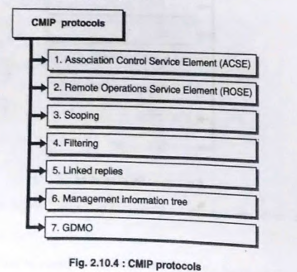
**Discuss conceptual views of managed objects with reference to the OSI perspective.**

**Describe the services offered by CMISE.**

* **Common Management Information Protocol (CMIP)** is a connection-oriented application layer protocol. It converts the service messages created by CMIS into corresponding PDU.
* These PDU are then transported over the network as a packet. For transmission, CMIP makes use of connection-oriented mechanism (TCP).
* This connection-oriented service makes CMIP more reliable and there is lesser number of retransmissions and packet loss.

A close-up of a sign

Description automatically generated



1. **Association Control Service Element (ACSE)**

* Association Control Service Element (ACSE) is the OSI method for establishing a call between two application programs (Manager and Agent).
* ACSE checks the identities and contexts of the applications and can apply an authentication security check.

1. **Remote Operations Service Element (ROSE)**

* It is an OSI service interface that allows remote operations capability, interactions between different entities in a distributed environment (Manager Agent Interaction in a multi-tier model) allows the remote entity (Agent) to perform the requested operation and sends the report back to the requesting entity (Manager).

1. **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. This is shown in Fig.

A diagram of a network management

Description automatically generated

1. **Base object only:** In this case operations are performed only on the base node of management information tree
2. **Nth level subordinate object:** In this type of scoping, operations are performed on Nth sublevel with respect to the base node.
3. **Base object plus all its subordinates:** In this scoping mechanism rules are applied to the entire subtree associated with a base object.
4. **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.

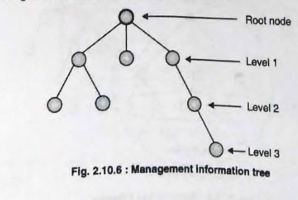
1. **Linked replies**

* When scoping and filtering are applied, a single filter rule may result in more than one object getting selected. The management system will return all the managed objects to the requesting entity.
* In the case of CMIP it is not possible to reply back with multiple objects. The reason for this is that the structure of the CMIP response PDU only has a single field for containing object instance information.
* Since each managed object will have its own instance information each object will be returned in a separate CMIP PDU. In cases where more than one objects have to be returned; CMIP makes use of Linked Reply PDU.
* This PDU provides a means of associating multiple replies to a single PDU request that requested the managed objects. Thus a single PDU request along with scoping and filtering will result in multiple linked replies.

1. **Management information tree**

* Every object known in the management system is represented in the management information Tree. These objects include physical networking elements like switches, hubs and routers.
* It is also used to model virtual objects like attributes and events associated with networking elements. It enables virtual representation of Managed Objects (MO) allowing network management protocols to use managed objects for changing the status of networking elements.
* CMIP makes use of MIT for accessing and modifying state of managed objects.
* A single global scheme is used to provide naming scheme for all data within the MIT. Each object in MIT is represented as nodes. There is a well-defined root node followed by a series of nodes that spread out in an inverted fashion. Fig. 2.10.6 shows the structure of a generic MIT.

A diagram of a network

Description automatically generated

1. **GDMO**

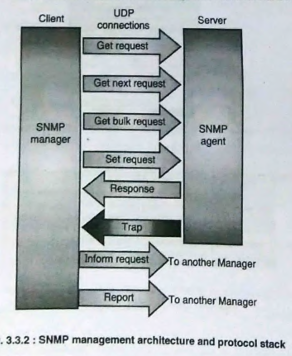
* GDMO stands for Guidelines for Definition of Managed Objects. GDMO is part of the Open Systems Interconnection (OSI), Common Management Information Protocol (CMIP).
* It is also the guideline used for defining objects under Telecommunication Management Network (TMN). GDMO is specified in ISO/IEC standard 10165/x.722. It makes use of ASN.1 as rules for syntax while creating objects.

| **Feature** | **MDB** | **MIBs** |
| --- | --- | --- |
| 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 |

| **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 |

**Module 3**

1. **Draw SNMP v1 architecture and discuss the messages involved.**



**SNMP Manager**

* An SNMP manager is a computer that is configured to poll SNMP agents for information.
* The manager can be any machine that can send query requests to SNMP agents with the correct credentials.
* Sometimes, this is implemented as part of a monitoring suite, while other times this is an administrator that uses some simple utilities (commands) to craft a quick request.

**Functions performed by a manager are:**

1. **Queries agents:** A manager collects information about managed devices by sending messages to agents under its management. These agents in turn collect this information from managed devices.
2. Gets responses from agents.
3. **Sets variables in agents:** Managers can remotely configure managed devices by issuing configuration commands.
4. Acknowledges asynchronous events from agents.

Apart from these functions a manager (SNMP manager) also interacts with another manager agent to give the NOC holistic view of the managed network.

**SNMP Agents**

* SNMP agents are responsible for gathering information about the local system and storing them in a format that can be queried. SNMP agents update a database called the "Management Information Base" or MIB.
* The agent computer configures which managers should have access to its information. It can also act as an intermediary to report information on devices it can connect to that are not configured for SNMP traffic.
* This provides a lot of flexibility in getting network components online and makes them accessible via SNMP. Some important functions performed by SNMP agents are:

1. Collection of management information about its local environment
2. Storage and retrieval of management information as defined in the MIB.
3. Signals an event to the manager.
4. Acts as a proxy for some non SNMP manageable network node.

**discuss the messages involved (answer below)**

1. **List and Describe various commands/messages with command syntax(10M)? List and describe SNMP commands with syntax? What are SNMP V1 commands(5M)? discuss the messages involved?**

* Most important aspect of SNMP is its simplicity is shown in the fact that there are only 5 protocol messages exchanged between manager and agent.
* Out of these 5 protocol messages, 3 are initiated by the manager and the remaining two are initiated by the agents.
* These protocol messages are:

1. **Get-request**

* A get message is sent by a manager to an agent to request the value of a specific OID (Object Identifier).
* This request is answered with a response message that is sent back to the manager with the data.
* The data sent back is a scalar value. This protocol message will help the manager to query any managed device and obtain values for certain device specific parameters.

1. **Get-next-request**

* A get-next-request message allows a manager to request the next sequential object in the MIB. This is a way to traverse the structure of the MIB without worrying about what OIDs to query.
* This request is used in case multiple values are present for a particular object.

1. **Set-request**

* A set message is sent by a manager to an agent to change the value held by a variable on the agent.
* This can be used to control configuration information or otherwise modify the state of remote hosts.
* This is the only write operation defined by the protocol. Using set-request, the settable configuration parameter can be changed.

1. **Get-response (Response)**

* This message, sent by an agent, is used to send any requested information back to the manager.
* It serves as both a transport for the data requested, as well as an acknowledgement of receipt of the request.
* If the requested data cannot be returned, the response contains error fields that can be set providing more information. A response message must be returned for any of the above requests, as well as Inform messages.

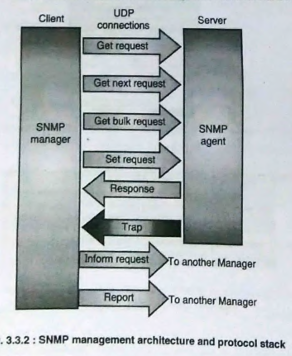
1. **Trap**

* A trap message is generally sent by an agent to a manager. Traps are asynchronous notifications in a way that they are unsolicited by the manager receiving them.
* They are mainly used by agents to inform managers of events that are happening on their managed devices.
* An example of trap is when an interface on a router or switch fails the agent monitoring the device must send an alarm to the manager, these messages are in form of a trap.

1. **GetBulkRequest**

**In later version of SNMP ie SNMP V2**

* The GetBulkRequest PDU is sent from the manager to the agent to retrieve a large amount of data. It can be used instead of multiple GetRequest and GetNextRequest PDUs.
* So when the manager is aware that it has to retrieve an entire table from the agent instead of sending sequential GetRequest, the manager simply makes use of GetBulkRequest.



1. **Why it is not possible to access entire table at one time in SNMP V1?**

**Get-next-request**

* A get-next-request message allows a manager to request the next sequential object in the MIB. This is a way to traverse the structure of the MIB without worrying about what OIDs to query.
* This request is used in case multiple values are present for a particular object. An example of this is routing tables of routers which will have multiple values.

**GetBulkRequest**

* The GetBulkRequest PDU is sent from the manager to the agent to retrieve a large amount of data. It can be used instead of multiple GetRequest and GetNextRequest PDUs.
* So when the manager is aware that it has to retrieve an entire table from the agent instead of sending sequential GetRequest, the manager simply makes use of GetBulkRequest.
* SNMPv1 does not have a command to retrieve an entire table in one request. The commands available (Get-request and Get-next-request) retrieve one or the next object, respectively. To retrieve a whole table, multiple Get-next-request commands must be issued sequentially, which can be inefficient. This limitation is addressed in SNMPv2 with the introduction of the GetBulkRequest, allowing for bulk retrieval of data.

1. **Describe different types of traps? SNMP Trap? Significance/purpose of trap?**

* 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.

1. **Generic Trap:**

* **Cold Start Trap:**Generated when a network device has just been powered on or restarted. The SNMP manager can use this trap to detect when a device has rebooted. It can then take necessary actions such as checking the device’s configuration and status.
* **Warm Start Trap:**Generated when a network device has been restarted without losing its configuration. The SNMP manager can use this trap to detect when a device has rebooted. After that, it can take action to check the device’s configuration and status.
* **Link Down Trap:**Generated when a network interface on the device has gone down. The SNMP manager can use this trap to detect when a network link has failed and notify the appropriate personnel to investigate and resolve the issue.
* **Link Up Trap:** Generated when a network interface on the device has come up. The SNMP manager can use this trap to detect when a network link has been restored and take actions such as reconfiguring the routing tables.
* **Authentication Failure Trap:** Generated when a user authentication attempt has failed. The SNMP manager can use this trap to detect when an unauthorized user attempts to access the network. After detection, it can take actions like blocking the user’s IP address.
* **EGP Neighbor Loss Trap:** Generated when a router loses an Exterior Gateway Protocol (EGP) routing protocol neighbor. It signals that a neighbor router is no longer available, indicating possible changes to the[**routing table**](https://en.wikipedia.org/wiki/Routing_table). The SNMP manager can use this trap to recognize changes in the network and take action, such as updating routing tables.
* **Enterprise-Specific Traps:** Enterprise-specific traps are customizable traps defined by the network administrator or the SNMP manager. These traps are used to indicate specific events or conditions in the network.

1. **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.
2. **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.
3. **Draw and describe with neat diagram SNMP V1 PDU format(5M)? Draw and describe SNMP v1 message and SNMP v1 PDU formats.**

The SNMPv1 Protocol Data Unit (PDU) format defines the structure of the messages exchanged between SNMP managers and agents. Each PDU consists of several fields that are used to identify the type of request and carry the necessary information.

****

SNMPv1 PDU Structure

1. **PDU Type:** Identifies the type of SNMP message (e.g., GetRequest, GetNextRequest, GetResponse, SetRequest, Trap).



1. **Request ID:** A unique identifier to match requests and responses.
2. **Error Status:** Indicates the error status of the response (e.g., noError, tooBig, noSuchName, badValue, readOnly, genErr).

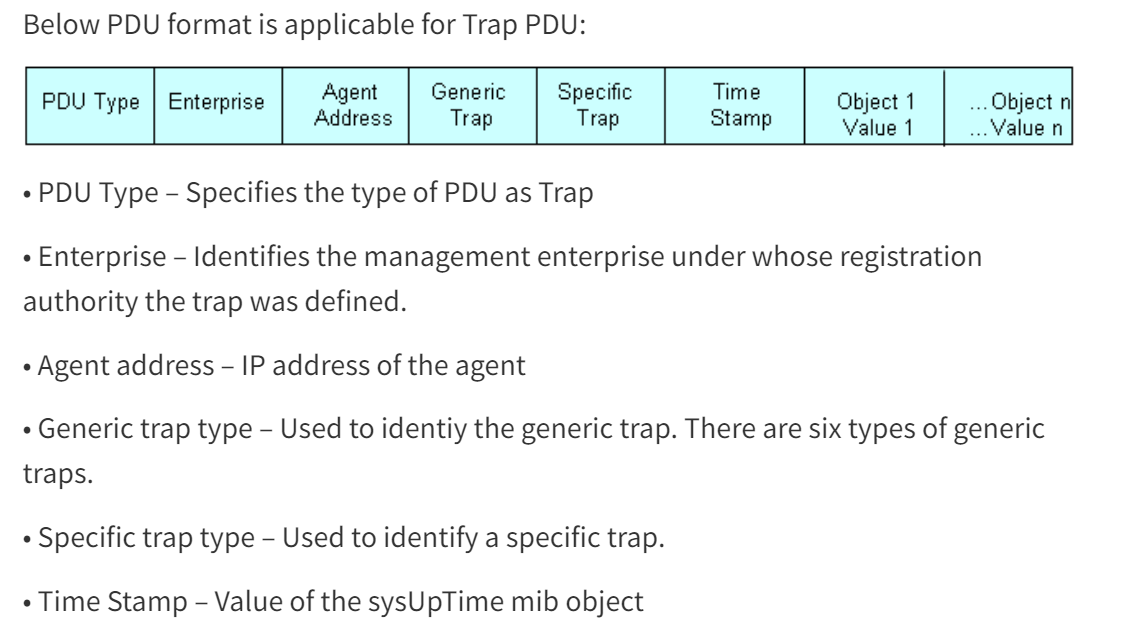


1. **Error Index:** gives additional information about the eroor, Indicates the position in the variable bindings (VarBind) list where an error occurred.
2. **Variable Bindings** (VarBind)

A list of variables (name and value pairs) for which the request or response is made. Each variable binding includes:

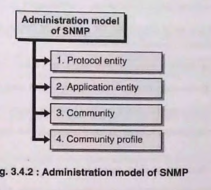
* Object Identifier (OID): Specifies the variable being referenced.
* Value: The value of the variable. This can be a requested value (in a response PDU) or the value to be set (in a SetRequest PDU).

**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 Administrative policy of communication model.**

The administrative policy of the SNMP communication model ensures secure and structured management of network devices by controlling which data is visible to which devices, based on defined rules and permissions. This model plays a crucial role in maintaining security and efficiency in network management. Here's an explanation based on the provided text:

****

1. **Protocol entity**

* A protocol entity is a device in the SNMP architecture that has SNMP application installed on it and it takes part in the communication process.

1. **Application entity**

* An application entity is the process or program installed on a device which makes it possible for the device to communicate using SNMP protocol.

1. **Community**

* The pair of two entities is called SNMP community. The name given to such a pair is called Community.
* A community can contain multiple pairs, Fig. 3.4.3 shows a community with three managers communicating with a single agent.

1. **Community Profile:**

* Consists of a community name, MIB view, and access privileges. This profile dictates what information is accessible and the permissions granted (read or write) to different entities within the community.

**MIB (Management Information Base) View:** Defines the subset of network elements (objects) that a manager can access. It specifies the read and write permissions for a particular device, ensuring that managers only access necessary information for management tasks. This permissions of read and write is called as access mode.

**Access Mode:** Determines the level of access a manager has to a device. The main access modes are:

* **Read-only:** Allows agents to monitor and retrieve data from a device. Operations include GET, RESPONSE, and TRAP.
* **Write:** Permits managers to send SET requests to change device configurations.

****

The next term used in SNMP administration model is SNMP Access Policy. SNMP MIB view when combined with access mode will result in SNMP access policy. All the terms put together (Protocol entity, application entity, community, MIB view access mode and access policy) define the administration model of SNMP.

The below fig shows SNMP access policy with a single community and 2 community profile.

****

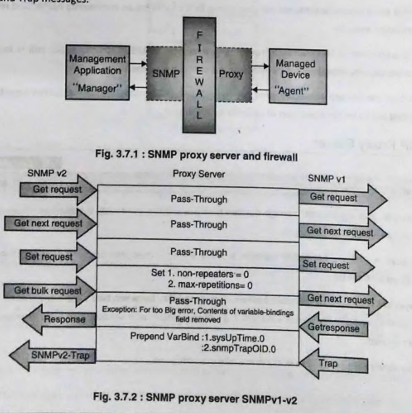
****

Fig SNMP administration model

Manager 1 manages community 1, manager 2, community 2,and manager 3 (MoM) both communities 1 and 2

1. **What is an SNMP proxy server**

* SNMP managers and agents can manage devices that have SNMP processes installed on them or if they have the capability of handling SNMP messages.
* In case of devices that are not SNMP capable, a proxy server is used that converts Non-SNMP entities into SNMP-entities defined by the MIB.
* Proxy servers are also used to maintain backward compatibility between two different versions of SNMP. As is the case with SNMPv1 and SNMPv2, where version 2 is not compatible with version 1, to make communication possible a proxy server is used.
* Finally proxy servers are used in networks that make use of firewalls.
* The goal of SNMP proxy is to enable a management application to be able to perform SNMP operations (Example SNMP GetRequest, SNMP SetRequest), on SNMP agents residing on managed DMZ devices (example routers, switches, servers, load balancers).
* SNMP proxy is required whenever the flow of SNMP traffic is restricted or prevented, due to a firewall installed between the management application and the managed devices.
* Fig. 3.7.1 shows the use of proxy servers in case SNMP messages have to bypass a firewall. The application-level proxy transports SNMP protocol data units (PDU) between the NMS and managed devices, allowing requests and responses between the NMS and managed devices and also forwarding autonomous messages to the NMS.
* The proxy agent requires little provisioning at the NOC and no additional provisioning at the managed devices.
* The second function performed by SNMP proxy server is where it makes it possible for SNMPv2 to be backward compatible with SNMPv1. Fig. 3.7.2 shows how SNMP proxy server allows communication between SNMPv1 and SNMPv2.
* Requests and responses from version 1 and 2 pass through the firewall, with some modifications. These modifications are introduced in the message PDUs by proxy server to maintain backward compatibility. For instance, GetRequest and GetNextRequest pass through the proxy server without modifications whereas; GetBulkRequest is modified by the proxy server by changing the PDU to make it similar to GetNextRequest. Similar modifications are made to getResponse and Trap messages.



1. **SNMP V2**

* SNMPv2, or Simple Network Management Protocol version 2, is an updated version of SNMPv1. It was developed to address some of the limitations and deficiencies found in SNMPv1, enhancing the protocol's functionality and performance. SNMPv2 retains the basic architecture of SNMPv1 but introduces several improvements and additional features.
* The main weakness of SNMPv2 was supposed to address are:

A close up of a document

Description automatically generated

1. **Expressiveness of MIB Definitions:**

* SNMPv1 lacked the ability to describe complex devices and protocols adequately. The MIBs needed greater expressiveness to handle the increasing complexity.

1. **Performance:**

* SNMPv1 generated excessive traffic overhead, especially when deployed over WANs. The simple scalar architecture with a single agent and manager was not efficient for large-scale deployments.

1. **Security:**

* SNMPv1 had poorly defined security mechanisms. The use of "Communities" for security was vague and varied between implementations, leading to interoperability issues.

**Improvements:**

* The basic components of SNMPv1 and v2 are the same, the functions performed by the manager and agent are still the same.
* The organization model remains the same. SNMPv2 adds more messages to improve the communication between management entities.
* It allows two managers to communicate with each other using informed messages.

A close up of a document

Description automatically generated

1. **Bulk messages**

* Get bulk message allows managers and agents to transfer large amounts of data.
* Initially in SNMPv1 this was accomplished by a series of get-request and get next requests.

1. **Manager to manager messages**

* The second improvement is adding the ability of interoperability.
* Version 2 allows the manager to manager communication using inform messages.

1. **MIB enhancements**

* SNMP v2 added new objects to incorporate security and SNMPv2 objects.
* There are also significant changes in the SNMP groups of version 1.
* The improvement in MIB2 for SNMPv2 is shown in Fig. 3.9.2.

A diagram of a computer

Description automatically generated

1. **Transport mapping**

* SNMP has always relied on UDP for communicating messages between managers and agents. In SNMPv2, other transport layer protocols are incorporated.

1. **SNMP V2 Architecture, messages**

**SNMP v2 architecture:**

* The architecture of SNMPv2 is essentially the same as SNMPv1 with some minor changes to allow manager-to-manager communication and additional message types.

**A diagram of a software application

Description automatically generated**

**Messages:**

1. **GetRequest:**

* Similar to SNMPv1, this message is used by a manager to request the value of a specific OID from an agent.

1. **GetNextRequest:**

* This message allows a manager to retrieve the next sequential object in the MIB.

1. **GetBulkRequest:**

* A new message type introduced in SNMPv2, allowing the retrieval of large amounts of data efficiently. It is used instead of multiple GetRequest and GetNextRequest messages.

1. **SetRequest:**

* Similar to SNMPv1, this message is used by a manager to set the value of a specific variable on an agent.

1. **Response:**

* This message is sent by an agent or a manager in response to a GetRequest, GetNextRequest, GetBulkRequest, SetRequest, or InformRequest message.

1. **Trap (SNMPv2-Trap):**

* Similar to the Trap message in SNMPv1, it is used to notify the manager about significant events.

1. **InformRequest:**

* A new message type introduced in SNMPv2, allowing a manager to send information to another manager and receive an acknowledgment in return. This facilitates manager-to-manager communication.

1. **Compatibility with SNMPv1? Explain the role of bilingual manager?**

* SNMPv2 is not backward compatible with SNMPv1. In an organization, there are sections of network that employ SNMPv1 while others may employ SNMPv2; to provide interoperability between two such networks some form of translation mechanism is needed.
* This translator entity (device) converts messages from SNMPv1 to SNMPv2 and vice versa.
* There are two mechanisms used to implement interoperability, one is proxy server. Another mechanism to provide interoperability is the use of a bilingual manager.

**Bilingual manager**



* 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 server.

**Proxy server**

* Another mechanism that allows SNMPv2 to become backward compatible with SNMPv1 is the use of Proxy servers.
* (**This is shown in previous snmp proxy server question**), where SNMPv2 messages are converted to SNMPv1 and vice-versa using an intermediate proxy server.

1. **SNMPv2 PDU?**

****

SNMPv1 PDU Structure

1. **PDU Type:** Identifies the type of SNMP message (e.g., GetRequest, GetNextRequest, GetResponse, SetRequest, Trap).

* GetRequest (0)
* GetNextRequest (1)
* GetResponse (2)
* SetRequest (3)
* Trap (4)
* GetBulkRequest(5)
* InformRequest(6)

1. **Request ID:** A unique identifier to match requests and responses.
2. **Error Status:** Indicates the error status of the response (e.g., noError, tooBig, noSuchName, badValue, readOnly, genErr).



1. **Error Index:** gives additional information about the eroor, Indicates the position in the variable bindings (VarBind) list where an error occurred.
2. **Variable Bindings** (VarBind)

A list of variables (name and value pairs) for which the request or response is made. Each variable binding includes:

* Object Identifier (OID): Specifies the variable being referenced.
* Value: The value of the variable. This can be a requested value (in a response PDU) or the value to be set (in a SetRequest PDU).

1. **What is user security model of SNMP V3?**

USM describes the security model for SNMPv3. It defines elements of procedures required to provide SNMP message level security. USM describes two primary and two secondary threats against which USM provides protection. These threats are:

**1. Modification of information**

The modification threat is the danger that some unauthorized entity may alter in-transit SNMP messages generated on behalf of an authorized user.

**2. Masquerade**

The masquerade threat is the danger that management operations not authorized for some user may be attempted by assuming the identity of another user that has the appropriate authorizations.

**3. Disclosure**

The disclosure threat is the danger of eavesdropping on the exchanges between managed agents and a management station.

**4. Message stream modification**

The message stream modification threat is the danger that messages may be maliciously re-ordered, delayed or replayed in order to effect unauthorized management operations.



* USM invokes privacy module w/ encryption key and scopedPDU
* Privacy module returns privacy parameters and encrypted scopedPDU
* USM then invokes the authentication module w/authentication key and whole message and receives authenticated whole message



* 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

1. **Compare SNMP V1 and V3(5M)**

|  |  |  |
| --- | --- | --- |
| **Features** | **SNMP v1** | **SNMP v3** |
| Information Model | RFC 1155 | RFC 1902 |
| Philosophy | Makes use of scalar structure for creating objects. | Makes use of a modular structure to implement management. |
| Protocol operations | Get, GetNext, Set, Trap, Response | Uses SNMPv2c protocol operations and its PDU message format. |
| Security | No security mechanisms are implemented. | Implements security based on VACM and USM. |
| Community strings | Plain text | Encrypted texts. |
| Compatibility | Only compatible with SNMPv2 through use of proxy server or bilingual managers. | Backward compatible with SNMPv1 due to modular architecture. |
| MIB | Defines limited, easily implemented MIB of scalar variables and two-dimensional tables. | Can configure agents to provide a number of levels of access to MIB. |
| Susceptible to attacks | Injection attack, replay, and sniffing attacks. | Security mechanisms make it immune to injection attacks. |

1. **Compare SNMP v1 , v2 and v3.**

|  |  |  |  |
| --- | --- | --- | --- |
| **Feature** | **SNMPv1** | **SNMPv2** | **SNMPv3** |
| **Release Year** | 1988 | 1993 | 2004 |
| **Security** | Minimal; community string in plain text | Minimal; similar to SNMPv1 | Enhanced; includes user-based security model (USM) and view-based access control model (VACM) |
| **Message Format** | Simple; Get, Set, Trap | Enhanced; includes GetBulk and Inform | More complex; includes cryptographic security features and improved message format |
| **Transport Protocol** | UDP, IP | UDP, IP | UDP, IP; also supports TCP, SSH, TLS |
| **Operations** | Get, Set, Trap | Get, Set, Trap, GetBulk, Inform | Get, Set, Trap, GetBulk, Inform |
| **Management Information Base (MIB)** | Supports SMIv1 | Supports SMIv1 and SMIv2 | Supports SMIv1 and SMIv2 |
| **Efficiency** | Basic, single operations per request | Improved; bulk operations | Efficient; supports bulk operations and enhanced security features |
| **Authentication** | None (community string is not secure) | None (community string is not secure) | User-based authentication, including MD5 and SHA |
| **Encryption** | None | None | Supports encryption (DES, AES) |
| **Privacy** | None | None | Ensures data privacy through encryption |
| **Interoperability** | Widely supported | Widely supported | Widely supported but requires more configuration due to security features |
| **Trap Handling** | Traps sent without acknowledgment | Inform operation allows acknowledgment | Inform operation with acknowledgment and security features |
| **Use Case** | Basic network management tasks | Enhanced data retrieval capabilities | Secure and scalable network management |

1. **Compare CMIP with SNMP**

|  |  |  |
| --- | --- | --- |
| **features** | **CMIP** | **SNMP** |
| Information Model | Object oriented | Simple scalar objects |
| MIB language | GDMO | SNMP SMI |
| Management entity interactions | Manager – Agent  Manager – Manager | Manager – Agent  Manager – Manager |
| Protocol operations | M-Create, M-Get, M-Action, M-Set  M-Delete, M-Event-Report | Get, Set, limited create/delete Trap |
| Managed object addressing | MIT with OID  scoping/filtering. | MIT with OID  at leaves of the tree. |
| Management applications | Five functional areas. | Not specified. |
| Standardization body | ITU-T, ISO. | IETF. |

1. **compare RMON with SNMP**

**A white sheet of paper with black text

Description automatically generated**

1. **Explain the features of SNMP V3 protocol?**

* **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.

1. **What is SNMPV3 MIB,Message format,architecture,engineID,security services?**
2. **Describe SNMP V3 policy based security management?**

Describe reasons for RMON development(5M)