APPLICATION OF COMMON MANAGEMENT INFORMATION PROTOCOL (CMIP) IN ATM NETWORK BANDWIDTH ALLOCATION SYSTEM

BY

ONYISHI, IFEYINWA ROSEMARY

PG/M.ENG./11/59432

DEPARTMENT OF ELECTRONIC ENGINEERING,

FACULTY OF ENGINEERING

UNIVERSITY OF NIGERIA, NSUKKA

JULY, 2014

TITLE PAGE

APPLICATION OF COMMON MANAGEMENT INFORMATION PROTOCOL (CMIP) ON ATM NETWORK BANDWIDTH ALLOCATION SYSTEM

BY

ONYISHI, IFEYINWA ROSEMARY

PG/M.ENG./11/59432

A PROJECT PRESENTED TO THE DEPARTMENT OF ELECTRONIC ENGINEERING, FACULTY OF ENGINEERING

UNIVERSITY OF NIGERIA, NSUKKA

IN PARTIAL FULFILMENT OF THE REQUIREMENTS FOR THE AWARD OF MASTER OF ENGINEERING (COMMUNICATIONS) DEGREE IN ELECTRONIC ENGINEEERING

SUPERVISOR: PROF. C. I. ANI

JULY, 2014.

APPROVAL PAGE

APPLICATION OF COMMON MANAGEMENT INFORMATION PROTOCOL (CMIP) ON ATM NETWORK BANDWIDTH ALLOCATION SYSTEM

ONYISHI, IFEYINWA ROSEMARY

PG/M.ENG./11/59432

A THESIS SUBMITTED IN PARTIAL FULFILMENT OF THE REQUIREMENTS FOR THE AWARD OF MASTER OF ELECTRONIC ENGINEERING (COMMUNICATION OPTION) IN THE DEPARTMENT OF ELECTRONIC ENGINEEERING UNIVERSITY OF NIGERIA, NSUKKA.

ONYISHI IFEYINWA ROSEMARY SIGNATURE................DATE.............
(STUDENT)

PROF. C.I.ANI SIGNATURE................DATE............
(SUPERVISOR)

EXTERNAL EXAMINER SIGNATURE................DATE.............

PROF. C.I.ANI SIGNATURE................DATE............
(HEAD OF DEPARTMENT)

PROF. E.S. OBE SIGNATURE................DATE............
(CHAIRMAN FACULTY POST-
GRADUATE COMMITTEE)

CERTIFICATION

Onyishi Ifeyinwa Rosemary a masterꞌs degree postgraduate student in the Department of Electronics Engineering and with registration number PG/M.ENG./11/59432 has satisfactorily completed the requirement for the award of Master of Engineering (M.ENG) in Electronic Engineering.

PROF. C.I. ANI	**PROF. C.I. ANI**
(SUPERVISOR)	**(HEAD OF DEPARTMENT)**

PROF. E.S. OBE

(CHAIRMAN FACULTY POSTGRADUATE COMMITTEE)

DECLARATION

I Onyishi Ifeyinwa Rosemary a postgraduate student of the Department of Electronic Engineering, University of Nigeria, Nsukka, declare that the work embodied in this thesis is original and has not been submitted by me in part or in full for any other diploma or degree of this or any other University.

ONYISHI IFEYINWA ROSEMARY DATE

DEDICATION

I dedicate this work to the Almighty God for his guidance and protection.

ACKNOWLEDGEMENT

I would like to express my gratitude to my project supervisor, Prof. C.I. Ani, for guidance, inspiration and supervision of this thesis. I was able to learn a lot from him. His achievements and attitudes have inspired me in many ways. His advice is always pertinent; it has led me to new ideas for solving the problems I have faced.

My thanks also go to the entire staff of the Department of Electronic Engineering, University of Nigeria, Nsukka, most especially, Prof. O.U Oparaku, Prof. C.C. Osuagwu Prof. A.N. Nzeako and Engr. Ahaneku. Their advice and constructive criticisms contributed in no mean measure to the successful completion of my programme.

There are many people who have made this dissertation possible; without them it would have been impossible for me to finish it. Though it is difficult to name them without omitting someone, I am happy to acknowledge them here, and I apologize if I have omitted anyone. First of all, I would like to thank my parents and Engr. P.C. Ngwu for their financial and moral support throughout this study.

I would also wish to express my sincere appreciation to all the members my class, Josiah, Kingsley, Godwin, Michael, Cresentus, Nenye to mention but a few, who gave me so many good suggestions when I did the implementation part for this thesis. Very big thanks to all my friends and classmates. Without their generous help, continuous encouragement and moral support, this work could not have been completed.

TABLE OF CONTENTS

CHAPTER ONE: INTRODUCTION

CHAPTER TWO: LITERATURE REVIEW

CHAPTER THREE: PROCESS MODELING

CHAPTER FOUR: SIMULATION RESULTS AND ANALYSIS

CHAPTER FIVE: CONCLUSION

ABSTRACT

Asynchronous Transfer Mode (ATM) of transmission is designed as a Broadband Integrated Services Digital Network (B-ISDN) transfer mode that supports a wide range of traffic classes with diverse flow characteristics. ATM guarantees different quality of service (Q_oS) demands placed on a network by different services (traffic types). The above powerful feats could be well achieved in ATM network with the application of an efficient and effective network resource management system. This thesis therefore, focused on the application of Common Management Information Protocol (CMIP) in the management of ATM network resources.

In this thesis, ATM network resource management system is modelled using CMIP principle. The management system was applied in the allocation of network bandwidth on a real-time basis. The performance of the system was analysed and considered satisfactory.

LIST OF FIGURES

LIST OF TABLES

LIST OF ABREVATIONS & ACRONYMS

AAL	ATM Adaptation Layer
ABR	Available Bit Rate
ABT	ATM Block Transfer
ACR	Allowed Cell Rate
ACSE	Association Control Service Element
AD	Area Director
ATM	Asynchronous Transfer Mode
ATM_PDU	ATM Protocol Data Unit
CCITT	Comitə Consultatif International De Telegrphique Et Telephniqe
CMIP	Common Management Information Protocol
CMIS	Common Management Information Service
CMISE	Common Management Information Service Element
CORBA	Common Object Request Broker Architecture
DN	Distinguishing Name
GDMO	Guideline for Definition of Managed Objects
GFC	Generic Field control
IDL	Interface Definition Language
IETF	International Engineering Task Force
ISO	International Standard Organisation
ITU	International Telecommunication union
ITU-R	International Telecommunication union- Radio
ITU-T	International Telecommunication union-Telecommunication
MIB	Management Information Base
MIT	Management Information Tree
MO	Managed Object
NCC	Network Control Centre
NEF	Network Element Function
NCCF/NPDA	Network Central Control Facility /Network problem determination Aid
NIC	Network Interface Card
NNI	Network-Network Interface

NM	Network Management
NMP	Network Management Protocol
NMS	Network Management system
OAM	Operation Administration Management
OAM&P	Operation Administration Management and Provision
OAN	Optical Access Network
OMG	Object Management Group
ORB	Optimum Required Bandwidth
OSI	Open System Interconnection
PDU	Protocol Data Unit
QoS	Quality of Service
RFC	Request for Comment
ROSE	Remote Operations Service Elements
SMASE	System Management Application Source Element
SMI	Structure of Management Information
SNMP	Simple Network Management
TCP/IP	Transport Control Protocol/Internet Protocol
TMN	Telecommunication Management Network
UDP	User Datagram Protocol
UNI	User-Network Interface
VC	Virtual Channel
VCC	Virtual Channel Connection
VCI	Virtual Channel Identifier
VP	Virtual Path
VPC	Virtual Path Connection
VPI	Virtual Path Identifier
VPN	Virtual Private Network
VPT	Virtual Path Termination
WSF	Work Station Function

CHAPTER ONE
INTRODUCTION

1.0 BACKGROUND

Since 1970s, some of the network management functions have been emphasized more than others and the tools have evolved from manual and standalone tools to sophisticated knowledge based integrated system. The methods and tools in network management have evolved in four stages.

In 1970s, the main focus was on fault management (terminals unable to logon, modem problems, and communication line problems) for small (a few hundred devices) networks.

The faults were managed through a ñproblem control deskò which receives customer calls, records the problems and dispatches them to technicians that will diagnose and correct the problems [1]. The technicians used manual procedure and system display commands, and ran diagnosis on the equipments. Most diagnostic tools then were primitive and stand-alone. An example of a more sophisticated tool in this stage is IBMôs NCCF/NPDA (Network central Control facility / Network problem determination Aid) which was introduced to diagnose SNA Networks.There was little interoperability among management systems provided by different manufacturers. [2]

In 1980s Network management were developed for homogenous (single) vendor, medium sized (few thousand devices) networks. The existing network diagnostic tools are integrated with network monitoring and control tools into network management system (NMSs). Monitoring involves determining the status and processing characteristics currently associated with the different physical and logical components of the network [3].The first management system known as Net View was introduced by IBM in 1986. Net View integrated many of the network diagnostics and control tools developed in the 1970 and early 1980s into a single package. NMS like DECôs EMA, AT and Tôs starkeeper, and Avant ï Gardeôs Net command have also been developed.

In 1990s NMSsô development focused on managing bigger Networks (internetwork) for thousands of devices connected over thousands of lines which may cross international boundaries. In most cases, the human network managers cannot see the device being diagnosed and the type and manufacture of a device is not known. Due to the complexity and size of networks being managed, this stage has witnessed development in three areas [4]:

- The growth of network management standard.
- The evolution of ñenterprise management systemsò which integrate individual network management systems for large heterogeneous environments.
- The increased utilization of expert systems and database technologies in network and enterprise management.

In 2000s the focus of Network management shifted to distributed system management where all system resources are managed through a platform. The main area of work is management of internet and the web resources. The focus is on enterprise management system that coordinates various other nature managers for managing large heterogeneous network environment. The next generation of management tools is appearing as Expert Support System (ESS) and Decision Support Systems (DSS) to support the network planning, installation, maintenance and performance activities. These systems are exploiting the advances and database technologies and software engineering for large and complex network management and enterprise management systems [5].

An ATM network is used as a multi-service network to integrate different services like voice, music, telephony and video over a single network. Such multi-device network realises its function by employing network resource allocation system that ensures that each service is offered with standard (Q_oS). This is achieved not minding that each service has a contradicting demand on the network resource [6].

The ATM network resources include [7]:

- set of VP and VC identifiers (VPI and VCI) to identify connections;
- Bandwidth available on the Transmission Paths;
- Buffer space evaluated in number of cells either internally (in switch fabric) or externally (outside switch fabric transmission buffer).

Having underscored bandwidth as one of the basic resources in an ATM network, there is need for effective bandwidth allocation strategy. Efficient allocation and management of bandwidth ensures the following [8]:

- Optimization of bandwidth utilization to enable networks run at its maximum capacity and thereby increasing network revenue generation.
- As new applications emerge and new networking equipment is deployed, network bandwidth management controls flow of traffic in the network during transitions.

The main network management standards are common management information protocol (CMIP) by ISO/OSI and simple Network management protocol (SNMP) for TCP/IP based network [9]. This network favours CMIP. Most network management systems are realised using SNMP protocol.

Performance management system assists the operator to effectively monitor and control the network. The main goal for the operator is to manage the network in a cost effective way and still retain the servicesô Q_oS. This project, therefore, focused on the *application of bandwidth resource allocation technique* in the ATM Network in the Common Management Information Protocol Environment.

1.1 PROBLEM STATEMENT

The management of modern telecommunication networks like ATM Networks is growing in complexity due to increased Network versatility and connectivity. Losses associated with bandwidth allocation increases as the traffic increases. The need for a sophisticated management protocol to handle this problem arises. CMIP will perform bandwidth allocation to avoid losses associated with it.

1.2 OBJECTIVE OF THE WORK

The aims of carrying out this study include:

- The application of CMIP on ATM resource management technique
- To use CMIP to allocate resources to minimize call drop

This work will be useful in any organisation that implements ATM network where it is required to solve problems associated with improper bandwidth utilization. It can also be applied in other types of network to allocate resources.

1.3 SCOPE OF THE WORK

This work is limited to ATM network bandwidth resource allocation for data, voice and video services. The function of bandwidth allocation is realised using Common Management Information Protocol. The analysis of the allocation system is based on the computer simulation of the model.

1.4 METHODOLOGY

The following steps were taken in order to realise this project.

1. literature review / review of related works
2. Model development
3. Model simulation in MATLAB Environment
4. Model Result Analysis

1.5 ORGANISATION OF THE WORK

The remaining part of this work is organized in chapters as follows: Chapter Two presents an overview of ATM Network and its Q_OS and performance parameters. Network management, management functions, network management protocol with detailed explanation in CMIP and review of network performance management. Related works are also reviewed and documented. Chapter Three presented models and simulation of CMIP protocol on ATM. Chapter Four presents the simulation, results and analysis. Chapter Five presented the recommendations and conclusions.

CHAPTER TWO

LITERATURE REVIEW

2.0 INTRODUTION

In this chapter, ATM network as it relates to network performance management, different network management architectures, protocols and standards are presented. Other related works on CMIP and other bandwidth allocation techniques are also presented.

2.1 ASYNCHRONOUS TRANSFER MODE (ATM)

ATM is a high-speed connection-oriented cell based switching and multiplexing technology with little or no error control [10, 11]. It is designed to offer flexible transmission support for a wide range of services including voice, video, and data [12]. ATM can support any traffic type in separate or mixed streams, delay-sensitive traffics, and non-delay-sensitive traffics. ATM combines both circuit switching and packet switching [13].

2.1.1 ATM Physical Architecture

ATM physical architecture shows how ATM switches and end systems are arranged in a network. Figure 2.1 is ATM physical architecture and below it are the explanation of its components and interfaces.

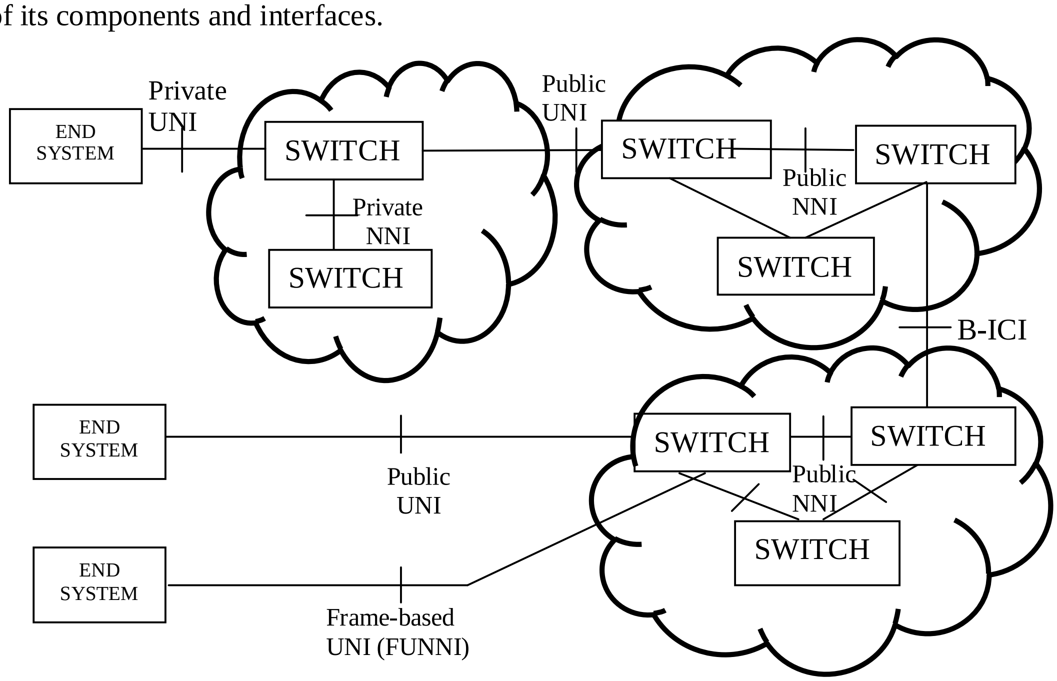


Figure 2.1: ATM Architecture [12]

ATM physical architecture is comprises of ATM components and interfaces linking one component to another.

A. *ATM Components*

An ATM network consists of end systems and switches.

1) ATM End System

ATM End system (also called an edge device) can be an ATM user terminal or a gateway between the ATM network and another type of network. They include ATM attached workstations, ATM attached server, ATM switches and ATM routers. They are points on an ATM network where an ATM connection is initiated or terminated.

2) ATM Switch

The basic function of an ATM switch is to switch cells between a virtual channels or paths on an incoming link and a preconfigured virtual channel or path on an outgoing link. The central part of the switch is a non-blocking, hardware, switching matrix known as a **switching fabric**.

B. *ATM Nodes and Interfaces*

ATM User-to-Network Interface (UNI) is the interface between an ATM switch and ATM end system [14]. It is known as access interface, the User-to-network Interface (UNI) specification defines two types of ATM UNI:

1. *Public UNI* is connection between a private ATM switch and an ATM switch residing within a public service provider, where the private ATM acts as a UNI device
2. *Private UNI* is connection between an ATM end system (such as ATM router interface or ATM attached server) and an ATM switch found within the same private ATM Network

ATM Network –to -Node Interface (NNI) is the interface between two switches of an ATM also known as network interface. NNI specification defines two types of ATM NNI.

1. *Public NNI* is the connection between two public ATM switches within the same public network that is network nodes of a WAN.

2. *Private NNI* is switch-to switch connection on an internal network such as connection between an inter private WAN, LAN.

C. ATM B-ICI is the connection between two public ATM networks.

2.1.2 ATM Protocol Architecture

ATM protocol model as defined by standards is presented using related ISO-OSI reference model.

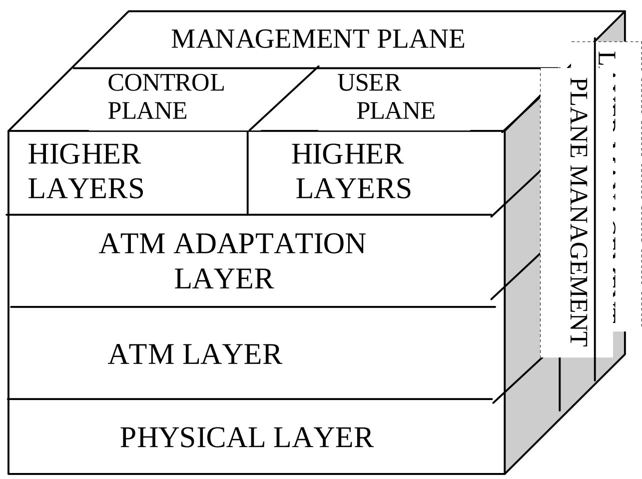


Figure 2.2: ATM Reference Model [15]

1) Physical Layer

Physical layer consists of two sub layers: [16]

i. <u>*Transmission convergence* (TC)</u> sub layer functions as:

- *Transmission frame generation/recovery:* Generates and maintains the required physical layer frame structure appropriate for a given data rate.
- *Transmission frame adaptation:* Packages incoming ATM layer cells into frames
- *Cell delineation:* Maintains the cell boundaries so that cells may be recovered after descrambling at their destination
- *HEC sequence generation/cell header verification:* Generates and checks the *header error-control* (HEC) code used to protect cell headers
- *Cell rate decoupling:* Inserts and suppresses idle cells in order to adapt the rate of valid ATM cells to the payload capacity of the transmission system in use.

ii. *Physical Medium (PM) Sub layer* provides the medium for physical connection. It is responsible for transmitting/receiving a continuous flow of bits with associated timing information to synchronize transmission and reception.

2) ATM Layer

- *Cell multiplexing and de multiplexing*: It does multiplexing and de multiplexing so that all ATM layer cells can be carried over a physical layer medium.
- Cell *virtual path identifier* (VPI)/*virtual channel identifier (VCI) translation*: It converts the VPI and VCI of incoming cells into the ones that are required for the next hop at a switch or a cross-connect during switching, as VCI/VPI only has local significance.
- *Cell header generation/extraction:* This appends cell header to user data from the AAL layer for physical layer transmission and extracting user *Asynchronous Transfer Mode* data from cells received. This function may also include the translation of an address to VPI/VCI.
- *Generic flow control* (GFC): This is used to control cell transfer in a shared PM by several subscribers; one possible use is to resolve multiple access contention among multiple users at the UNI.

3) ATM Adaptation Layer

The *ATM adaptation layer* (AAL) adapts the services provided by the ATM layer to support the functions required by the next higher layer, such as network management protocols. It has two sub layers

- *Segmentation and Reassembly (SAR) sub layer* which is responsible for the segmentation of higher-layer data into a size suitable for an ATM cell information field and the reassembly of the contents of ATM cell information fields into higher layer information.
- *Convergence Sub layer (CS)* that provides the *ATM adaptation layer* (AAL) service at the AAL-*service access point* (SAP)

4) User ***Plane***

It provides for the transfer of user application information [17]. It contains physical layer, ATM layer, and multiple ATM adaptation layers required for different service users such as CBR and VBR service.

5) The Control Plane

Its protocols deal with call-establishment and call-release and other connection-control functions necessary for providing switched services. The Control-plane structure shares the physical and ATM layers with the User-plane. It also includes ATM adaptation layer (AAL) procedures and higher-layer signalling protocols [18].

6) The Management Plane

This provides management functions and the capability to exchange information between the User-plane and the Control-plane. The Management-plane contains two sections:

- *Layer management* performs management functions (e.g. meta-signalling) relating to resources and parameters residing in its protocol entities. Layer Management handles the operation and maintenance (OAM) information flow specific to the layer concerned. It detects failure and protocol problems [19].
- *Plane management* performs management functions related to a system as a whole and provides coordination between all the planes. Plane management has no layered structure. VPI and VCI are called connection identifiers.

2.1.2 ATM Cell

The unit of transmission, multiplexing and switching in ATM is the fixed-length cell of 53 bytes. [20, 21] A cell contains 48-octect cell payload (information field carrying user information) and a 5-octect header (information field carrying network information [22]). Its fixed length is chosen to simplify the design of electronics in ATM switches and multiplexers, because hardware manipulation of variable-length packets is more complex than processing a fixed length cell [23].

ATM Cell Structure

ATM cell is of two types UNI cell and NNI cell

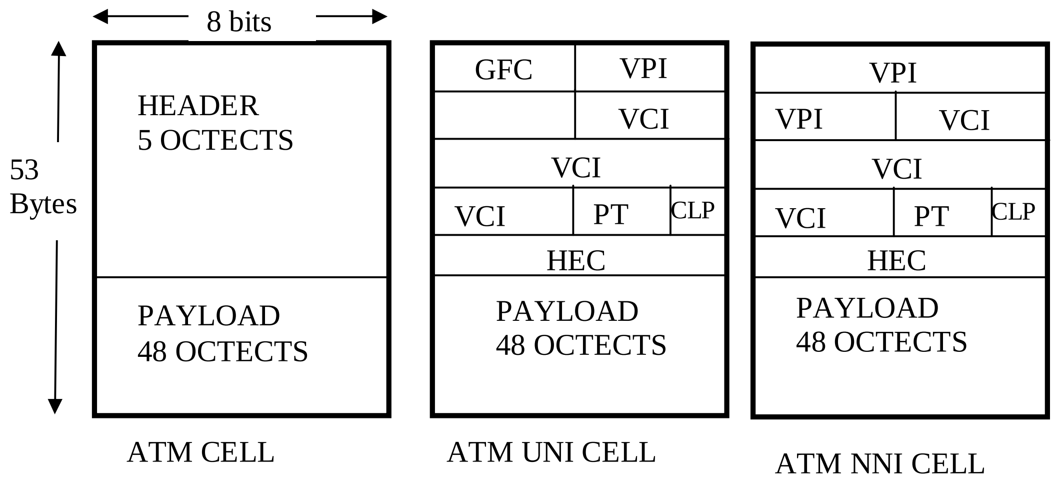


Figure 2.3 ATM Cell Structures [24]

Generic Flow Control (GFC) is for end to end flow control. It is added to support the connection of ATM Networks to shared access Networks. It gives the UNI 4bits which is used to negotiate multiplexing flow control among the cells of various ATM connections [25]. ATM cell at Network node interface (NNI) eliminates GFC field and uses the 4bits to increase the VPI instead.

Virtual Path Identifier (VPI) is used for routing. It is an 8 bit field in UNI and 12 bit field in UNI. In a UNI interface there is maximum of 256 virtual paths and 4096 virtual paths in NNI [15]

Virtual Channel Identifier (VCI) is a 16-bit field in both UNI and NNI interface used for routing.

Cell Loss Priority (CLP) prioritizes the order in which cells may be discarded in time of network problems. It acts as an indicator as to whenever or not this cell is expendable, should the Network start becoming congested. ñ1ò indicates ñcan discard the cellò and ñ0ò indicates ñmight not discard cellò.

Payload Type (PT) identifies the cell content, if it is data cell, and idle, an OAM cell, VCC- level OAM information, explicitly forward congestion indication (EFCI), AAL Information or resource management information.

Header Error Control (HEC) is an 8-bit CRC calculated over the remaining 32 bits in the header. It is used for error detection and single-bit error correction.

Payload contains User information or in band signalling information

2.1.4 ATM Virtual Connections

ATM connections are made up of VCs, VP and Physical Transmission Path as shown below.

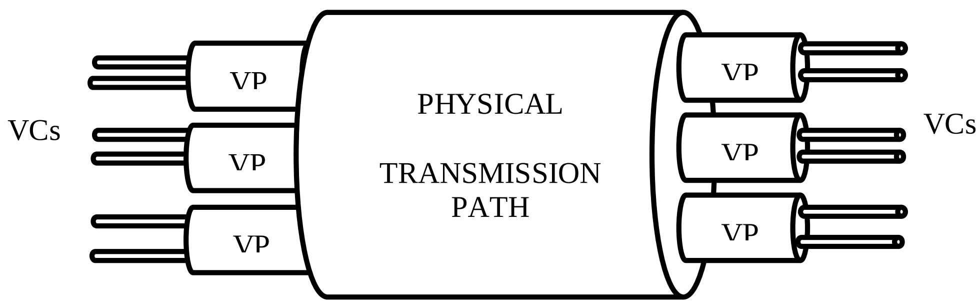


Figure 2.4: ATM Virtual Connections [26]

Physical Transmission Path is bundle of VPs. VCs concatenate to create VPs; VPs concatenate to create a transmission path [27].

The virtual path (VP) is a bundle of virtual channel links; all the links in a bundle have the same endpoints. A VPI identifies a group of VC links, at a given reference point, that share the same VPC. A specific value of VPI is assigned each time a VP is switched in the network. A VP link is a unidirectional capability for the transport of ATM cells between two consecutive ATM entities where the VPI value is translated [28]. A VP link is originated or terminated by the assignment or the removal of the VPI value.

Virtual channel (VC) is a unidirectional communication capability for the transport of ATM cells. A VCI identifies a particular VC link for a given virtual path connection

(VPC). A specific value of VCI is assigned each time a VC is switched in the network. A VC link is a unidirectional capability for the transport of ATM cells between two consecutive ATM entities where the VCI value is translated. A VC link is originated or terminated by the assignment or removal of the VCI value [29].

2.1.5 ATM Connection

ATM has two types of virtual connections:

Permanent virtual connection (PVC) is a connection that is setup and taken down manually by a network manager. A set of network switches between the ATM source and destination are programmed with predefined values for VCI/VPI.

Switched virtual circuit (SVC) is a connection that is setup automatically by a signalling protocol. SVC is more widely used because it does not require manual setup, but it is not reliable.

2.1.6 ATM Services

ATM forum specifies six types of services [30]. They are:

Constant bit rate (CBR). This is used for emulating circuit switching. The cell rate is constant with time. Telephone traffic, videoconferencing and television use CBR.

Variable bit rate–non real time (VBR–NRT). This service allows users to send traffic at a rate that varies with time depending on the availability of user information. Statistical multiplexing is provided to make optimum use of network resources. Multimedia email is an example of VBRï NRT.

Variable bit rate–real time (VBR–RT). This service is similar to VBRï NRT, but it is designed for applications that are sensitive to cell delay variation. Examples of real time VBR are voice with speech activity detection (SAD) and interactive conference video.

Available bit rate (ABR). This service provides rate based flow control and is aimed at data traffic such as file transfer and e-mail.

Unspecified bit rate (UBR). This class is widely used today for TCP/IP. Maximum cell transfer delay (Max CTD) Mean cell transfer delay (Mean CTD).

Guaranteed Frame Rate (GFR). This service provides the user with a Minimum Cell Rate (MCR) guarantee under the assumption of a given maximum frame size (MFS) and a given Maximum Burst Size (MBS). The MFS and MBS are both expressed in units of cells.

2.1.7 ATM Switch Architecture

For an ATM switch to perform its switching function there are components in it that performs the action. The diagram below shows a generic ATM switch and explanation of the components.

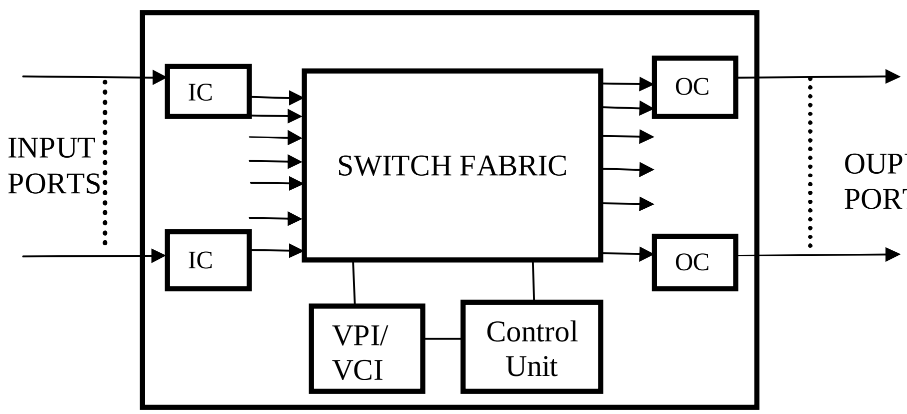


Figure 2.5: Generic ATM Switch [31]

- ***Components of an ATM switches***

An ATM switch is made up of: [32]

<u>*Input Port*</u> receives cells, identifies boundaries between adjacent cells, synchronizes timing between the external link and the switch, and buffers cells if necessary, changes VPIs/VCIs to the new VPIs/VCIs, appends necessary internal routing information to the cells.

<u>*Output Port*</u> removes any information appended to the cells by the input ports, identifies boundaries between adjacent cells, synchronizes timing between the external link and the switch, buffers cells if necessary and transmits the cells to the external link.

<u>*Control Unit*</u> performs control functions, such as cell header translation, arbitration among input modules, and performance management of the switch. Controls entire operation of switch that is Cell switching, Signalling (UNI and NNI), Call Admission

Control (CAC), Policing, Congestion control, Usage Parameter Control (UPC) and Accounting statistics

VPI/VCI memory is physical memory that is used to keep track of how to map cells of different VCôs from input ports to output ports.

Switch Fabric performs the core switching functions by delivering the input cells received by the input modules to the output modules. It also resolves any contentions between cells.

- ***Operation of an ATM Switch***

The cell is received across a link on a known VCI or VPI value. The switch looks up the connection value in a local translation table to determine the outgoing port (s) of the connection and the new VPI/VCI value of the connection on that link. The switch then transmits the cell on that outgoing link with the appropriate connection identifiers. Because all VCIs and VPIs have only local significance across a particular link, these values are remapped, as necessary, at each switch. An ATM switch performs Cell switching, Signalling, Call admission control, Usage parameter control and Accounting. [33]

2.1.8 ATM Network Management

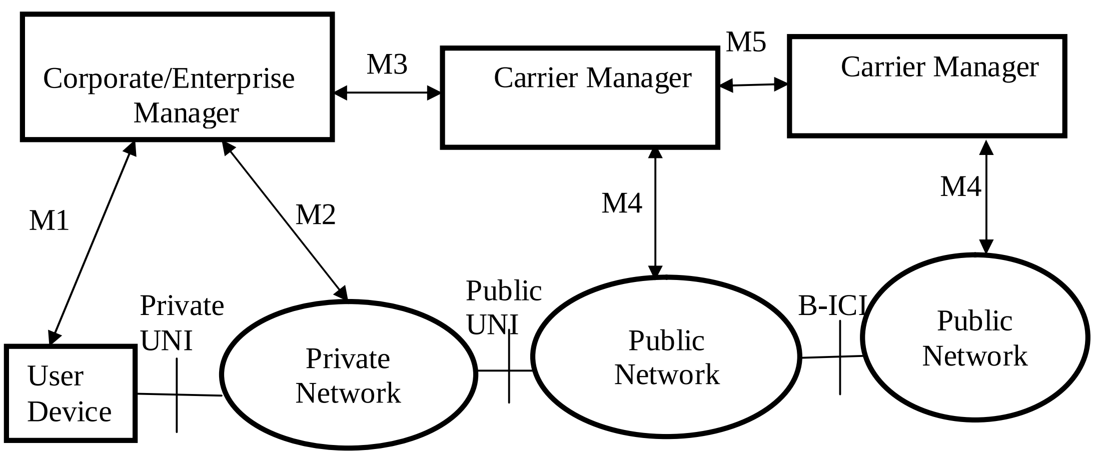


Figure 2.6: ATM Network Management Model [34]

M1: Management Interface between private Manager and an end user.

M2: Management Interface between an ATM switch of a private network and cooperate/ enterprise network manager.

M3: Management Interface between management system of a public network and management system of a private network.

M4: management interface between a public network and a network management system

M5: management interface between network management systems of two public networks.

2.2 Network Management

Network management may be defined as planning, organizing, monitoring and controlling of activities and resources within a networking system to provide a level of service that is acceptable to the user and the provider (owner) [35,36]. It can also be defined as OAM&P (Operations, Administration, Maintenance, and Provisioning) of network and services [37]. It may be performed by a human being, by automated systems or both. From Business Management point of view, Network management involves strategic and tactical planning of the engineering operations and maintenance of network and Network services for current and future needs at minimum overall cost.

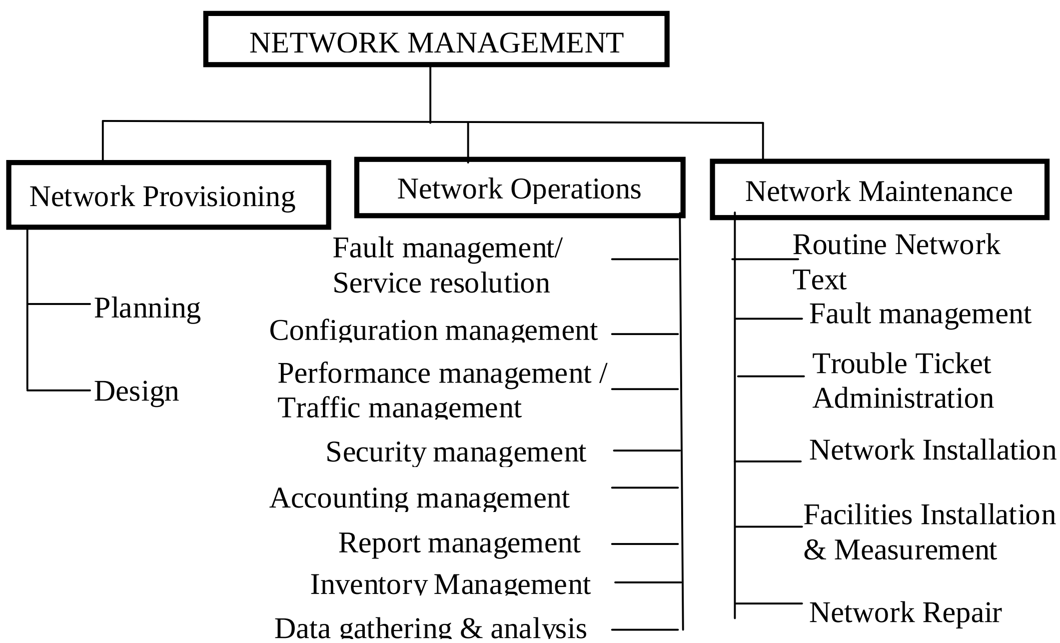


Figure 2.7: Network Management Functional Groupings [38]

NM is made up of 3 major functional groupings: Network provisioning, network operation and network maintenance as shown in figure 2.7.

- **Network Management Goal**

A NMS should achieve the following at the end of management operations [39]:

1) *Reduced operational cost:* A NMS should help the operator operate and maintain the network effectively at reduced cost.
2) *Provide security:* It should block an unauthorized user.
3) *Maximizing availability:* It should make the network available when it delivers services to the user with the required Q_OS.
4) *Enabling adaptability:* NMS should adapt to the new/change in network structure.
5) *Easy to change services and the Q_OS:* Services and users requirements of Q_OS evolve in time, so NMS should easily change or add new services and adjust their Q_OS.
6) *Easy network upgrade:* NMS should support network components from many vendors, so it becomes easy to expand or upgrade the network.

2.2.1 Network Management Model

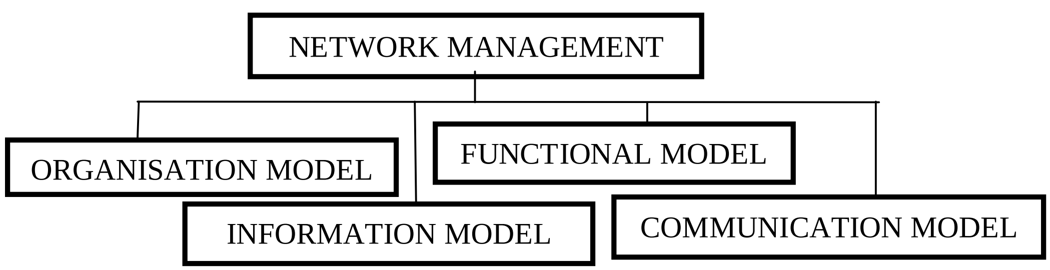


Figure 2.8: OSI Network Management Model [40]

Organisation Model describes components of network management and their relationships. Component of network management system are managed object, agent and the network manager.

Information Model is concerned with the structure and the storage of management information. It specifies the information base to describe managed objects and their relationships.

Functional Model addresses the user-oriented application specified in the OSI model. It describes NM functions such as Fault, Configuration, Accounting, performance and security management.

Communication Model addresses the way information is exchanged between systems (agents/managers). It is constitutes of 3 components: the management Application Process, Layer Management between layers and Layer Operation within the layers [41].

2.2.2 Network Management Architecture

Network management architecture determines how and where management mechanisms are applied in a network. Most network management systems have the same basic structure and set of relationship even if the components can be named differently [35]. Network management system comprises of these components: A Network Manager, An Agent, Managed Objects (MO), Management Information Base (MIB) and A Network Management Protocol.

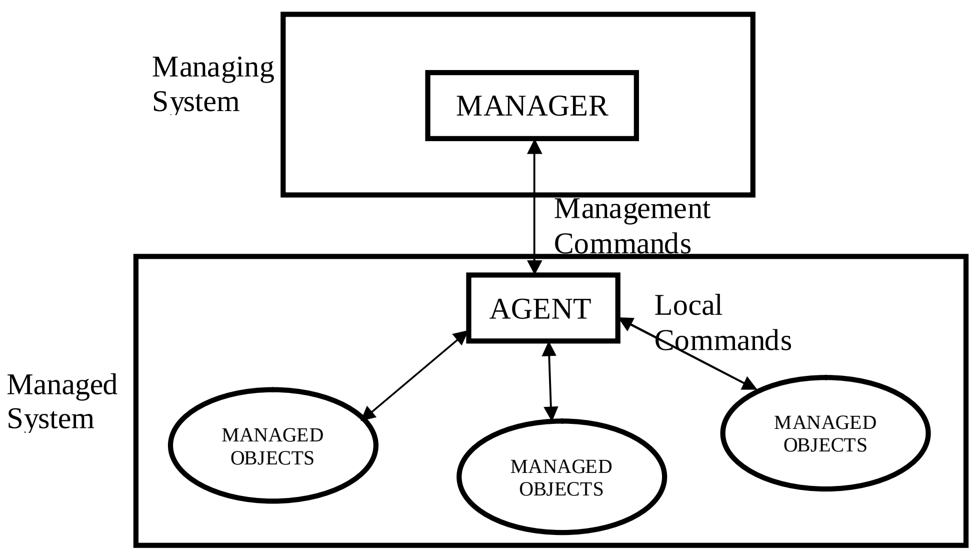


Figure 2.9: Generic Network Management Systems [36]

1. *Network Manager*

A network manager is a stand-alone device, but can be implemented on a shared system that runs applications to display management data, monitors and control managed devices by communicating with their agents [42]. A manager has sophisticated graphics, memory, storage and processing capabilities. It handles polling, which is about getting data about objects from the MIBs residing in the network devices. These objects information are stored in the manager MIB.

2. *An agent*

An agent is network management software package that resides in every managed system. An agent tracks local management information and uses a protocol to send information to the manager. That is it administrates the MIB and handles the communication with the manager and other devices in the network. Summarily, Agent gathers information from managed objects, Configure parameter of the objects, respond to managersô requests and generate Alarms and send them to manager

3. *Managed Objects*

This is a logical view for the purposes of network management of a manageable physical or logical resource of the network [36]. It can be protocol entities, a switch, a router, a multiplexer, a workstation a buffer management routine, a routing algorithm, an access scheme, or other software packages.

Each managed object has an **object class** which represents a collection of managed objects with the same or similar properties. A particular managed object existing in a particular network is defined as an object instance of the object class to which it belongs. Thus, an **object instance** represents an actual realization of an object class (i.e., a managed object of a particular class bound to specific values). A managed object is described by four parameters [37]:

PARAMETERS	**DESCRIPTION**
ATTRIBUTES	Describes the current state and condition of operation of managed objects.
OPERATION	Actions that are performed on the managed objects.
NOTIFICATION	Reports provided by the managed objects about events that occurred within its domain.
BEHAVIOUR	Actions exhibited by the managed objects in response to the operations performed on it, or to internal stimuli like notice.

4. *Management Information Base (MIB)*

MIB is a virtual database used to define the functional and operational aspects of network devices [36]. The MIB contains an abstract image of the managed objects within a network, and provides a method of relating managed objects to each other. It is by manipulation of the virtual objects within the MIB that the actual resources within a managed system can be examined or changed by the network manager [37]. Managed objects are organised in a containment hierarchy or tree structure, where the subordinate nodes on the tree are contained within superior objects in the MIB. This tree is called a management information tree (MIT). Each managed object has a name, and this name is formed by concatenating the names of all its superior objects within the MIT. The object at the top of the tree is the root and an objectôs name relative to the root is called its distinguishing name (DN). These names are used to select managed objects during the information exchanges that occur between managers and agents [43].

5. *Network Management Protocol*

A Network management protocol is used by the manager and the agents to communicate with each other. Well known network management protocols are Simple network management protocol (SNMP), and Common management information protocol (CMIP) [39]. Network management protocol shall be discussed in details later.

2.2.3. Structure and Arrangement of Network Management Systems

Network management architecture can be classified as [44]:

1) Mode of transfer of management information

    a) In-band management
    b) Out-of-band management
    c) Combination of in-band and out-of-band management.

2) Structural arrangement of components
    a) Centralized management
    b) Distributed management
    c) Hierarchical management.

1) Mode of transfer of management information

a) In-band Management

Network management data travels across an internetwork using the same path as user traffic [45]. It has simple structure, cheap and easy to set up, but management data flows can be affected by the same problems that affects user traffic flows like congestion. So when network management is most needed, it may not be available. This network management architecture does event monitoring when the network is under stress and takes the necessary action.

b) Out-of-band Management architecture

Network management data and user data travel on different paths. It allows the management system to continue to monitor the network during most network events, even when such events disable the network. This allows you to effectively see into portions of the network that are unreachable through normal paths (i.e., user data flow paths) [39]. A trade-off with out of-band monitoring is that there are security risks associated with adding extra links between managers and agents. To reduce risk, the links should be carefully controlled and added only if absolutely necessary. Another trade-off is that it is expensive since it require extra path.

c) In-band and out-of-band management combined

In this architecture, there is still the expense and complexity of out-of-band management, as well as the additional security requirements [35]. However, the combination allows (typically) higher performance in-band management to be used for monitoring (which is the high-capacity portion of network management), yet still allows out-of-band management to be used at critical times (e.g., when the user data network is down).

2) Structural arrangement of components

a) Centralized Management

In this architecture all management data radiate from a single management system. Agents are distributed across the internetwork and send data to the centralized manager. The data can be sent via out-of-band or in-band paths. This workstation is a single point of failure, and if it fails, the entire network could collapse. In case the management host does not fail, but a fault partitions the network, the other part of the network is left without any management functionality. Also, a centralised system cannot easily be scaled up when the size or complexity of the network increase [5,6]. A variation of centralised systems is the platform approach [47], in which a single manager is divided into two parts: the management platform and the management application. The management platform is mainly concerned with information gathering and simple calculations, while management application uses the services offered by the management platform to handle decision support and higher functions [7]. The advantage of this approach is that applications do not need to worry about protocol complexity and heterogeneity. The drawback is that it still inherits limited scalability from its centralised nature. The diagram of centralized network management architecture is shown in figure 2.10.

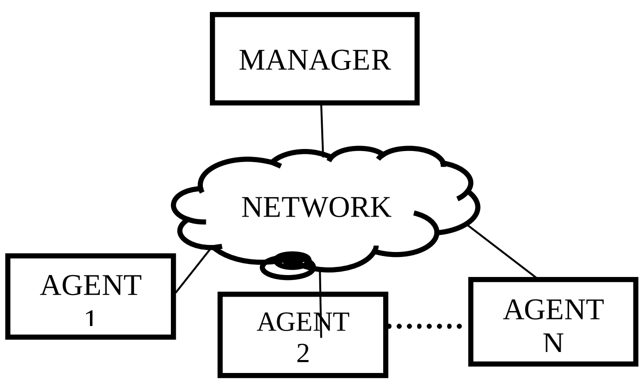


Figure 2.10: Centralized Management Architecture [34]

b) Distributed Management:

It consists of multiple separate components that are strategically placed across the network, localizing network management traffic and distributing management domains. Multiple managers are used to distribute management functions across several domains mean that is managers and agents are spread out across the internet work [35]. Distributed management may take the form of having multiple management systems on the network (e.g., one management system per campus or per management domain, as shown, or a single management system with several monitoring nodes. There is no direct communication between different domains managers. The generic diagram of distributed network management architecture is shown in figure 2.11.

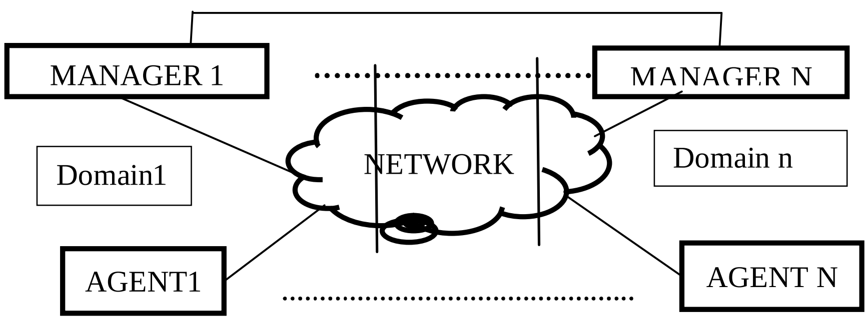


Figure 2.11: Distributed Network Management Architecture

c) *Hierarchical Management*

This occurs when the management functions are separated and placed on separate devices. Management is hierarchical in that, when the functions are separated, they can be considered as layers that communicate in a hierarchical client-server fashion. In hierarchical management, localized monitoring devices collect management data and pass these data either directly to display and storage devices or to monitoring devices to be processed. When the management data are passed on to display and storage devices without processing, the monitoring devices act as they did in distributed management, localizing the data collection and reducing the amounts of management data that transit the network [35]. The hierarchical architecture uses the concept of ñManager of Managersò ($M_O M$) and manager per domain paradigm [48]. Each domain manager is only responsible for the management of its domain, and is unaware of other domains. The manager of managers sits at a higher level and request information from domain managers. In this architecture, there is no direct communication between domain managers. This architecture is quite scalable, and by adding another level of M_OM a multiple level hierarchy can be achieved. The generic diagram of hierarchical network management architecture is shown in figure 2.12.

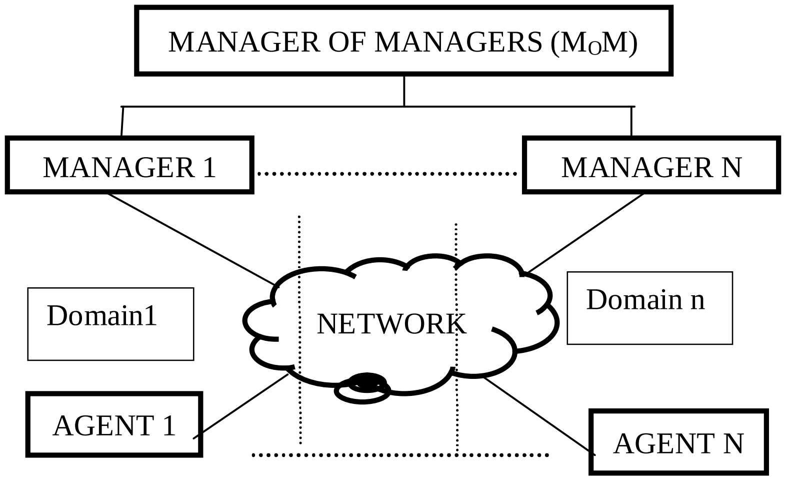


Figure.2.12: Hierarchical Network Management Architecture

d) *Network Architecture:*

This is combination of the hierarchical and distributed architectures [47]. This architecture uses both manager-per-domain and manager of managersô concepts, but instead of a purely peer-system or hierarchical structure, the managers are organised in a network scheme. This approach preserves the scalability of both systems and provides a better functionality in diverse environments. The generic diagram of network architecture is shown in figure 2.13.

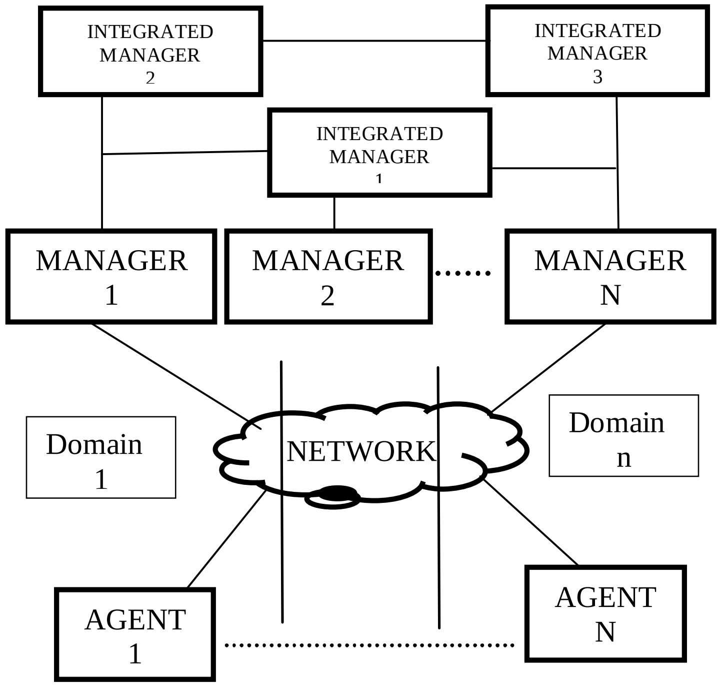


Figure.2.13: Network Architecture.

2.2.4 Network Management Functions

Network functions entail Fault Management, Configuration Management, Accounting Management Performance Management and Security Management.

1) <u>Fault Management</u>

This involves monitoring, provision and response to facilities so as to detect, isolate and resolve abnormal conditions in a network and restore it to normal operating condition [36, 37]. Fault management includes the ability to detect faults, to perform diagnostic test on a managed object to define the fault and to perform operation on managed objects to correct the fault (if its software faults) or to take the object out of service for physical maintenance (if its hardware faults). The manager makes use of event reporting, confidence and diagnostic testing, log control, and alarm report in fault management. Fault management functions include [49]:

1. To maintain and examine error logs.
2. To accept and act upon error detection notifications.
3. To trace and identify faults.
4. To carry out sequences of diagnostic tests.

5. To correct faults.

Fault management functions are achieved with the following steps [39]:

1) Fault detection: Detects fault in the network and identify problem symptoms.
2) Identification and isolation: Identify the network element where a fault has occurred. Isolate the problem and take the faulty network element out of operation.
3) Fault measures: Fix the problem.
4) Test the fault measures: Test if the fault measures really fixed the problem and that they do not have any negative side effects to the rest of the network. Then put it on operation as usual.
5) Logging: Record the fault detection and the management actions that were used to solve the problem.

2) <u>Configuration Management</u>

This involves maintaining, adding and updating records of hardware and software components, defining their functions and usability initializing the network, and ensuring that the network is described correctly and completely at all times. It also assigns, maintains and updates records of users, including billing responsibilities and communication privileges. A critical feature of configuration management is the ability to cope with the control, change [36]. Configuration management includes functions to [49]:

a) Set the parameters that control the routine operation of the open system;
b) Associate names with managed objects and sets of managed objects;
c) Initialize and close down managed objects;
d) Collect information on demand about the current condition of the open system;
e) Obtain announcements of significant changes in the condition of the open system;
f) Change the configuration of the open system.

In describing the states of the objects in a network, configuration management distinguishes between administrative states and operational states [37]:

1) Administrative state descriptors are

a) Unlocked (managed object can be used);
b) Locked (managed object cannot be used);
c) Shutting down (managed object will honour current users but will not accept new users).

2) Operational states descriptors are

a) Enabled (managed object is operate available and not in use);
b) Disabled (managed object is not available);
c) Active (managed object is available for used and can accept new user) and
d) Busy (Resources is available but cannot accept new users).

3) Accounting Management

The goal of accounting management is to measure network utilization parameters so as to regulate the network access. Such regulation minimizes network problems (because network resources can be apportioned based on resource capacities) and maximizes the fairness of the network access across all user [37]. It involves tracking the usage of network resources by performing password administration and billing. Measurement of resource use can yield billing information as well as information used to achieve optimal resources utilization [40]. Accounting management functions include [49]:

a) To inform users of costs incurred or resources consumed;
b) To enable accounting limits to be set and tariff schedules to be associated with the use of resources; and
c) To enable costs to be combined where multiple resources are invoked to achieve a given communication objective.

4) Performance Management

Network performance management involves monitoring network utilization, end-to-end response time, availability accuracy throughput and other performance measures at various points in a network so as to improve the performance of the network [36, 37]. Therefore the goal of Network performance management is to measure and make available various aspects of network performance so that network performance can be maintained at an acceptable level [5]. Performance management functions includes: [49]

a) To gather statistical information;

b) To maintain and examine logs of system state histories;

c) To determine system performance under natural and artificial conditions; and

d) To alter system modes of operation for the purpose of conducting performance management activities.

5) Security Management

The goal of security management is to control access to the network resources according to local guidelines so that the networks cannot be sabotaged and to ensure that sensitive information cannot be accessed by those without appropriate authorization [37, 39]. The purpose of security management is to support the application of security policies by means of functions which include: [49]

a) The creation, deletion and control of security services and mechanisms;

b) The distribution of security-relevant information; and

c) The reporting of security-relevant events.

2.2.5 Network Management Standards

These are bodies that are responsible for the regulation of network management protocols. Each standard has a particular network management protocol they are regulating. Below are the descriptions of standards and their network management protocols.

1. *The International Telecommunication Union (ITU):*

The International Telecommunication Union (ITU) is a specialized agency of the United Nations responsible for telecommunications. It has nearly 200 member countries and their head-quarter at Genera [50]. Standardization work is divided between two major standardization bodies: ITU-T and ITU-R The Comité Consultatif International de Télégraphique et Téléphonique, or International Telegraph and Telephone Consultative Committee (CCITT/ITU-T) is presently called ITU-T, where the ñTò comes from telecommunications. The website is http:/www.itu.ch/itudoc/itu-t/red.html. The Comité Consultatif International des Radiocommunications or International Radio Consultative Committee (CCIR/ITU-R) is presently known as ITU-R, where the ñRò stands for radio. The website is http:/www.itu.ch/itudoc/itu-r/red.html.

2. *The International Standard Organization (ISO)*

ISO is a worldwide federation of national standards bodies with representatives from over 100 countries. It is a non-governmental organization established in 1947. Its mission is to promote the development of worldwide the international exchange of goods and services and to develop co-operation in the spheres of intellectual, scientific, technological and economic activity. The open system interconnection (OSI) reference model is a seven layer decomposition of network function published by the ISO [51]. OSI is a set of communication standards and protocols that aims at establishing an open environment for the movement of data between devices. The website is http://www.iso.ch/

3 *The Internet Engineering Task Force (IETF)*

IETF is responsible for the evolution of the Internet architecture. It takes care of the standardization of the TCP/IP protocol suite used in the Internet. The technical work is divided by topic into several working groups where each group is managed by an Area Director (AD). Work in progress is published as Internet-drafts which are not approved standard documents. An Internet draft is only valid for a limited time. When a specification document is approved as standard, the work is published as an RFC (Request for Comments).

4 *The Object Management Group (OMG)*

OMG is a non-profit organization that promotes the use of object-oriented technologies. Among other things, it defines the CORBA and UML standards. The OMG web site (www.omg.org) provides all of its standards documents available free-of-charge in the form of downloadable PDF files. The OMG focuses on administrative tasks, such as maintaining the OMG web site and organizing meetings of its members [52]. Any organization (or individual) that is interested in the work of the OMG can become a member. Member organizations typically include universities, software vendors and software users. Members can volunteer to take part in task forces that have the goal of defining new OMG standards or enhancing existing OMG standards. It is through this work that the OMG standards evolve in directions directed by the real-world concerns of its members.

2.2.6 Network Management Protocols.

Network management protocols and their respective standard bodies include:

1. Simple Network Management Protocol(SNMP) by IETF
2. Common Management Information Protocol (CMIP) by OSI
3. Common Object Request Broker Architecture(CORBA) by OMG
4. Telecommunication Management Network (TMN) by ITU-T

1) *Simple Network Management Protocol (SNMP)*

The Simple Network Management Protocol (SNMP) is a network management protocol widely used in networks that supports the TCP/IP (Transport Control Protocol/ Internet Protocol) communication stack. SNMP provides a method of managing network hosts from a centrally-located computer running network management software. SNMP performs management services using management systems and agents [53]. SNMP evolved in three versions:

- SNMP Version 1 (SNMPv1)

SNMPv1 is the standard version of the SNMP protocol. It is defined in RFC 1157 and it is a full Internet Engineering Task Force (IETF) standard. Security in SNMPv1 is based on the so-called communities which are just passwords. It reports whether only a device is functioning properly [53]. There are three communities in SNMPv1, read-only, read-write and trap. Read-Only allows reading of data values but cannot modify the data. The Read-Write community allows us to read and also modify the data. Trap allows us to receive traps.

- SNMP Version 2 (SNMPv2)

SNMPv2 was developed to provide the security functions and a remote monitoring (RMON) management information base. The RMON MIB provides continuous feedback without having to be queried by SNMP console [54]. It is defined in RFCs 1905, 1906, and 1907.

- SNMP Version 3 (SNMPv3)

SNMPv3 was developed to provide the best possible security in SNMP management. It is defined in RFCs 2571, 2572, 2573, 2574, and 2575. It provides a framework for the previous versions and future developments in SNMP management with minimum impact on existing systems.

- Protocol Architecture

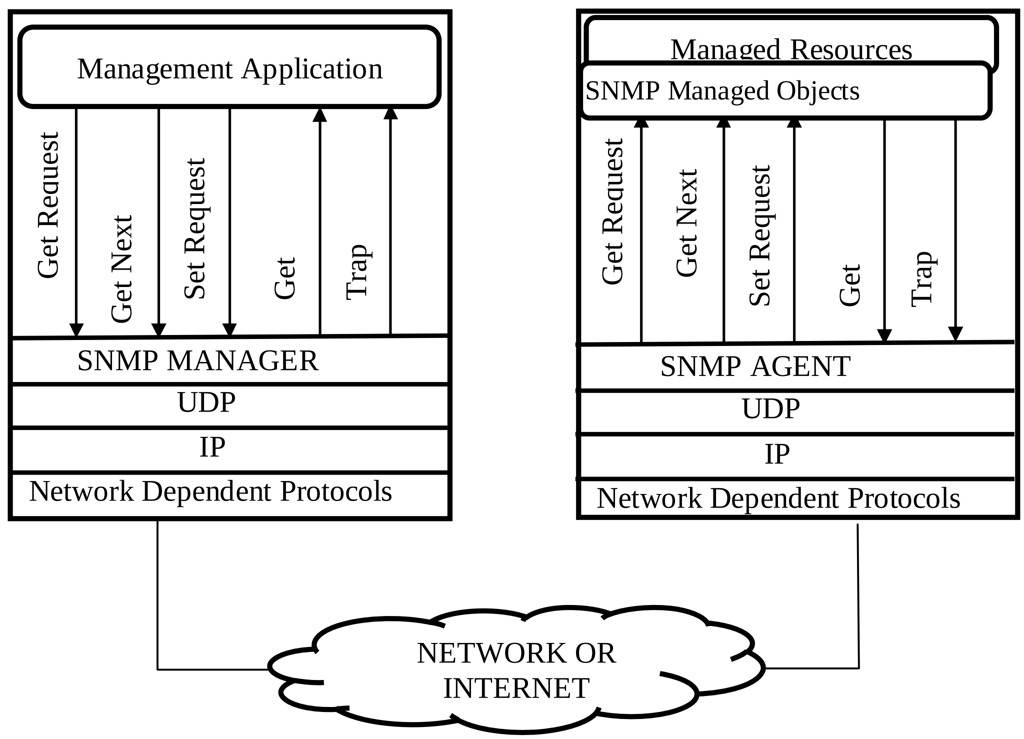


Figure 2.14: SNMP Protocol Architecture

Figure 2.14 shows the protocol architecture of communication between a SNMP manager and agent indicating the layers and the SNMP commands as explained below.

- *Application layer*

This provides services to an end user, such as an operator requesting status information for a port on an Ethernet switch. The SNMP application decides what to do. For instance, the application can send an SNMP request to an agent through the manager, send a response to an SNMP request or send a trap from the agent to manager.

- *UDP*

User Datagram Protocol (UDP) is the connectionless protocol within TCP/IP and corresponds to the transport layer in the OSI model. UDP allows two hosts to communicate with each other. The UDP header contains the destination port of the device to which it is sending the request or trap. The destination port will be either 161 (query) or 162 (trap).

- *IP*

The IP (Internet Protocol) layer delivers the SNMP packet to its intended destination as specified by its IP address.

- *Network Dependent Protocol*

The final event that must occur for an SNMP packet to reach its destination is to be forwarded to the physical network where it can be routed to its final destination. The MAC layer is comprised of the network adapters and their drivers and these place data onto a physical device such as an Ethernet card.

SNMP Network Management is made up of three parts [55]: SNMP Commands, Structure of Management Information (SMI) and Management Information Base (MIB)

- <u>SNMP Commands</u>

SNMP has five protocol data units (PDU) formats commands:

Command	**Description**
Get	A manager to agent command that causes a Get Request PDU to be sent containing a command code, object name, and specification of an MIB variable. The receiving entity responds by sending a Get Response PDU containing values of the variable requested or an error code in the event of an error
Get-Next	A manager to agent command is similar to Get Request except that the request is for values of variables that ñfollowò the ones specified in the PDU. The notation of following is based on a lexicographic order determined by the MIB design. This is specially, useful for traversing tables maintained by the management server
Response	An agent to manager PDU sent in response to a previously neared Get Request PDU. It contains value requested or error codes

Set	This command allows the manager to update values of MIB variable maintained by remote management program and to remotely alter the characteristics of a particular object, which in turn, can affect network operation the format does not violate any security measures that prevent unauthorized updates.
Trap	The PDU is sent from the server to the manager when specific conditions or events have occurred. It allows the manager or to stay abreast of the changes in the operating environments.

- Structure Management Information (SMI)

This is a standard dedicated to specifying a machine independent syntax for every data type. These data types are independent of the data structures and representation techniques unique to particular computer architectures. SMI specifies the syntax for data types such as object identifiers, counters, rows, tables, octet strings, network addresses, and other SNMP elements [40]. Managed Objects are arranged in hierarchy or tree shown below:

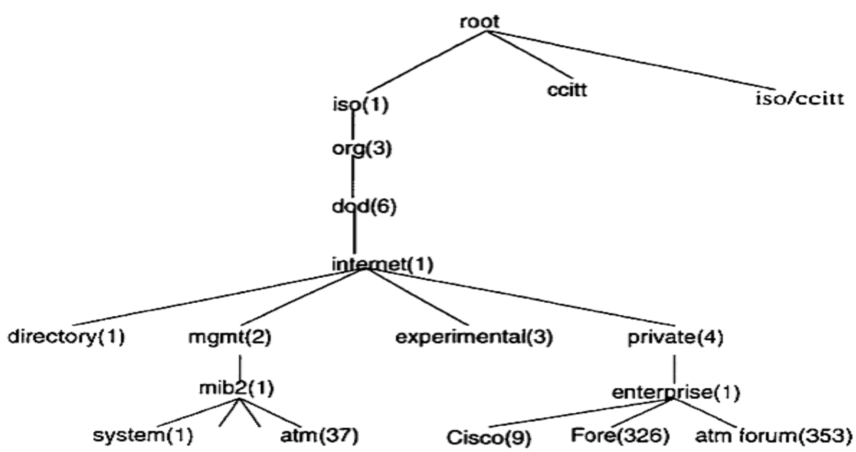


Figure 2.15 Structure of Management Information Object Tree [40]

The node at the top of the tree is called the root, and anything below is called a subtree (or branch). Thus, in the tree of Figure 2.5, iso (1), org (3), dod (6), internet (1), directory (1), mgmt. (2), experimental (3), and private (4) are all subtrees. Where ISO is the International Standards Organization, and DoD is the U.S. Department of Defense which started with the ARPANet. CCITT is the Consultative Committee for

International Telegraph and Telephone. The CCITT has to do with telephony and other communications standards. It is now known as the International Telecommunications Union (ITU), but the CCITT acronym still appears in several standards.

An object identifier is a series of integers based on nodes in the tree, and separated by dots. Thus, iso(1).org(3).dod(6).internet(1) in object identifier form is represented as 1.3.6.1 or in textual form as iso.org.dod.internet. Thus, each MIB object has a numerical object identifier and an associated textual name, much like the association of DNS and IP. The directory (1) subtree is not currently used. The mgmt. (2) subtree defines a standard set of Internet management objects. MIBs are listed below the mgmt. (2) subtree. The experimental (3) subtree is reserved for testing and research purposes. Objects under the private (4) subtree are used by individuals and organizations to define other objects under this subtree.

- Management Information Base (MIB)

An SNMP MIB is a set of parameters which an SNMP management station can query or set in the SNMP agent of a network device such as a router. SNMP contains two standard MIBs. The first, MIB I, established in RFC 1156, was defined to manage the TCP/IP -based internet. MIB II is basically an update to MIB I. The MIBII refers to the current definition. SNMPv2 includes MIBII and adds some new objects. There is MIB extensions for each set of related network entities that can be managed. [40]

2) Common Management Information Protocol (CMIP)

Common management information protocol (CMIP) is a more sophisticated object oriented network management protocol used in OSI networks. It allows any devices to report to the Network Manager when there is a problem. It is more advance and with greater functionality than SNMP that is limited to reporting only network conditions [56]. CMIP is connection-oriented protocol running on top of the seven-layer OSI stack. It relies on both manager- to-agent and manager ï to-manager communications. CMIP is much more secure with MIB allowing use of inheritance in defining managing objects. CMIP is better suited for management of large, complex, multi-vendor enterprise Networks. [57]

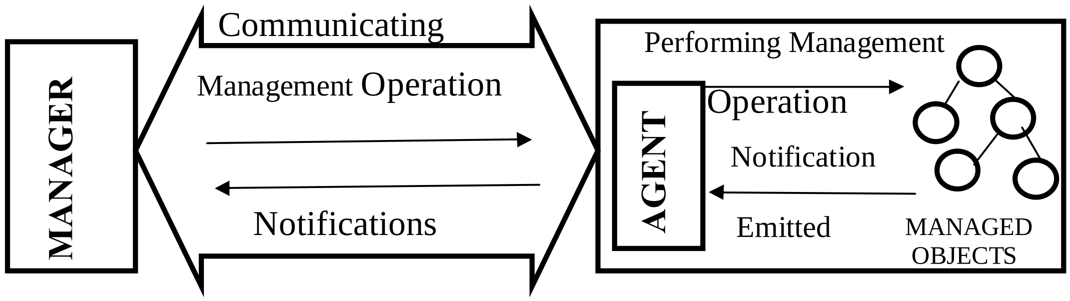


Figure 2.16: CMIP Communication Model [57]

CMIP Agent is that part of a distributed application that manages the managed objects within its local system environment. An agent performs management operations on managed objects as a consequence of management operations communicated from a manager. An agent may also forward notifications emitted by managed objects to a manager. [58]

CMIP Manager is that part of a distributed application which has responsibility for one or more management activities, by issuing management operations and receiving notifications.

CMIP Protocol Architecture

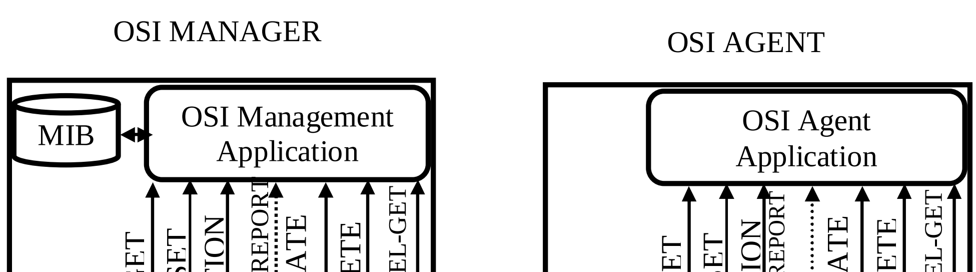


Figure 2.17: CMIP Protocol Architecture

CMIP protocol architecture (figure 2.17) corresponds to the OSI-ISO layers. Network management takes place at layer seven of the OSI reference model. Figure 2.18 shows only the layer seven and its protocol units.

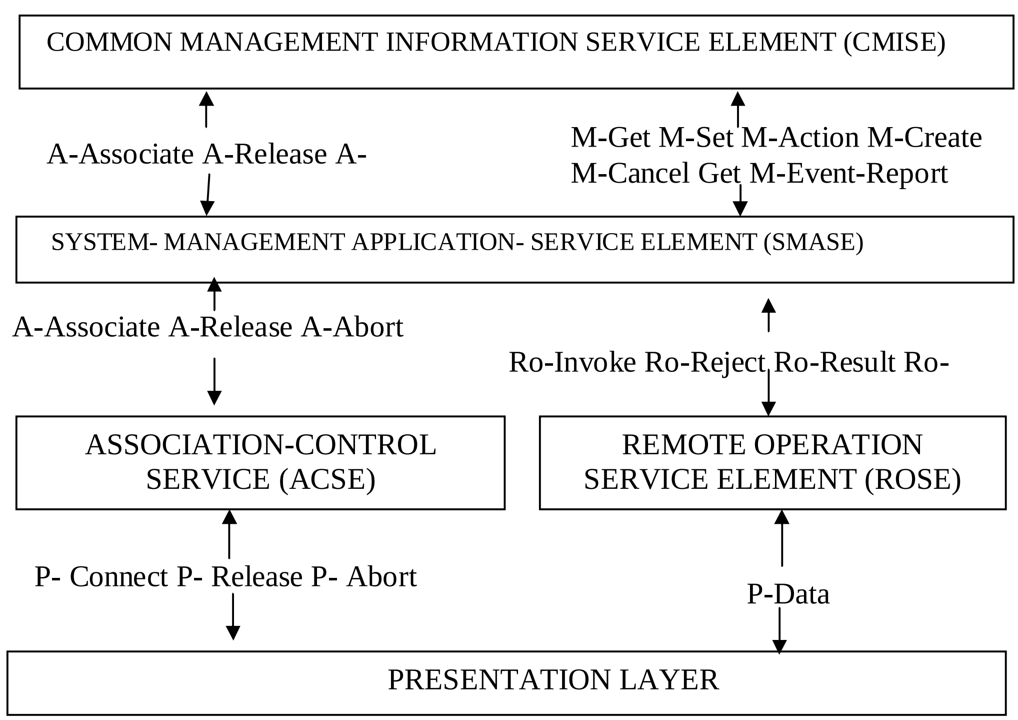


Figure 2.18: CMIP layer seven Protocol units

System Management Application Source Element (SMASE)

It creates and uses the protocol units that are exchanged during the management process. It employs communication services by specific applications service elements (ASEs) by CIMSE

Common Management Information Service Element (CMISE)

It provides management notification services that can be used to report any event about a managed object and management operation services that define the operation required to perform actions on a managed object. Also, provides a frame work for common management procedures that can be invoked from remote locations. It has 3 categories: management association services (MAS), management notification services (MNS) and management operation services (MOS) [59, 60].

TYPE	SERVICE	TYPE	DESCRIPTION
MAS	M-INITIALIZE	Confirmed	Generates connection establishment to peer CMISE users for transferring management function
	M-TERMINATE	Confirmed	Terminates an establish connection between peer CMISE service users
	M-ABORT	Non-Confirmed	Terminates connection between CMISE peer abruptly
	M-CANCEL-GET	Confirmed	Cancel previously requested and currently outstanding invocations
	M-GET	Confirmed	Requests managed object attributes. The request can handle one object or a set of objects
	M-SET	Confirmed/ Non-Confirmed	Set managed object attributes
	M-ACTION	Confirmed/ Non-	Request an action to be performed on a managed object

MOS		Confirmed	
	M-CREATE	Confirmed	Creates an instance of a managed object in agent MIB
	M-DELETE	Confirmed	Deletes an instance of a managed object in the agent MIB
MNS	M-EVENT REPORT	Confirmed/ Non-Confirmed	Reports an event about a managed object to the CMSE manager

Remote Operation Service Element (ROSE)

This is the ISO equivalent of remote procedure call. ROSE allows the invocation of an operation to be performed on a remote system. The Remote Operation protocol contains an invoke identifier for correlating requests and responses, an operation code, and an argument field for parameters specific to the operation. ROSE can only be invoked once an application association has been established. CMIP uses the transaction-oriented services provided by ROSE for all its requests and responses. CMIP also uses the error response facilities provided by ROSE. In synchronous mode, Rose requires the receiver to reply before the originator can invoke another operation. In asynchronous mode ROSE permits the originator to continue invoking operations without waiting for a response [61].

Service overview [62]

SERVICE	TYPE	DESCRIPTION``
RO-INVOKE	Non-Confirmed	Enables an invoking Application Entity to request an operation to be performed by the performing Application Entity.
RO-RESULT	Non-Confirmed	Enables the performing Application Entity to return the positive reply of a successfully performed operation to the invoking Application Entity.

RO-ERROR	Non-Confirmed	Enables the performing Application Entity to return the negative reply of an unsuccessfully performed operation to the invoking Application Entity.
RO-REJECT-U	Non-Confirmed	Enables one Application Entity to reject the request or reply of the other AE if the ROSE-user has detected problem
RO-REJECT-P	Provider-initiated	Enables the ROSE-user to be informed about a problem detected by the ROSE-provider

Association Control Service Element (ACSE) **:** This is used to establish and release associations between application entities. Before any management operations can be performed using CMIP, it is necessary for the two application entities involved to form an association. Either the manager or the agent initiates association establishment. ACSE allows the manager and agent to exchange application entity titles for the purpose of identification and application context names to establish an application context. An application context defines what service elements (for instance, ROSE and CMISE) may be used over the association. After the association is established, ACSE is not used again until the association is released by the manager or agent. It supports the establishment, maintenance and formation of a cooperation relationship between application entities. Below is the description of ACSE services [62].

MODE	SERVICE	TYPE	DESCRIPTION
Connection Oriented	A-ASSOCIATE	Confirmed	causes the start of use of an association by those ASE procedures identified by the value of Application Context Name parameter
	A-RELEASE	Confirmed	Causes the completion of the use of an association by those ASE procedures identified by the application context that is in effect without loss of information in transit (in an orderly manner).

	A-ABORT	Non-Confirmed	Causes the abnormal release of the association with the possible loss of information in transit. It is done abruptly.
	A-P-ABORT	Provider Initiated	Indicates the abnormal release of the association as a result of action by the underlying presentation-service with the possible loss of information in transit.
Connectionless	A-UNIT-DATA	Non-Confirmed	Simultaneously establishes and releases an association.

- **SNMP AND CMIP Comparison**

SNMP and CMIP are the most commonly used management protocols. Below is the comparison of the two protocols [63, 64].

	SNMP	**CMIP**
AGENT INTELLIGENCE	Simple	Complex and powerful
ENVIROMENT	TCP/IP	OSI
MANAGER INTELLIGENCE	Polling ï Based	Event-Based
BANDWIDH REQUIREMENT	Excessive polling can result in high bandwidth requirement	Larger message can result high bandwidth consumption
CODE SIZE	Small	Fairly large
SCALABILITY	Polling requires careful tuning of the network.	Event driven creates a more scalable solution for large reliable network.
SECURITY	Secure SNMPV2 offers authentication and access control, including alarm reporting.	CMIP offers security as well as audit trial service.
PDU LIMITATION	484 octets	Unlimited

NAMING	Naming requires more information to make it globally unique	Uses X.500 naming to facilitate manager to manager distribution
DATA RETRIVAL	Simple reads and writes	Structure of query
COMMUNICATIONS	Connection less datagram using UDP/IP; places burden on the manager for recovery.	Connection oriented upper layers using OSI service layer stack
PERSPECIVE ON DATA	Flat file	Object oriented
MODE OF OPERATION	Unconfirmed	Confirmed
REDUNDANCY OF MANAGEMENT	Agent may send traps to multiple managers	Management services can be distributed to multiple destination
REPRESENTATION	ASN1	Object oriented
DATA SYNCHRONISATION	One row at a time	Scoped get provides agent synchronization of data.

3. Common Object Request Broker Architecture (CORBA)

This is a complementary technology that offers powerful mechanism for the development of distributed management application without necessarily over-lapping the already existing standards such as CMIP and SNMP [65]. It provides a computing environment to support multiple collaborating managers. It borrows the concept of a ñsoftware object busò from the software engineering community, with a particular application to the inter-operability of disparate managers of networking equipment. CORBA standard is made up of an interface definition language (IDL) to define the external behaviour of managers, specifications for building manager ïto- manager request dynamically and an interface repository which contains descriptions of all manager interfaces in use in a given system [66].

Some advantages [67]:

1. It is vendor-neutral and open standard, portable, wide variety of implementations, hardware platforms, operating systems, languages
2. It takes the grunt work out of distributed programming

Some disadvantages:

1. It has no reference implementation

2. It is specified by consensus and compromise
3. It is not perfect

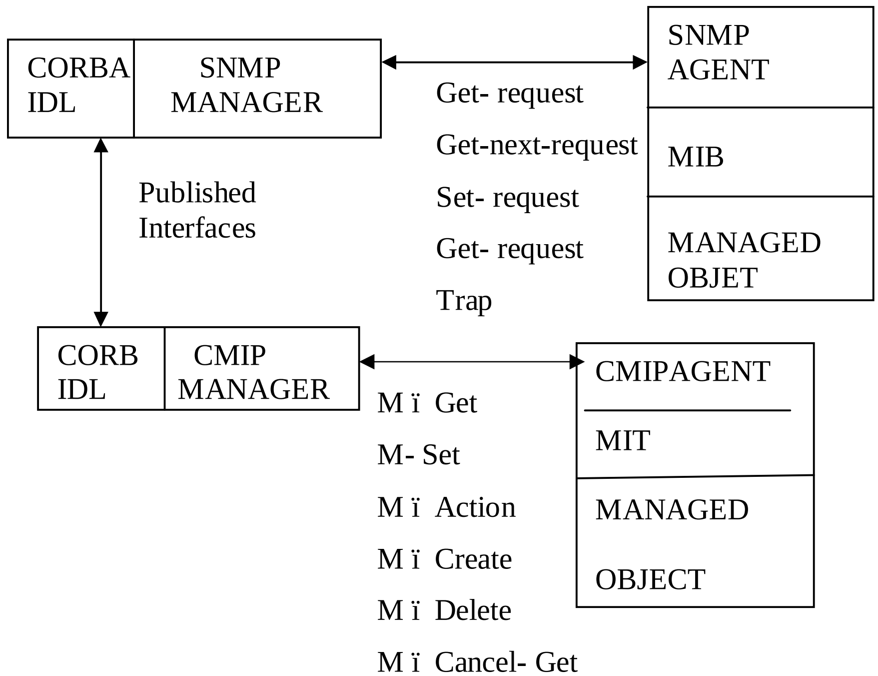


Figure 2.19: SNMP, CMIP and CORBA Generic Architecture

The figure 2.19 shows the primitive commands between an SNMP manager and an SNMP agent, Primitive command between CMIP manage and CMIP agent and Communication between SNMP and CMIP managers in CORBA IDL.SNMP CMIP manager to agent primitives are predefined, but CORBA manager-to- manager communications are dynamically defined and published or anyone who wishes to use them[68].

4. Telecommunication Network Management (TMN)

The ITU has developed a network management architecture called Telecommunication Management Network (TMN) that is useful in managing large, complex, multivendor networks. Most telecommunications vendors conform to the TMN specifications, making it possible for an operator to easily integrate equipment purchased from various vendors into a network with unified network management [69]. TMN has 3 functional units [70]:

1) *Operations Systems Function (OSF)*

The OSF processes information related to the telecommunications management for the purpose of monitoring/coordinating and/or controlling telecommunications functions including management functions that is the TMN itself. This is actual TMN functionality.

2) *Network Element Function (NEF)*

The NEF is a functional block which communicates with the TMN for the purpose of being monitored and/or controlled. The NEF provides the telecommunication and support functions which are required by the telecommunications network being managed. The NEF includes the telecommunications functions which are the subject of management. These functions are not part of the TMN but represented to the TMN by the NEF. The part of the NEF that provides this representation in support of the TMN is part of the TMN itself, whilst the telecommunications functions themselves are outside.

3) *Work Station Function (WSF)*

The WSF provides the means to interpret TMN information for the management information user. The WSF includes support for interfacing to a human user. Such aspects of support are not considered to be part of the TMN and thus this part of the WSF is shown outside the TMN boundary.

2.3 NETWORK PERFORMANCE MANAGEMENT

Performance Management includes the task of determining whether a system's behaviour is meeting a particular target. In applying this to networks we need to know if a network is underutilised or over burdened by traffic load; whether unusual effects are taking place that might affect user traffic; or if operation is satisfactory [71] When looking at performance management systems, the administrator looks for the following traits: Utilization and error rates, Performance data collection, Consistent performance level, Performance data analysis, Problem reporting, Capacity planning, Performance report generation and Maintaining and examining historical logs

2.3.1 Performance Management Steps

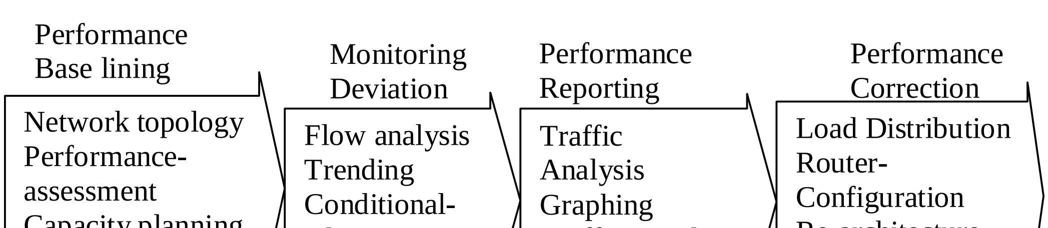


Figure 2.20: Performance Management Steps

Performance Base lining

Base lining involves truly understanding your network performance. Knowing what you consider good performance gives you the quantitative metrics to justify or invalidate usersô complaints of the network. There are three major components of performance base-lining: Documenting your network topology and the components that make up that topology, completing a performance assessment of the critical applications you want to bring under management, and the use of both of these tools for understanding and planning for capacity needs [71].

Monitoring Deviation

It involves configuration of NMS tool to watch out for changes in the network performance after understanding the nominal performance of your network. This performance monitoring is often done through the use of network probes (hardware devices are installed in-line with devices). These agents or devices report back to the NMS on the traffic characteristics going through the probe. While installing the probes the administrator should ensure that it will not affect the network traffic flow. A good NMS should be able to keep records of all data characteristics and alerting in a searchable .Some examples of interesting characteristics are:

Input/output bits/second, Current/average response time, Peak traffic load, Interface errors/discards, Per cent packet loss etc.

Performance Reporting:

NMS must have a robust reporting engine that can align statistics with the network map and across multiple devices.

Performance Correcting

This involves using the information given to you by the NMS, the graphs and trending analysis done in concert with the data in your NMS, and your own network intuition to determine that a change is necessary to bring the network back to nominal performance [72]. That change can take a number of forms. Adding extra interfaces to key network devices reduces the load and increase performance. Depending on the type of device and load balancing capabilities, performance can increase linearly with the number of additional interfaces added to the problem.

2.3.2 Network performance (NP)

Network performance can be defined as the ability of a network or network portion to provide functions related to communication between users [73]. It is a measure of how well a system works. Network performance is measured in terms of parameters which are meaningful to the network provider and are used for the purposes of system design, configuration, operation and maintenance. NP is defined independently of terminal performance and user actions [74]. Network performance information falls into two categories: [69]

- *Service – oriented (user-oriented):* items such as availability response time and accuracy- parameters that are important to the users.
- *Efficiency – oriented (provider-oriented):* items such as throughput and utilization-parameters that are important to the network owners.

NP is divided into the categories [39]

- *Traffic performance:* This shows how effective the network is in sending data packets. Examples of such parameters are throughput, number of discarded, errored and lost cells. This information helps the operator to discover bottlenecks and tune the network for better performance.
- *Signalling performance:* It shows how effective the network elements are ñcommunicatingò with each other, e.g. during the connection establishment.

2.3.3 Network Performance Parameters

NP parameters are used for the purpose of [39]:

- *Analysing network performance:* They help the operator to reach optimal resource utilization and cost effective operation and maintenance of the network.

- *Strategic network growth planning:* NP statistics are important when operators plan for network expansion or upgrade.
- *Preventive handling:* Good preventive handling minimizes downtime in the network.

NP parameters should have the following characteristics [39]:

- Independent from the end-user equipment, thus equipment used to connect services to the network is not of interest.

- Measurability at boundaries of network elements.
- Should have a clear relation to the technical architecture of the network and individual network elements.

Generic Network Performance /Quality of Service parameters

Network Performances are measured by the following metrics [74]:

- *Throughput:* Effective rate of transfer of messages across the network.
- *Response time:* Time between generating and satisfying a request associated with the measure are those times that have to do with setting up, usage and tearing down delay, connection establishment delay, transit delay and connection release delay.
- *Waiting time:* Time spent in queues waiting for service, time spent in processing and forwarding messages and time between arrival events.
- *Work load:* The number of managed objects idle, number of managed objects active, number of managed objects busy and number of managed objects rejecting service requests because of over load.
- *Statistical analysis*: Analysis of event records to determine quantities such as utilization, availability, error rate, mean-time failure, mean-time to repair etc.

ATM performance parameters

Cell Error Ratio (CER) is the ratio of total errored cells to the total of successfully transferred cells, plus tagged cells, plus errored cells in a population of interest.

Successfully transferred cells, tagged cells, and errored cells contained in severely errored cell blocks are not included [75].

Cell Loss Ratio (CLR) is the ratio of total lost cells to total transmitted cells in a population of interest. Lost cells and transmitted cells in severely errored cell blocks are excluded from the calculation of cell loss ratio.

Cell Misinsertion Rate (CMR) is the total number of misinserted cells observed in a specified time interval divided by the time interval duration1 (equivalently, the number of misinserted cells per connection second). Misinserted cells and time intervals associated with severely errored cell blocks are not included.

Severely Errored Cell Block Ratio (SECBR) is the ratio of total severely errored cell blocks to totalcell blocks in a population of interest.

Cell Transfer Delay (CTD) is the delay experienced by a cell between network entry and exit points. It includes propagation delays, queuing delays at various intermediate switches and service time at queuing points.

a) *Mean Cell Transfer Delay* is the arithmetic average of a specified number of cell transfer delays.

b) *Cell Delay Variation (CDV)* is a measure of variance of cell transfer delay. High variation implies lager buffering for delay ï sensitive traffic such as video and video conferencing.

   - *1-point CDV* describes the variations of cell arrivals in one MP. Network queues and buffering procedures between the source and the MP affect the value.
   - *2-point CDV* is based on observation of cell arrivals at two MPs that delimit a virtual connection portion. It gives e.g. indication of queues within the connection portion

2.3.4 Quality of Service (QoS)

It measures performance across an internetwork. It can measure availability, capacity, utilization delay, delay variation, throughput, reachability response time, errors, and the burstiness of traffic.

ATM Quality of Service Parameters

Here are some important traffic parameters for bandwidth requirements in an ATM network [76, 77]:

a) *Peak Cell Rate (PCR):* Maximum bandwidth the connection is allowed to generate.

b) *Sustainable Cell Rate (SCR):* Average traffic bandwidth the connection is allowed to generate.

c) *Minimum Cell Rate (MCR):* Demands on minimum available bandwidth for the connection.

d) *Maximum burst size (MBS):* Maximum allowed traffic burst size, when bandwidth is PCR.

QoS parameters for requirements on delay in an ATM network [78]:

a) *Maximum Cell Transfer Delay (max CTD*)**:** Maximum allowed difference between reception and transmission time for a cell between two end-user points.

b) *Peak-to-peak Cell Delay Variation (peak-to-peak CDV):* Maximum allowed difference between the maxCTD and minCTD for a cell between two end-user points. The minCTD represents

2.4 RELATED WORKS

2.4.1 Performance monitoring model

Performance monitoring model in [79], the author proposes a general model for performance management in ATM networks based on interaction between management and control functions. The paper discusses the functionality of the Network Management System, the plane & layer management in switching systems, the call control functions and that of QoS management from the perspective of a service platform. The paper then goes on to define performance monitoring in ATM networks and illustrates the use of OAM cells for in-service performance measurements. Overall the paper brings out a number of issues and highlights the problems.

2.4.2 CMIP based interface for Optical Access Network

In [80] the authors introduced the standard CMIP-based management interface for Optical Access Network (OAN), heterogeneous OAN devices from different suppliers can be managed in a unified way. The paper discussed the CMIP based management interface for OAN. It described the components of CMIP-based management interface for OAN and then introduces a prototype implementation for the CMIP based management interface.

2.4.3 A software architecture for supporting CMIP management information bases of ATM switches.

[81] Introduced software architecture for supporting CMIP management information bases of ATM switches. The architecture has three logical levels with specific functionality and data. It is able to support ATM switches with management capabilities conforming to existing standards, and is suitable for implementation. The architecture provided a basis for the development, evaluation and evolution of software supporting CMIP management information bases of ATM switches.

2.4.4 Bandwidth allocation for evaluating traffic congestion

Hui [82] outlined methodologies for computing the probability of packet, burst, and call blocking to evaluate congestion for integrated traffic. A bandwidth allocation mechanism is allocated to traffic states (packets, burst, and call) to improve network efficiency. The system model follows a 3-step algorithm: Request, Acknowledge and Send. The scheme allocates a subset of resources at level $l + 1$, and guarantees the allocation does not cause excessive blocking at level $l - 1$ within the assigned subset. The trunk is partitioned into channels i, each with capacity C_i, calls are placed into the channel i such that the maximum blocking probability among i is minimized. Blocking probability at the burst level provides better traffic control.

Model

The system model follows a 3-step algorithm. At level l, the scheme allocates a subnet of resources allocated at level $l+1$, and guarantees the allocation would not cause excessive blocking at level $l - 1$ within the assigned subnet.

Blocking probability at packet level:

Given the service rate q, the arrival rate λ, the queue length distribution P_l, average queue length L, buffer overflow, and the blocking probability,

$$P_0 = 1- \lambda/q; \; P_{l>0} = \lambda/q \, (1-\omega)\,\omega^{l-1}; \; \omega = \frac{\lambda(q-1)}{q(\lambda-1)} \; ; \; L = \frac{\lambda(1-\lambda)}{q-\lambda}$$

$$P_B < P\,(L> |B|) = \sum_{T=/B/+1}^{\infty} P_l = \frac{\lambda}{q}\,\omega^{|B|} \qquad (2.1)$$

Blocking probability at burst level: (Provides better traffic control)

The blocking probability for type i pulses for the lossy system is given by

$$P(WN(t) > Z\text{-}a_i) = \frac{1}{1-[(w(t)>Z}\,(\,P\,(W\,(t)> Z\text{-}a_i\,)\text{-}\,P(W(t)\text{-}\,Z)) \quad (2.2)$$

W'(t) = carried traffic, *W(t)* = offered traffic, a_i = amplitudes (jumps), Z = total bandwidth.

The trunk is partitioned into channels i, $1 \le i \le m$, each with capacity C_i, f_j *callls* for various j are placed into channels i, such that the maximum burst blocking probability among the i is minimized.

2.4.5 Admission control using the minimal effective bandwidth

Cheng and Zhuang [83] investigated the statistical multiplexing and admission control for a partitioned buffer, where the traffic is generated by multiclass markov-modulated fluid sources. They demonstrated that the minimal effective bandwidth can be used for admission control when traffic from heterogeneous markov-modulated sources enters the partitioned buffer; while it is required to dynamically adjust buffer partition vector according to the accepted traffic load in other to guarantee Q_OS.

Model

The system model considered a portioned buffer of size, B, served by a channel of constant capacity; c. the input traffic is from a markov-modulated flow source with *J* classes of traffic $(J \geq 2)$. The QoS Requirement is specified by packet loss.

The admission policy is based upon a space reservation scheme, using the buffer partitioning vector Bt = (B_1, B_2,é , B_{j-1}) to provide *J* loss priorities. The QoS is satisfied for all traffic if

$$G(B_J) \leq \varepsilon_j, \forall \in \{1,2,....,J\} \tag{2.3}$$

Where $\mathcal{E}_1 > \mathcal{E}_2 > ... > \mathcal{E}_J > 0$, $G(B_j)$ = long run probability that buffer above(B_j).
B_j = threshold, $_j$ = packet loss probability

The asymptotic solution of the fluid model analysis is given by

$$G(B_j) \approx G(0)\prod_{r-1}^{j} \exp[Z_1^r(B_r - B_{r-1)})] \tag{2.4}$$

Where, Z_l^r = eigen value, B_r = buffer class *r* fluid

$$G(B^{J\,)} \approx L\prod_{R=1}^{J} \exp[Z_1^r\left(B_r - B_{R-1}\ \right)] \tag{2.5}$$

Where, L= loss probability in the bufferless multiplexing system. This equation can be used directly for admission control in a partitioned buffer.

For a two-class on-off source:

$$\begin{aligned} G(B_1) &= 1 - [\pi_0(B_1) + \pi_1(B_1)] = G(0)\exp(\ Z_1^1 B_1) \\ G(B) &= 1 - [\pi_0(B) + \pi_1(B)] \\ G(B) &= G(0)\exp(\ Z_1^1 B_1)\exp[\ Z_1^2(B - B_1) \end{aligned} \tag{2.6}$$

Where,

$$G(0) = \frac{\lambda^2}{c}\frac{\alpha}{\alpha+\beta}\frac{c - (\lambda^2 + \lambda^1)_{\frac{\alpha}{\alpha+\beta}}}{c - (\lambda^2 + \lambda^1 e^{Z_1^1 B_1})_{\frac{\alpha}{\alpha+\beta}}} \tag{2.7}$$

c= Channel capacity, α = silence duration, β = talk spurt duration, λ= fluid rate

The $Q_O S$ satisfaction requires that $c \geq \max\{c_{1,} c_{2\ldots,} c_j\}$

Optimal buffer partitioning involves solving the equation

$$\sum_{j=1}^{J} \frac{\ln \frac{\varepsilon_j}{\varepsilon_j - 1}}{Z_1^j (c^*)} - B = 0 \tag{2.8}$$

Where c^* = minimum effective bandwidth of the markov modulated source. c^* can be solved using Newton iterative technique.

Numerical analysis of the model shows that in a heterogeneous multiplexing situation, to guarantee the $Q_O S$ of admitted traffic, the buffer partitioning vector should be optimized dynamically in response to the traffic variation and if the input peak rate of traffic decreases below the channel capacity, the minimal effective bandwidth can be used for admission control.

2.4.6 Dynamic algorithm for resource allocation

Bashandy, Chong and Ghafoor [84] presented a dynamic programming algorithm to find an optimal path between the source and destination nodes and determining the amount of resources along the intermediate nodes needed to satisfy the QoS requirements. They also analyzed various rate-based service disciplines and used the dynamic algorithm to solve the problem of QoS routing with resource allocation for networks that employ the service schemes. The system model used the graph theoretical model which is based on the concepts of jitter graph. A jitter graph consists of jitter nodes (switches, routers) and jitter links (service disciplines at output interface). It uses optimization procedures to allocate resources.

Model

The system model used graph theoretical model which is based on the concept of jitter graph. A jitter graph consists of jitter nodes *v* (processors and connectors in switches, routers, and computers) and jitter links, *E* (service disciplines at output interfaces and the physical communication lines).

The reliability of a jitter link *(u,v),* Q_{uv} is

$$\eta_{rec} / \eta_{tran} \geq Q_{uv} \tag{2.10}$$

η_{tran} = total number of packets transmitted by jitter node u to ward jitter node v,

η_{rec} = total number of packets received at the jitter node v,

Q_{uv} is affected only by data dropage, two resources were identified: buffer allocated $b(u,v)$ and bandwidth allocated $r(u,v)$. The above resources are restricted by the maximum value imposed by hardware and/or software limitation of a node.

Jitter, reliability, and end-to-end delay are considered as functions of the resources and traffic shape

$$\begin{aligned} 0 < J_{uv} &= f_{J_{uv}}(b(u,v), r(u,v)) < \infty \\ 0 \leq Q_{uv} &= f_{Q_{uv}}(b(u,v), r(u,v)) \leq 1 \\ 0 < D_{uv} &= f_{D_{uv}}(b(u,v), r(u,v)) < \infty \end{aligned} \tag{2.11}$$

For a given path, $P = <V_0\ldots, V_n>$, the jitter $J_p(P)$, the reliability $Q_p(P)$, the maximum delay $D_p(P)$, the bandwidth $r_p\ (P)$ are a function corresponding to the amount of resources allocated along the path.

$$\begin{aligned} J_P(P) &= f_J(b(V_0,V_1), r(V_0,V_1), \ldots, b(V_{n-1},V_n)) \\ Q_P(P) &= f_Q(b(V_0,V_1), r(V_0,V_1), \ldots, b(V_{n-1},V_n)) \\ D_P(P) &= f_D(b(V_0,V_1), r(V_0,V_1), \ldots, b(V_{n-1},V_n)) \\ r_P(P) &= f_R(b(V_0,V_1), r(V_0,V_1), \ldots, b(V_{n-1},V_n)) \end{aligned} \tag{2.12}$$

A Path p is said to satisfy the Q_OS requirement of the stream if,

$$\begin{aligned} J_P(P) &\leq J_{req} \\ Q_P(P) &\geq Q_{req} \\ D_P(P) &\leq D_{req} \\ r_P(P) &\geq R_{req} \end{aligned} \tag{2.13}$$

$$r_P(P) = \min_{(u,v)\in P} r(u,v)$$

The logarithm reliability parameter $Z_P(P)$ for a path P is given by

$$Z_P(P) = -\ln[Q_P(P)] \tag{2.14}$$

Hence a path p satisfies the reliability requirement Q_{req} if $Z_P(P) \leq Z_{req}$, where

$$Z_{req} = -\ln(Q_{req}) \tag{2.15}$$

The path resource problem is defined as

$$Z_P^*(P_j) = \min\{Z_P(P_j)\}$$
$$J_P(P) \le J_{req} \tag{2.16}$$

Subject to
$$0 \le b(u,v) \le B(u,v) \forall (u,v) \in P_j$$
$$R_{req} \le r(u,v) \le C_{uv}^{\max} \forall (u,v) \in P_j \tag{2.17}$$

The probability of $Q_O S$ routing with resource allocation is defined as follows:

$$\zeta^*(s,d) = \min_{P_j \in P(s,d)} \{Z_P^*(P_j)\} \tag{2.18}$$

The dynamic algorithm to solve the equation above is defined by the recursive relation

$$Z^{K+1}(s,x) = \min\{Z^K(s,x), \min_{w \in adj^{-1}(x)} \{Z_P^*(P^K(s,w) \oplus (w,x))\}\} \tag{2.19}$$

Where,

$P^K(s,x)$ is the path computed at the k^{th} iteration $Z^K(s,x) = Z_P^*(P^K(s,x))$

2.5 CONCLUSION

This chapter has presented a general overview ATM network; overview of network management was presented. Network performance management including steps, generic network performance parameters, ATM performance parameters and quality of service parameters was presented.

Finally, a review of related works was done. Although all the classes of techniques resource allocation techniques presented above are flexible as they ensure fairness while allocating resources. They also allocate priority to flows and the delay bounds can be maintained or kept within manageable limits. This work will look at the strength of CMIP as a more sophisticated protocol in ATM network bandwidth allocation.

In the next chapter the implementation of the CMIP protocol will be represented in block diagram and used to implement ATM Network bandwidth allocation.

CHAPTER THREE

PROCESS MODELLING

3.0 INTRODUCTION

This chapter presents the implementation of the CMIP on ATM network bandwidth allocation. The manager communicates with an agent using a CMIP protocol as shown in the previous chapter. The process (communication between managed objects, agents and manager) will be represented with a flow chart showing the stages involved in ATM bandwidth allocation.

3.1 CMIP OPERATION

The flow chart of operation presented in figure 3.1 shows the main stages involved in bandwidth allocation, namely: Start, Initialization process, scanning / waiting for request for bandwidth and Resource allocation. These stages are activated when request for bandwidth allocation is received.

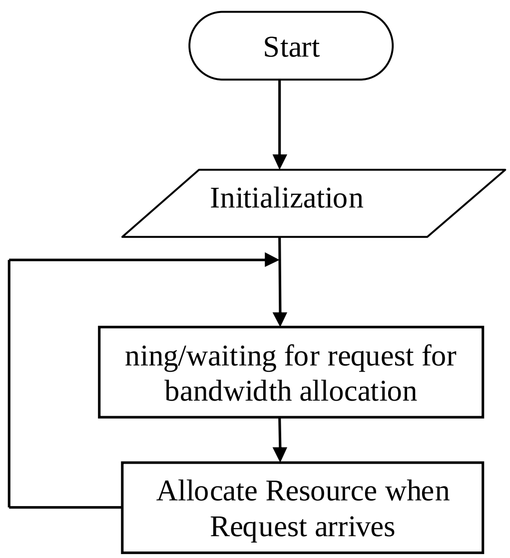


Figure.3.1: CMIP operation

3.1.1. Start

The start involves the putting on of network management system, system booting and setting up of the connection between manger and the agent. When the system is fully on, it goes to the next stage which is initialization process.

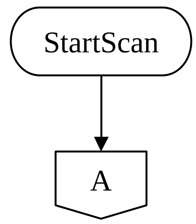


Figure 3.2 CMIP Start Operations

3.1.2. Initialization

Initialization process provides for the configuration and population of the MIB with the state of the system to be managed. The initialization process involves three phases: create, set and delete managed objects, see figure 3.2. The manager employs M-create, M-set and M-delete in the initialization process.

- **Create:**

At the create phase, the manager creates the required managed object (MO). The manager uses M-Create command to query the MIB to create an instance of a managed object in the MIB. After the creation of the managed object, the manger sets the attribute of the managed object using M-Set command. If there is need to create more managed objects the manager loops back to create managed objects, it continues in the loop until there is no need to create more managed object . If there is no need to create managed object, the manager now goes to the next phase to modify the existing managed objects.

- **Modify:**

This phase allows only change/modification of the managed objectôs attribute. If there is no need for MO modification, the system takes the manager into the last stage- M-delete. The manager uses the M-get command to fetch the Managed Object from the

MIB and M-set command to perform modification (to change the value of attribute). If there is need to modify another managed objects the manager loops back to get managed object then goes down to set (modify) the managed object, it continues in the loop until there is no need to modify any other managed object . The manager now goes to the next phase to delete managed objects.

- **Delete:**

  This phase deletes the managed object from the MIB. This is last phase of the initialization process. This phase starts by asking if the manager wishes to delete already created managed objects if the answer is ñNOò, it goes to the next stage of CMIP management process (scanning and waiting for request) else it gets the managed object to be deleted. The manager uses the M-get command to fetch the Managed Object and then asks to confirm deletion. If confirmed, it deletes the appropriate MO using M-delete else it cancels get using M-cancel-get command and goes to next stage of CMIP management process (scanning and waiting for request). If the manager still wishes to delete another MO the manager loops back to get managed object then goes to delete the managed object, it continues in the loop until there is no need to delete any other managed object. Then the manager now goes to the next stage of CMIP management process (scanning and waiting for request).The flow chart on Figure 3.3 below shows the initialization stage of CMIP operation.

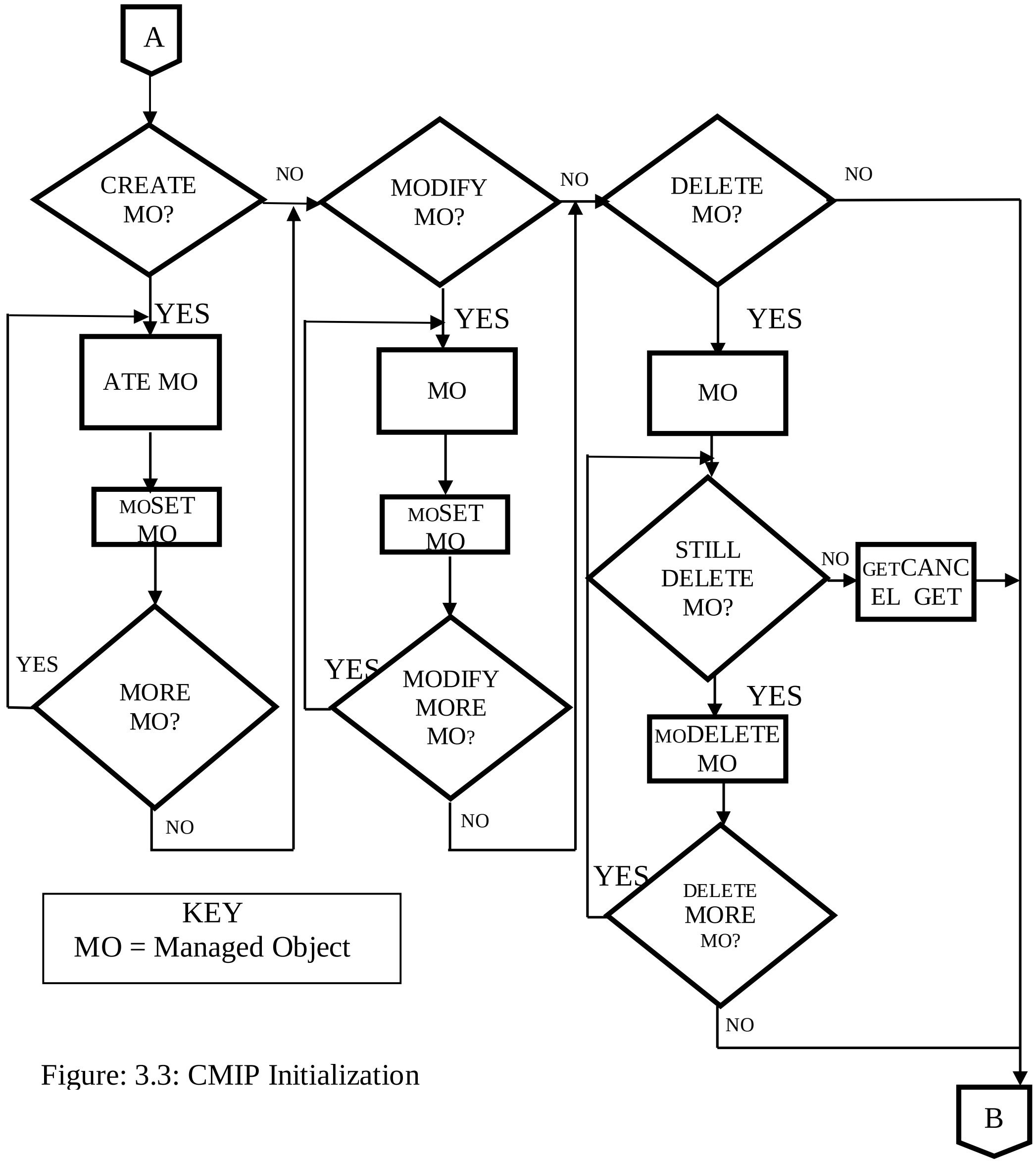


Figure: 3.3: CMIP Initialization

3.2.3 Scanning/Waiting for Request for Bandwidth

In this stage the manager is in a scanning state, it waits for bandwidth allocation request. It continues in the loop until an allocation request comes in, it then goes to allocate bandwidth to the request. Figure 3.4 shows the flow chart of CMIP Scanning/waiting stage where the manager waits for request for bandwidth allocation.

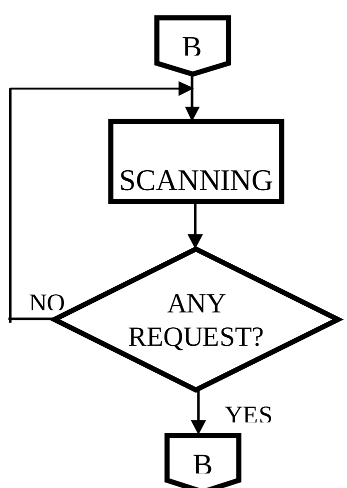


Figure 3.4: CMIP Scanning/waiting for request for bandwidth

3.2.4 Resource Allocation

Once a request comes in, the manager checks the service type and determines the requested bandwidth. Therefore, in the case of either data, voice or video service the Q_oS parameter value is applied in determining the appropriate required bandwidth. If it is outside the defined services error is flagged off. It then defines the Required Bandwidth using the associated Q_oS parameters .Therefore using the Q_oS parameter value relating to the service of the Requested Bandwidth the Optimum Required Bandwidth (ORB) is calculated using equation 3.9. Equation 3.9 was derived from the graph in figure 3.5. Equation 3.9 is the power series conversion of the graph in figure 3.5. The graph was developed in earlier work [85]. Given a specific required bandwidth, the graph is used to determine the optimum required bandwidth. Figure 3.4 therefore illustrates the relationship between ATM networks, optimum required bandwidth and standard (typical) bandwidth requested by network user. the standard bandwidth requirements relate to ATM network traffic intensity. The resultant series is employed in calculating the optimum required bandwidth for each bandwidth request to reduce waste associated with redundancy in bandwidth.

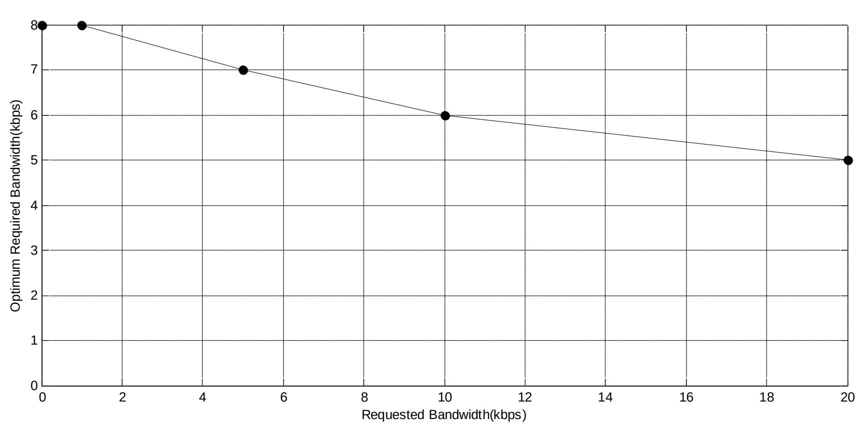


Figure 3.5: Number of resources versus bandwidth [85]

The power series that resulted from graph in figure 3.4 above were derived below.

So, Power series has the form [86]:

$$y = Ax^0 + Bx^1 + Cx^2 + Dx^3 + \ldots\ldots. \tag{3.1}$$

Basically, the constants define the series. The task of determining the constants when a curve is given is actually not included in the scope of this work. This not withstanding, the process that may be adopted for the determination of the constants is presented below

Where A, B, C, D are constants

From figure 3.5 above, equations (3.2) was obtained by substituting choice points on the curve in equation (3.1).

$$\begin{aligned} 8 &= A + B + C + D \\ 7 &= A + 5B + 25C + 125D \\ 6 &= A + 10B + 100C + 1000D \\ 5 &= A + 20B + 400C + 8000D \end{aligned} \tag{3.2}$$

Then solving equation 3.2 simultaneously, for the four unknown constants - A, B, C and D ï and substituting back into equation 3.1 then equation 3.3 results.

$$y = 8.275 - 0.28x + 0.0046x^2 + 0.0001x^3 \tag{3.3}$$

In this case, y represents the Optimum Required Bandwidth, ORB and x represents the requested bandwidth, B. so equation 3.3 can be rewritten as in equation (3.4) below.

$$ORB = 8.275 - 0.28B + 0.005B^2 - 5.848 \times 10^{-5} B^3 \tag{3.4}$$

Therefore equation 3.4 is used to calculate the number of the ORB by substituting the value of requested bandwidth for each arrival. After which the manager compares the Available Bandwidth (AB) in the MIB and the ORB for the bandwidth request, if the ORB is greater than the Available Bandwidth (AB) it means there is no enough bandwidth so it flags an error and drops the call and goes back to wait for another request. But if the Optimum Required Bandwidth (ORB) is less than or equal to the Available Bandwidth (AB) it means there is enough bandwidth for the request it will then decrement Available Bandwidth (AB) by the size of Optimum Required Bandwidth (ORB) that is ñAB - ORBò and then gets the resource and issues a command to agent to Connect Call and goes back to wait for another request. The flow chart on figure 3.5 shows the CMIP resources allocation stage.

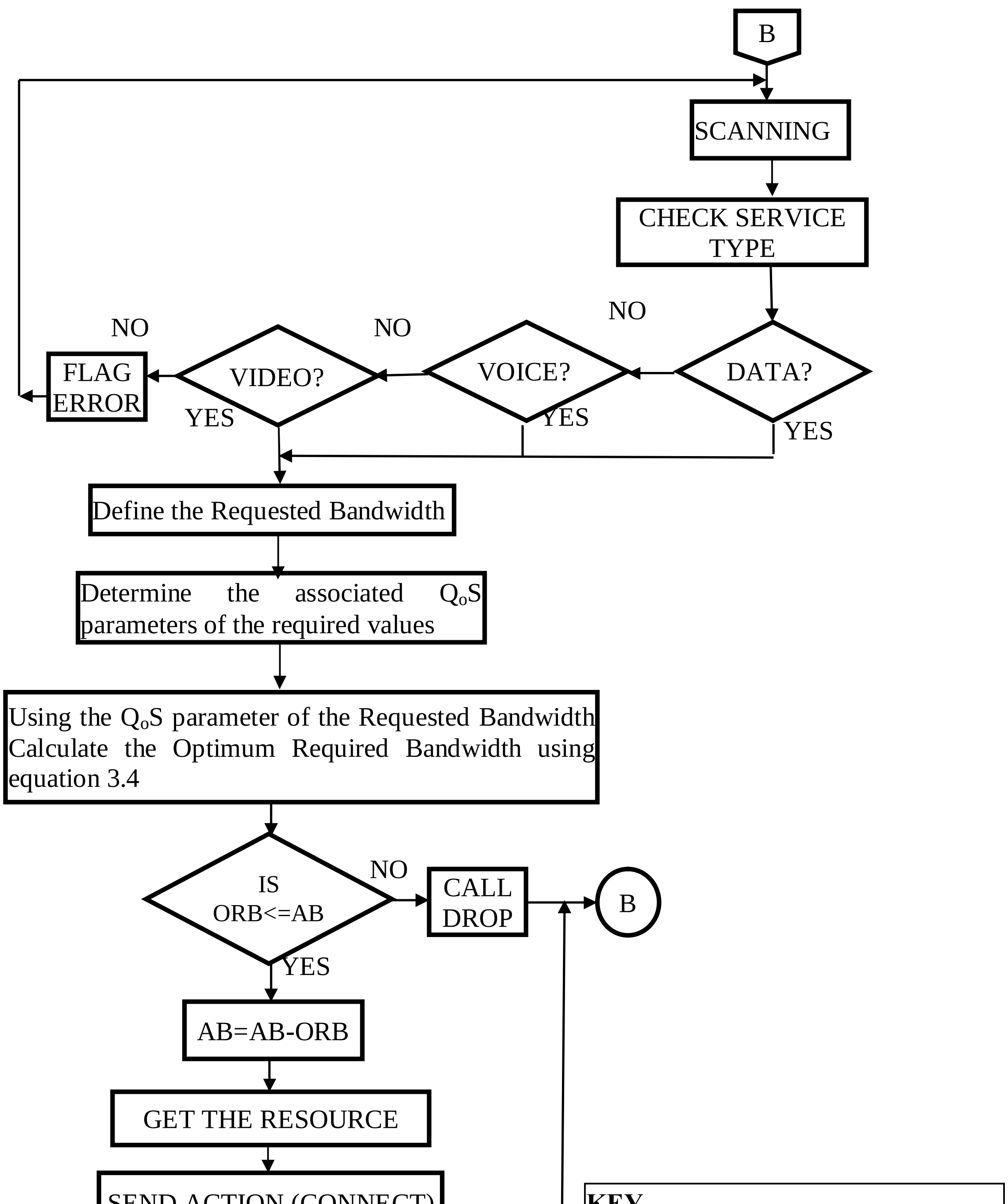


Figure 3.5 CMIP Resources Allocation

3.3 CONCLUSION

This chapter explained CMIP operation as it concerns ATM bandwidth allocation using a flow chart. It shows the diagrams of different stages in CMIP flow chart of operation for ATM bandwidth allocation. Complete flow chart containing all the stages fused together is in appendix A and B. The next chapter will look at the presentation and analysis of the results obtained from the simulation of the model.

CHAPTER FOUR

SIMULATION RESULTS AND ANALYSIS

4.0 INTRODUCTION

In this chapter, the results obtained from the simulation of figure 3.1 were presented. A snap shot of the process in Simulink is shown in figure 4.1. The results in tables 4.1 & 4.2 and in graphs are presented in Figures 4.6 - 4.15. The simulation was run several times using different values of bandwidth and available bandwidth. The simulations were all analysed to produce the results presented.

4.1 SIMULATION

The block diagram in Figure 4.1 which is MATLAB model shows the implementation of the flow chart developed in chapter 3 in MATLAB Simulink environment. The processes involve Request Generation, definition of Required Resource Capacity, Resource and Available Resources Dump (MIB) Subsystem. Probes were inserted in each subsystem in order to monitor and collect the parameter values required to analyse the management system. The MATLAB model (figure 4.1) was simulated for 1000seconds to enable data to be collected when the system has attained steady state.

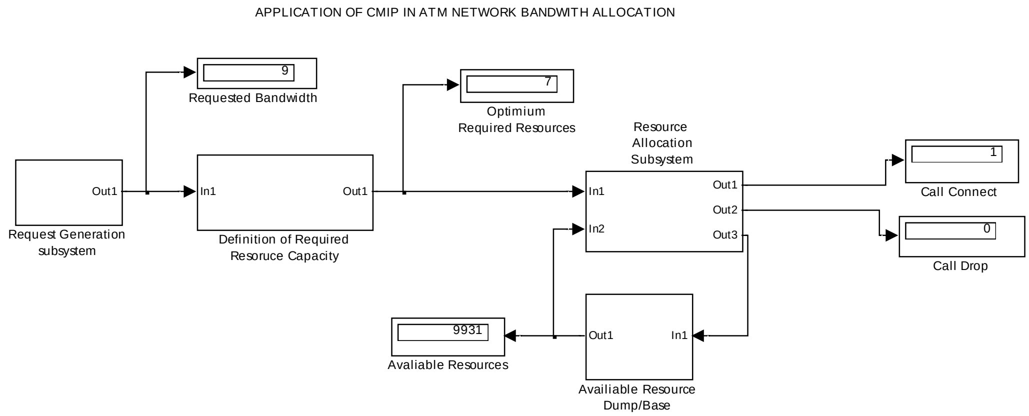


Fig.4.1 CMIP bandwidth allocation block diagram

4.1.1 Request Generation Subsystem

This system is the source of the entire system. It is made up of two blocks: the uniform random bitrate generator and a rounding function.

- The uniform random bitrate generates sets of requests for bandwidth. The bitrates generated for the purpose of this work is set of twenty (20) bitrates representing twenty (20) random requests for bandwidth.
- The rounding function approximates each bandwidth generated to the nearest whole number in order to eliminate decimals.

The figure 4.2 shows Request Generation Subsystem with the output port (Out1) providing the input port (In1) for the next subsystem.

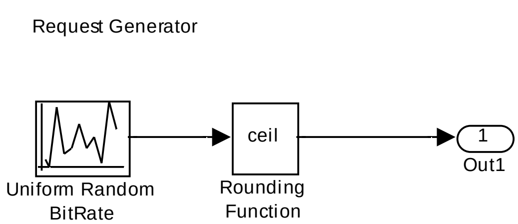


Figure 4.2: Request Generation Subsystem

4.1.2 Definition of the Required Resources Subsystem

This subsystem computes the optimum required bandwidth. It implements the power series expansion $ORB = 8.275 - 0.28B + 0.0046B^2 + 0.0001B^3$ in equation 3.4 for each bandwidth request. This subsystem defines the capacity of the required resources for each bandwidth each request (from port In1). The result of this computation is rounded up to the nearest whole number. All the blocks in this subsystem were extracted from simulink math operation blocksets.

Figure 4.3 shows CMIP ATM Definition the Required Resources Subsystem with the output port (Out1) providing the input port (In1) for the next subsystem (CMIP Resource Allocation Subsystem)

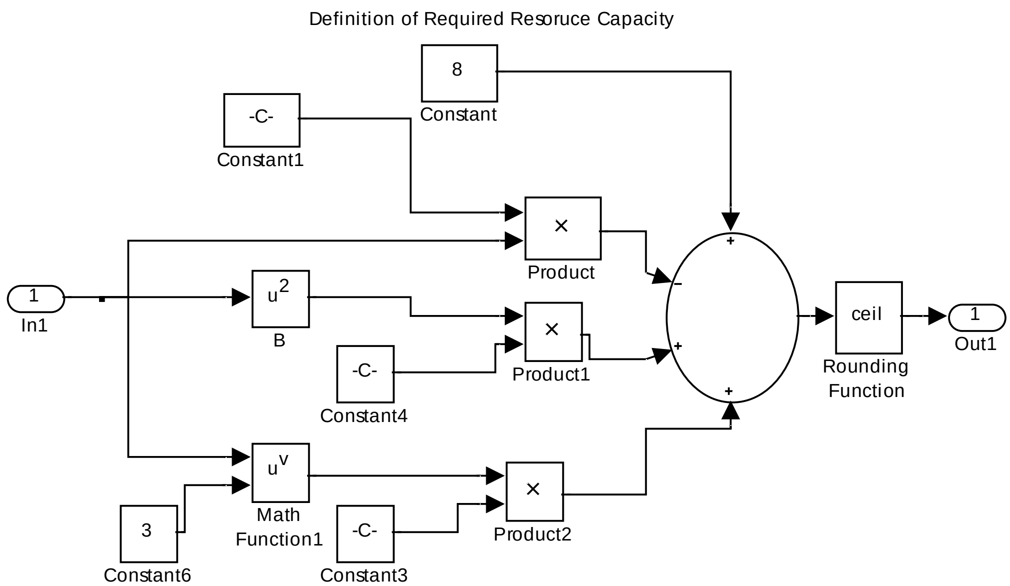


Figure 4.3: CMIP ATM Definition the Required Resources Subsystem

4.1.3 Resource Allocation Subsystem

This subsystem performs the resource allocation by comparing the value of output (Out1) from the Definition the Optimum Required Bandwidth Subsystem (In1) and the Available Bandwidth in the MIB (In2). If the value in MIB is greater than the Optimum Required Bandwidth the output will be a ñoneò else a ñzeroò. The result (either a ñoneò or a ñzeroò) will be multiplied by the bandwidth to get the actual value in order to decrement/update the MIB by subtracting the value of the Optimum Requested Bandwidth from Available Bandwidth in the MIB.

This subsystem has two inputs and three outputs. The input 1(In1) comes from the output of the Definition the Required Bandwidth Subsystem previous subsystem and the input 2 (In2) comes from the MIB (Available Resources Dump Subsystem). The output1 (Out 1) connects to the Call Connect display if itôs a ñoneò it accepts the call. The output2 (Out 2) connects to the Call Drop display if itôs a ñoneò it will drops the call. The output 3 (Out 3) connects to the next subsystem the Available Bandwidth Dump (MIB) Subsystem to update the system of the current value of the MIB. The figure 4.4 shows the CMIP Bandwidth Allocation Subsystem.

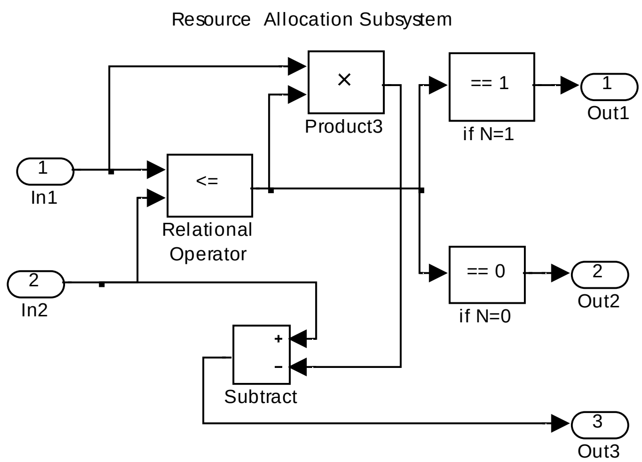


Figure 4.4 CMIP Bandwidth Allocation Subsystems

4.1.4 Available Bandwidth Dump (MIB) Subsystem

This subsystem serves as a database where the managed objects are stored. This is where the initialization process in the flow chart (figure 3.3) is carried out. The value of the available bandwidth is stored here for use by the system. The value of the available bandwidth is set as 20kbps.

The input port (In1) get its signal from output port (Out3) of the resource allocation subsystem and the output port (Out1) goes to the input port (In2) of the resource allocation subsystem. Figure 4.5 shows the diagram of Available Resources Dump (MIB) Subsystem.

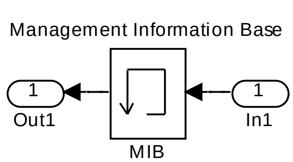


Figure 4.5: Available Resources Dump (MIB) Subsystem

The detailed complete diagram of the CMIP implementation for bandwidth allocation is in appendix C and below is the results and the analysis the entire system.

4.2 SIMULATION RESULTS

The table below shows the simulation results gotten from figure. 4.1. It contains the bandwidth, Optimum Required Bandwidth gotten from the power series expansion, Available Bandwidth, Cumulative Bandwidth Usage and the Command (i.e. whether to connect call or to drop the call).The results of the simulation with 20kbps for the first 20 call arrivals are given in tabular form :

Nth Arrivals	Requested Bandwidth (kbps)	Optimum Required Bandwidth (kbps)	Cumulative Bandwidth Usage(kbps)	Available Bandwidth (kbps)	Command
0	0	0	0	20	Waiting
1	2	8	8	12	Call Connect
2	6	7	15	13	Call Connect
3	17	6	21	14	Call Connect
4	1	8	29	12	Call Connect
5	19	6	35	14	Call Connect
6	15	6	41	14	Call Connect
7	10	6	47	14	Call Connect
8	12	6	53	14	Call Connect
9	5	7	60	13	Call Connect
10	10	6	66	14	Call Connect
11	20	5	71	15	Call Connect
12	11	6	77	14	Call Connect
13	11	6	83	14	Call Connect
14	5	7	90	13	Call Connect
15	10	6	96	14	Call Connect
16	13	6	102	14	Call Connect
17	14	6	108	14	Call Connect
18	8	7	115	13	Call Connect
19	8	7	122	13	Call Connect
20	20	5	127	15	Call Connect

Table 4.1 1st simulation result for 20 kbps Available Bandwidth for first 20 arrivals

The table 4.1 shows the summary of the result for 20kbps and first 20 arrivals with random values of bandwidth between 0 and 20kbps. The graphs below show behaviours of the bandwidth, required resources, available resources and the utilization of the resources.

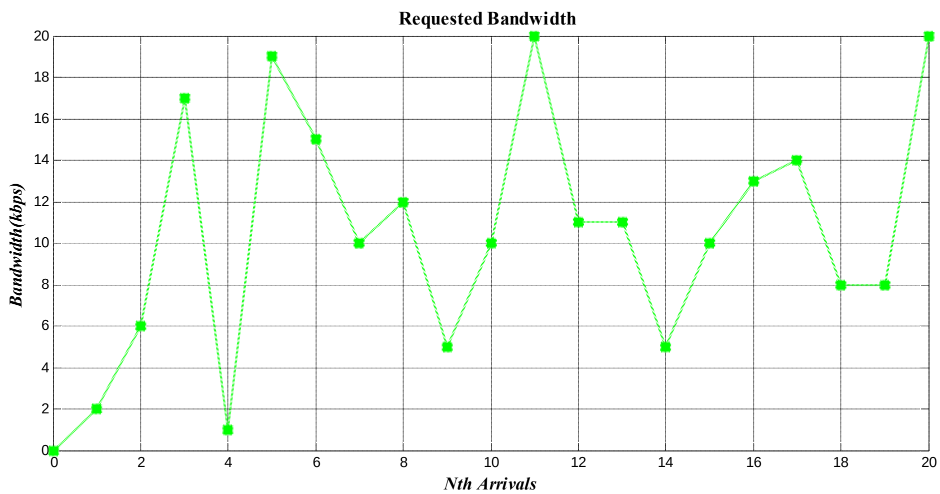


Figure 4.6: Bandwidth Requirements

The fig above shows the bandwidth generated randomly from the Request Generation Subsystem in figure 4.1. The11th and 20th arrivals the bandwidths were at its peak and lowest value at 4tharrival. Peak and the lowest value of the bandwidths were gotten from the Request Generation Subsystem.

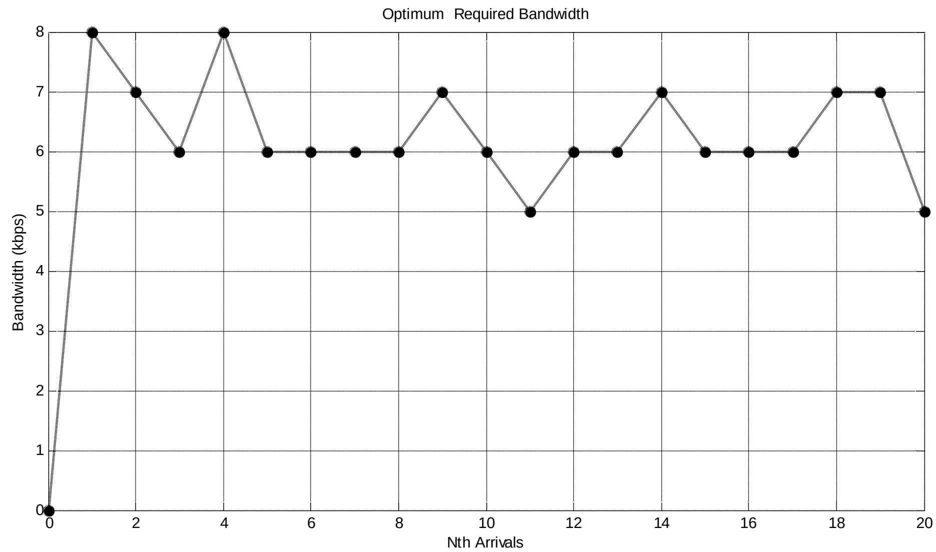


Figure 4.7: Optimum Required Bandwidth

Fig.4.7 shows the computed optimum required bandwidth for the each bandwidth using the power series represented in the MATLAB SIMULINK environment. The required number of resources has peak values at the 1st and 4^{th} arrivals. These values are gotten from the solution of the equation3.9 implemented in figure 4.1.

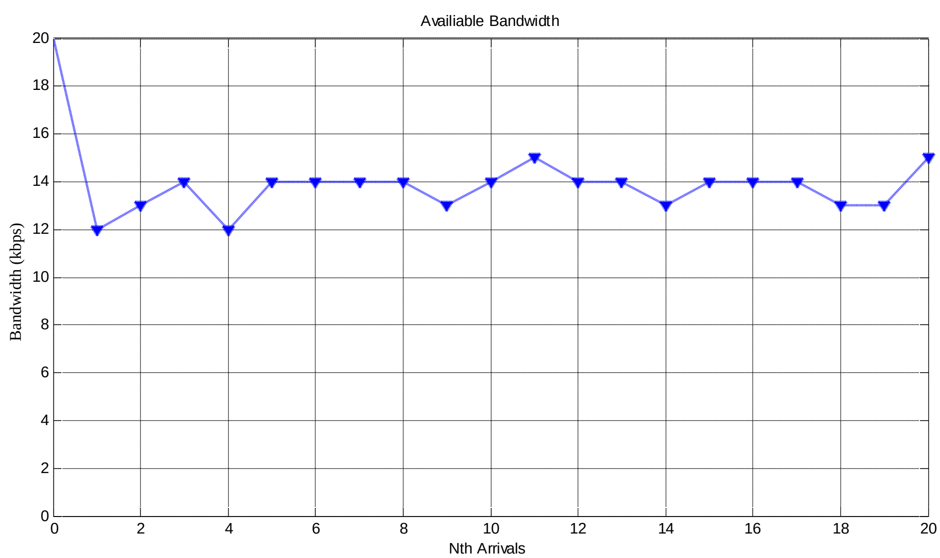


Figure 4.8: Available Resources

The graph above represents the available resources after allocating the resources to the agent.The drops at the 1st and 4^{th} arrivals are as a result of the rise in the optimum required bandwidth.

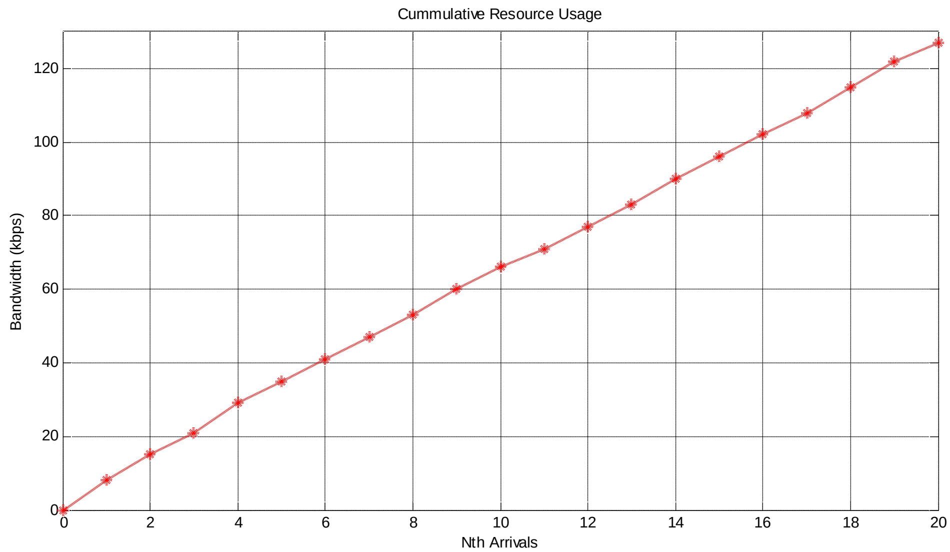


Figure 4.9: Cumulative Resources Usage

Figure 4.9 shows the cumulative resource usage of the first set of 20 arrivals for 20kbps initial available bandwidth. It started from 0 and rose up to 127kbps for the first 20 arrivals

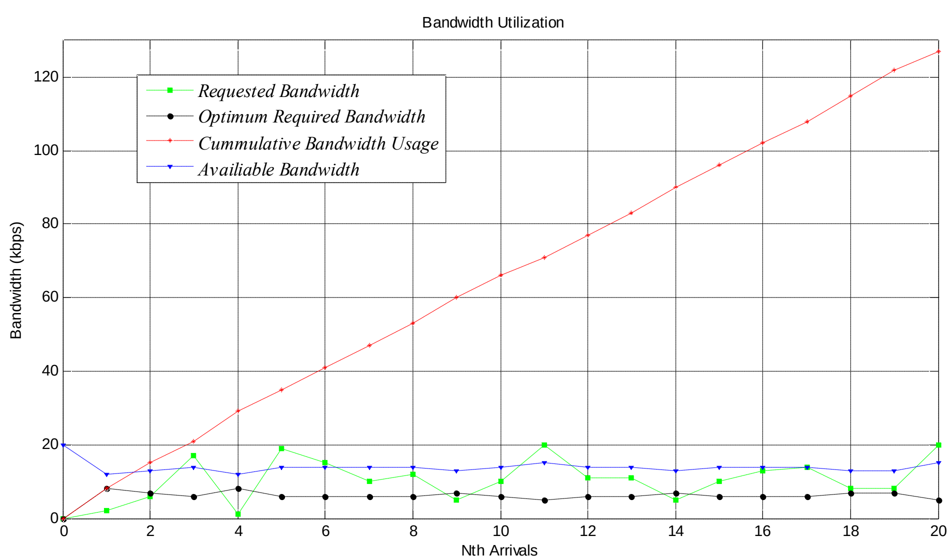


Figure 4.10: Resources Utilization

The graph above represents the utilization of the available bandwidth using CMIP protocol.

From the utilization graph it was discovered that the increase in the number of resources required for each bandwidth requirement there will be a decrease in the available resources.

Comparing the cumulative bandwidth of 127kbps and the available bandwidth of 20kbps, it was discovered 20kbps was used to serve 127kbps requests without call drops. This is to there is effective utilization of the bandwidth.

The table below shows the results of the simulation figure 4.1 for 20 kbps for another set of 20 call request.

Nth Arrivals	Requested Bandwidth (kbps)	Optimum Required Bandwidth(kbps)	Cumulative Resource Usage(kbps)	Available Resources (kbps)	Command
0	0	0	0	20	Waiting
1	11	6	6	14	Call Connect
2	14	6	12	14	Call Connect
3	9	7	19	13	Call Connect
4	17	6	25	14	Call Connect
5	15	6	31	14	Call Connect
6	20	5	36	15	Call Connect
7	11	6	42	14	Call Connect
8	7	7	49	13	Call Connect
9	3	8	57	12	Call Connect
10	13	6	63	14	Call Connect
11	16	6	69	14	Call Connect
12	9	7	76	13	Call Connect

13	2	8	84	12	Call Connect
14	6	7	91	13	Call Connect
15	4	8	99	12	Call Connect
16	6	7	106	13	Call Connect
17	9	7	113	13	Call Connect
18	11	6	119	14	Call Connect
19	10	6	125	14	Call Connect
20	18	6	131	14	Call Connect

Table 4.2: 2nd Simulation Result for 20kbps and first 20 arrivals

The table 4.2 shows the simulation result of 20kbps available bandwidth for another set of arrivals with random bandwidth requirement for the first 20 requests. From the table all the calls that came in were allocated resource. The graphs in figures 4.11-4.16 show behaviours of the bandwidth, required resources, available resources and the utilization of the resources.

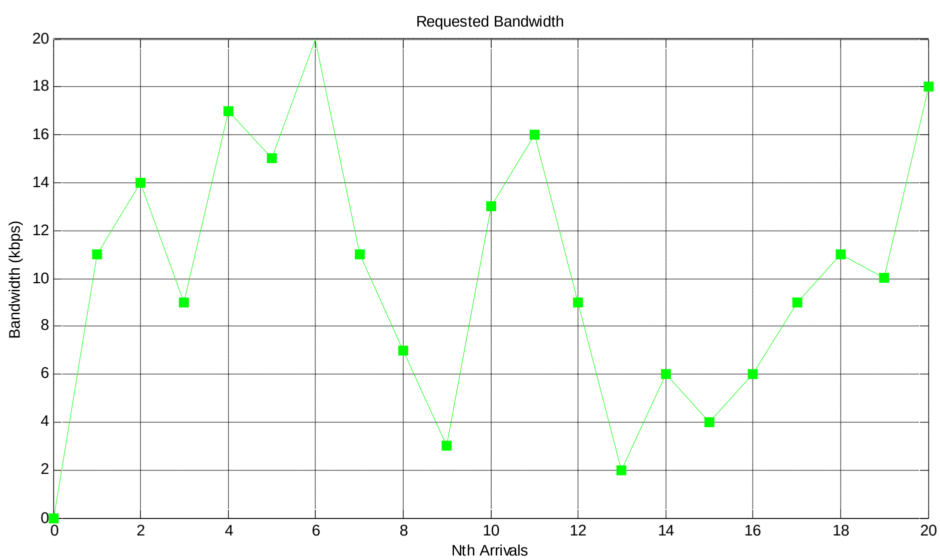


Figure 4.11: Bandwidth Requirements

The figure 4.11 above shows the bandwidth generated randomly from the uniform random bitrate in figure 4.1, for 20kbps for first 20 arrivals. The 9th, 13th and 15th arrivals the bandwidths were at its peak and drops at 6th arrival. The rise and fall in the value of the bandwidths were gotten from the Request Generation Subsystem in the figure 4.2.

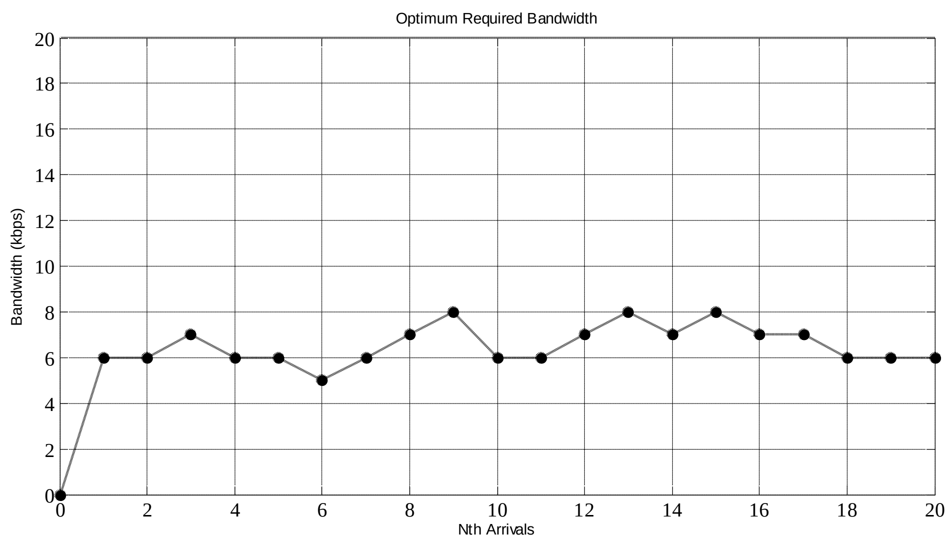


Figure 4.12: Required Number of Resources

Figure 4.12 shows the computed optimum required bandwidth from random bandwidth with the power series represented in the MATLAB SIMULINK environment. The required number of resources has peak values at the 9th 13th and 15th arrivals. These values are gotten from the solution of the equation, 3.9 implemented in figure 4.3.

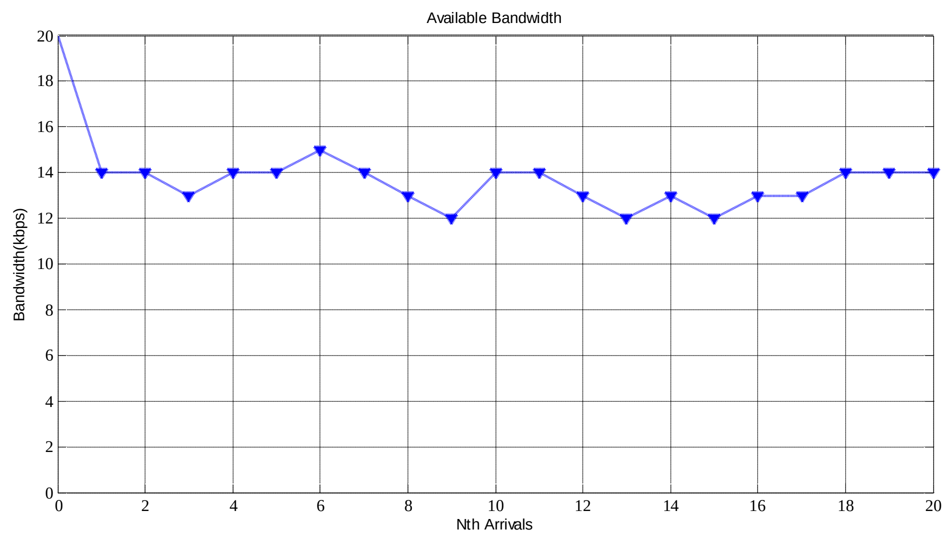


Figure 4.13: Available Resources

The graph above represents the available resources after allocating the resources to the agent.

The drops at the 9th 13th and 15th arrivals were as a result of the rise in the required resources.

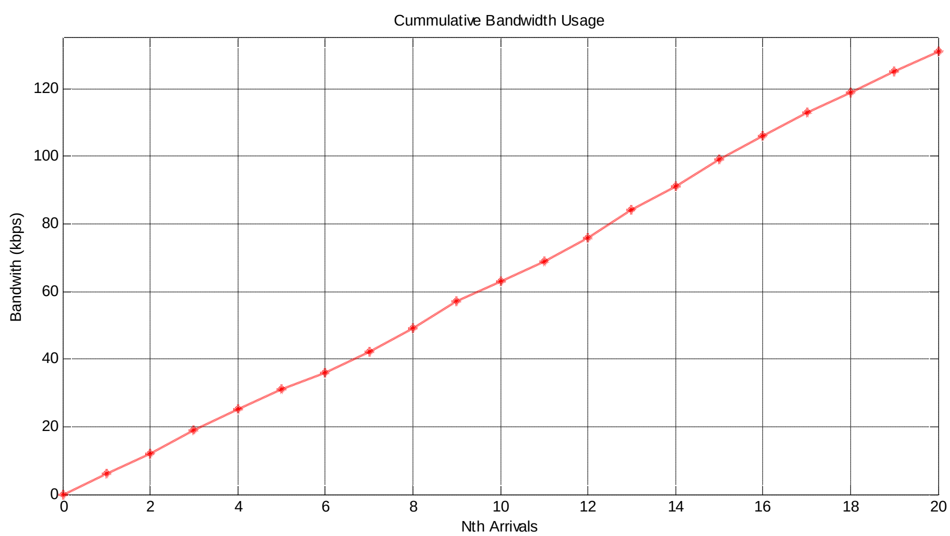


Figure 4.14: Cumulative Resources Usage

The graph on figure 4.14 shows the cumulative resource usage of the first set of 20 arrivals for 20kbps initial available resources. It started from 0kbps and rose up to 131kbps at the 20th arrival. This means that the total bandwidth request for 20 requests is 131kbps.

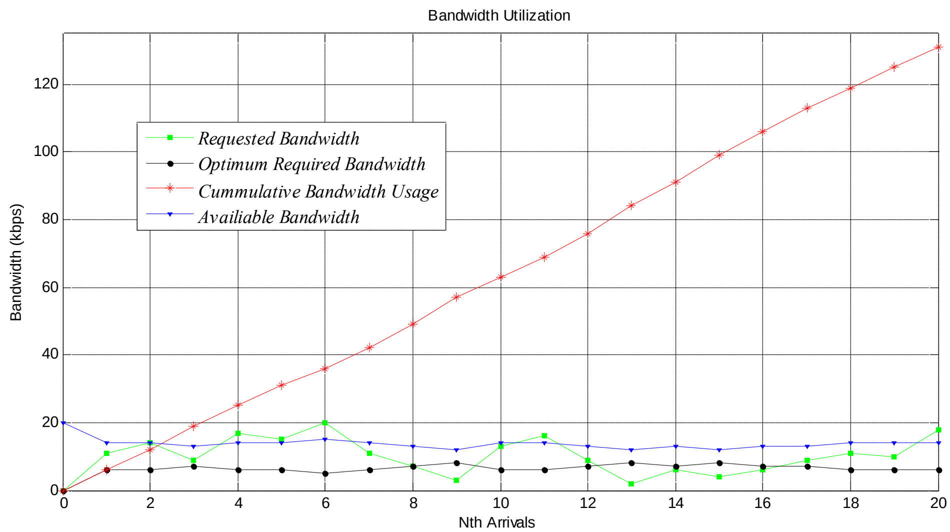


Figure 4.15: Bandwidth Utilization

The graph in figure 4.15 represents the utilization of the available bandwidth using CMIP protocol.

From the utilization graph it was discovered that the increase in the number of resources required for each bandwidth requirement there will be a decrease in the available resources.

The highest drop occurred at 9th 13th and 15th arrivals because of the rise in the optimum required bandwidth. The cumulative bandwidth usage of 131kbps were served with available bandwidth of 20kbps this is to say that there was effective utilization of the bandwidth.

CONCLUSION

This chapter presented the simulation of CMIP protocol as a bandwidth resource allocation tool and results obtained. Next chapter presents the conclusion of whole work and recommendation for further research.

CHAPTER FIVE
CONCLUSION, RECOMMENDATIONS AND CONTRIBUTIONS

5.0 CONCLUSION

In this concluding chapter, the major findings of this work were summarized, and the recommendation for further research given. The achievements of this work will also be highlighted.

The aim of this research work has been to present the state-of-the art of a Common Management Information Protocol (CMIP) that will assist an ATM network in bandwidth resource allocation in order to achieve the required Quality of Service. The results of the simulations in chapter four have clearly shown the following:

- CMIP can manage ATM bandwidth allocation efficiently and effectively.
- CMIP allocates resources to every call without much delay or call drop

This is to say that there was maximum utilization and throughput of network resources.

The results with respect to the QoS parameters of delay, throughput and utilization can be summarized thus:

Delay increases with increase in bandwidth requirements. Delay decreases with increase in number of the available resources. The throughput of this system increases as the available resources increases. Throughput decreases with increase in the required resources and arrivals

From the findings it can be deduced that CMIP is reliable when it concerns ATM bandwidth allocation since there was maximum utilization of the available resources without call drop. Reliability increases with increase in bandwidth allocation and number of resources available.

The major contribution of this work is in the following areas:

- It provided the plat form for resource management and bandwidth sharing.
- It determines the Capacity of the bandwidth for each resource requirement

5.2 RECOMMENDATION FOR FURTHER RESEARCH

In order to improve the performance of the CMIP as an ATM resource allocation protocol, those cases that lead to complexity of the protocolôs MIB has to be tackled. The further work from these results and analysis could be the development CMIP based network resource allocation software to be used by network administrators. Also, try to implement this model into an ATM and see how those allocated resource returns back to the MIB to increment the values there.

And also how to use CMIP to perform other network management functions in ATM Network and other networks.

REFERENCE

1. A. Umar, ñE-Business and distributed systems Hand Book: Overview moduleò, Nge solution copyright, 2003, page 2-19.
2. D. C. Verma, ñPrinciple of Computer Systems and Network Management, Springer copyright, 2011, page 12.
3. C. M. Kozierok, ñThe TCP/IP Guide: A comprehensive illustrated internet, 2005, page 1070.
4. L. G. Ghetie, ñNetworks and Systems management: platform analysis and evaluation. Springer copyright, page 37.
5. S. Z Asit, ñNext Generation Mobile Communications Ecosystemò, 2011.
6. C.I. Ani, R. Ahmad and F. Halsall,ñMethodology for the Derivation of Network Resources to support Video-Related Services in ATM Based Private Wide Area Networkò,IEE.Proc. Communication, vol. 142 Number 4, 1995.
7. ITU-T Recommendation I.732, ñfunctional characteristics of an ATM Equipmentsò, Genevia 2000.
8. J.W. Roberts, ñInternet traffic, QoS and pricing,ò France Telecoms.
9. R. C. Newman, ñComputer Security Protecting Digital Resources, Jones & Bartlett publishers copyright, 2009.page 310.

10. K. Ahmad, ñSource Book of ATM and IP internationalò, John Wiley, 2004, p3.
11. R. Sternmetz,ñMultimedia: Advanced Teleservices and high speed Communication architectureò,Springer copyright, 1994,p 115
12. H. G. Perros, ñAn Introdution to ATM Networksò, NC State University, Raleigh USA, John Wiley and sons ltd, 2002.
13. D. McDysan& D. Spohn,ñATM Theory and Applicationsò, signature edition, USA, McGraw Hill,1999.
14. J. N. Giacopelli, J. J. Hickey, W. S. Marcus, W. D. Sincoskie, and M. Littlewood,óóSunshine: a high-performance self-routing broadband packet switch architecture,ôôIEEE J. Select. Areas Communication, vol. 9, no. 8, pp. 1289_1298, Oct. 1991.
15. ITU-T I.321 (1991), B-ISDN Protocol Reference Model And Its Application.
16. P. Heng, ñSNMP-based ATM network managementò Artech House, Boston London, 1996.
17. S. Kasera, ñATM Networks Concept and Protocolsò ,Tata McGraw-Hill Education, 2006,p48
18. C. A. Johnson and H. Jonathan Chao,ñ The ATM Layer Chip for BISDN Applicationò, IEEE Journal on selected area in Communications, vol9 No 5,June 1991.
19. A. Pattavina, ñSwitching Theory Architecture and performance in broadband ATM Networksò, John Wiley and sons ltd, 1998.
20. S. Verma, ñATM Switch Architecture,ò Department of electrical engineering, Concordia University Canada, 1994.
21. L.G. Culhbert and J.C. Sapanel, ñATM: The Broad Band Telecommunication Solutionsò, IET Copyright, 1993, p7.
22. R.J. Bates, ñBroadband Telecommunication Handbookò, The McGraw Hill, 2000
23. D. Hardy; Guy Mallaeus; Jean-NoeL Maereur, ñNetwork: Internet, Telephony,Multimedia: Convergences and Complementaries ò,Deboeck Superior Copyright, 2002,p202.
24. J. D. Gibson ñMultimedia Communication Direction and Innovationsò, Accademic Press, 2008,p134
25. J. Knapp, ñThe Complete reference Nortel Networksò 2^{nd} editionò, The McGraw Hill, 2002.

26. S. Fahmy, ñA Survey of ATM Switching Techniquesò, fahmy@cse.ohio-state.edu, (1995).
27. H.J. Chao,Cheuk H.Lam & Eiji,Oki,ñ Broadband packet switching Technology; A practical guide to ATM Switches and IP Routers ò,John Wiley & Sons, Inc., New York (2001).
28. J.V. Bosse &Fabrizio,Devetak, ñsignalling in a Telecommunication Networksò 2nd edition,John Wiley and sons ltd,2007.
29. CISCO: internetworking handbook, Cisco Press 2004 P 500.
30. V. Acharaya, ñTCP/IP and Distributed Systemsò, Laxmi Publication, 2006, p37.
31. H.J. Chao,Cheuk H. Lam & E. Oki,ñ Broadband packet switching Technology; A practical guide to ATM Switches and IP Routers ò,John Wiley & Sons, Inc., New York (2001).
32. J. N. Giacopelli, J. J. Hickey, W. S. Marcus, W. D. Sincoskie, and M. Littlewood,óóSunshine: a high-performance self-routing broadband packet switch architecture,óóIEEE J. Select. Areas Communication, vol. 9, no. 8, pp. 1289_1298, Oct. 1991.
33. A.Ben-Artzi, A.Chandna, and U.Warrier, ñNetwork Management of TCP/IP networks: Present and Futureò, IEEE Network Management system July, 1990.
34. ATM Forum Technical Committee: traffic management Specification Version 4.1, AF-TM-0121.000, March 1999.
35. J. D. McCabe Amsterdam, ñNetwork Analysis Architecture, and Designò, 3rd Ed,   Morgan Kaufmann Publishers, USA, 2007.
36. L. G. Widjaja,ñCommunication Network Fundamental Concept and Key Architecturesò 2009.
37. J. Ding,ò Advances in Network managementò, CRC Press Taylor& Francis, 2010.
38. M. Subramian; Timothy A. Gonsalves; N. Usha Rani, ñNetwork Management: Principles and Practiceò, Pearson Education India, 2010.
39. M. Jonnerby,ñTraffic Performance in an ATM networkò1999,MSc Thesis, Department of Teleinformatics, Royal Institute of Technology, Ericsson Telecom AB, Datacom Networks & IP Services.
40. B. Singh, ñNetwork Security and Management,ò3rd edition, PHI Leraning pvt ltd, 2012, New Dehli.

41. B. Singh, ñData Communication and Computerò 2nd edition, PHI Leraning pvt ltd, 2012, New Dehli. Management models

42. S. T. Karis, ñNetworks Design and Managementò, 2nd Edition, Orchard publication, 2009.

43. P. Oppenheiner, ñTop-down Network Designò,Cisco Press, 3rd edition,2007,pp 300-305.

44. So, Y.; Durfee, E., ñDistributed Big Brotherò, 8th International Conference on Artificial Intelligence and Applications, 1992, pp. 295-301.

45. Herman, J., ñEnterprise management Vendors shoot it outò, Data Communication International, November 1990.

46. F. Stamatelopoulos; T. Chiotis; B. Maglaris, ñA Scalable, Platform-Based Architecture for Multiple Domain Network Managementò, 2002.

47. M. J. Castelli,ñNetwork Consultants Handbookò, Cisco Press,2002,page 650

48. M. J. Castelli,ñNetwork Sales and services Handbookò, Cisco Press,2002,p258

49. ITU-T RecommendationX.700, ñManagement Framework for Open System Interconnection (OSI) for CCITT Applicationò, Geneva, 1992

50. P.G.Nanasivam,ñTelecommunication Switching and Networksò, New Age International (P) Limited,New Dehli, India, 2nd edition, 2006, pp21-23.

51. R.L. Freeman, ñFundamentals of Telecommunicationsò, 2nd edition, John Wiley & Sons, Inc., Hoboken, New Jersey, 2005.

52. C. Chung, ñWeb Communication Technologies and Internet-Related Social Issues.ò,springer copyright,2003,page 412.

53. D. Nikolik, ñA Managerôs Primer on E-Networkingò, 2003, Kluwer academic publishers, p264.

54. G. Shields, ñThe Shortcut Guidetm to Network Management for The Mid-Market,òReal Time Publishers, 2012.

55. G. Farahani,ñDesign and Implementation of New Architecture to Improve Management Performance of IP-Based networkò 18-ICICN2012

56. CCITT Recommendation X.701 (1992)1) | ISO/IEC 10040:19921), Information technology ï Open Systems Interconnection ï Systems management overview.

57. K. Kotsopoulos, ñManaging Next Generation Networks (NGNS) Based On The Service-Oriented Architecture (SOA)ò, School of Engineering Design and Technology, University of Bradford, 2010.

58. ITU-T Recommendation X.710 (1997) | ISO/IEC 9595:1998, Information technology ï Open Systems Interconnection ï Common management information service.
59. CCITT Recommendation X.711 (1991), Common management information protocol specification for CCITT applications. ISO/IEC 9596-1:1991, Information technology ï Open Systems Interconnection ï Common management information protocol ï Part 1: Specification
60. ITU-T Recommendation X.229 (1988), Remote operations: Protocol specification. ISO/IEC 9072-2:1989, Information processing systems ï Text communication ï Remote Operations ï Part 2: Protocol specification
61. CCITT Recommendation X.219 (1988), Remote operations: Model, notation and service definition. ISO/IEC 9072-1:1989, Information processing systems ï Text communication ï Remote Operations ï Part 1: Model, notation and service definition
62. ITU-T Recommendation X.217 (1995) | ISO/IEC 8649:1996, Information technology ï Open Systems Interconnection ï Service definition for the association control service element.
63. T. Krammer, ñNetwork Management protocols and tools studyò, GRIN Verlag, 2002.
64. Lundy, Lewis, ñManaging Business and Service Networksò, Springer copyright, 2001, pp 27.
65. C. McHale,ñCORBA Explained simplyò www.CiaranMcHale.com, 2007.
66. B. Ben, ñA Generic Management Model for COBRA, CMIP and SNMPò, (1997) www.books.google.com.ng/books?id=ZEVztwAACAAJ .
67. P. Lorenz, ñNetworking - ICN 2001: First International Conference on Networking, springer copyright, 2001, page 411.
68. A. Kumar, D. Manjunath, Joy Kuri, ñCommunication Networking: An Analytical Approachò, Morgan Kaufmann Publishers is an imprint of Elsevier, 2004, page 44.
69. ITU-T Recommendation M.3010 (2000), Principles for a telecommunications management network.
70. M. DePrycker , ñAsynchronous Transfer Mode Solution for Broadband ISDN,ò 1995,
ISBN 0-13-342171-6

71. ATM Forum, ñTraffic Management Specification Version 4.0ò, AF-TM-0056.000, 9703 April, 1996

72. I.W.Phillips, J.M.Sandford, D.J.Parish, ñGeneric Performance Management of Multiservice Networks,òDepartment of Electronic Engineering, Loughborough University, Leics, LE11 3TU,U

73. ITU-T Recommendation E.800 (1994), Terms and definitions related to quality of service and network performance including dependability.

74. ITU-T Recommendation I.350 (1993), General aspects of quality of service and network Performance in digital networks, including ISDNs.

75. T. S. Randhawa, Stephen Hardy, ñNetwork Management in Wired and Wireless Networksò, Kluwer Academic Publishers, USA, 2002.

76. C. M. White, ñData Communication and Computer Networks; A business userôs approachò, Course technology, USA, 2001.

77. ITU-T Recommendation I.356 (11/1993), B-ISDN ATM layer cell transfer performance.

78. T. Lindh, ñPerformance management in switched ATM networks,ò in Proceedings, Intelligence in Services and Networks: Technology for Ubiquitous Telecom Services, pp. 439ï 450, March 1998.

79. D. Ying, Q. Feng, M. Luoming, ñImplementation of a CMIP Based Management Interface for Optical Access Networkò National Laboratory of Switching Technology &Telecommunication Network P. 0. Box 198, Beijing University of Posts & Telecommunications (BUPT) Beijing, 100876, China.

80. D. Tian, ñA Software Architecture Supporting CMIP Management Information Bases of ATM Switches,ò Broad-work Technologies, 107 Esplanade Court, Cary. NC 275 1 1, 0-7803-2509-5195, IEEE explore, 1995.

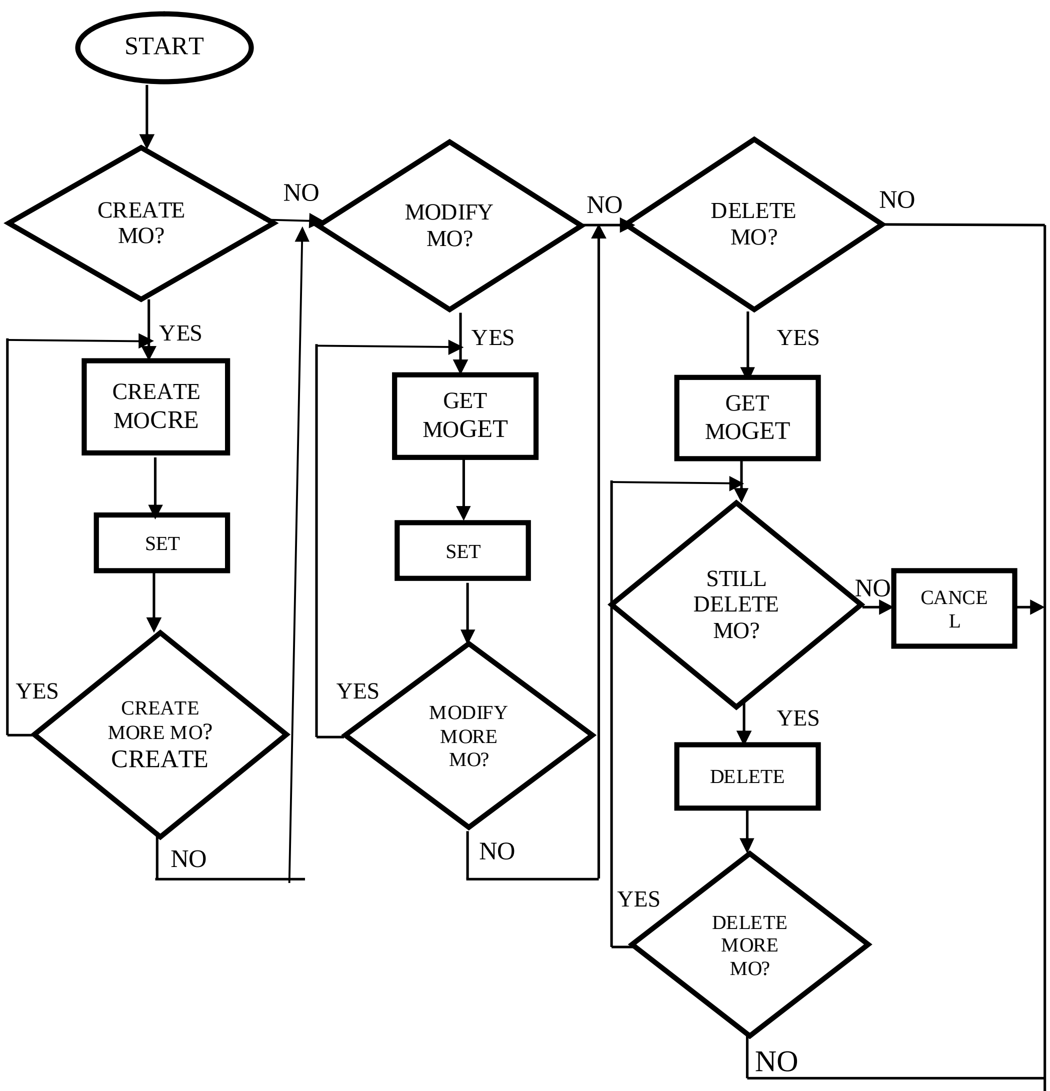
81. J.Y. Hui, ñResource allocation for broadband networks,ò *IEEE J. Sel. Areas Commun.*, vol. 6, no.9, pp. 1598-1608, December 1988.

82. Y. Cheng and W. Zhuang, ñEffective bandwidth of multiclass markovian traffic sources with admission control with dynamic buffer partitioning,ò *IEEE Trans. Commun*., vol. 51, no. 9, pp. 1524-1535, September 2003.

83. A.R. Bashandy, E.K.P. Chong and A. Ghafoor, ñGeneralized quality-of-service routing with resource allocation,ò *IEEE J. Sel. Areas Commun.*, vol. 23, no. 2, February 2005.

84. C. I. Ani, ñResource Allocation Methodology for internet Heterogeneous Trafficò, Department of Electronic Engineering UNN, Nigerian Journals of technology vol. 223 No 1, March 2004, page 21.
85. J. Bird, ñHigher Engineering Mathematicsò fifth edition, Newness an imprint of Elsevier ltd USA, 2006, page 29.

APPENDIX A



APPENDIX B

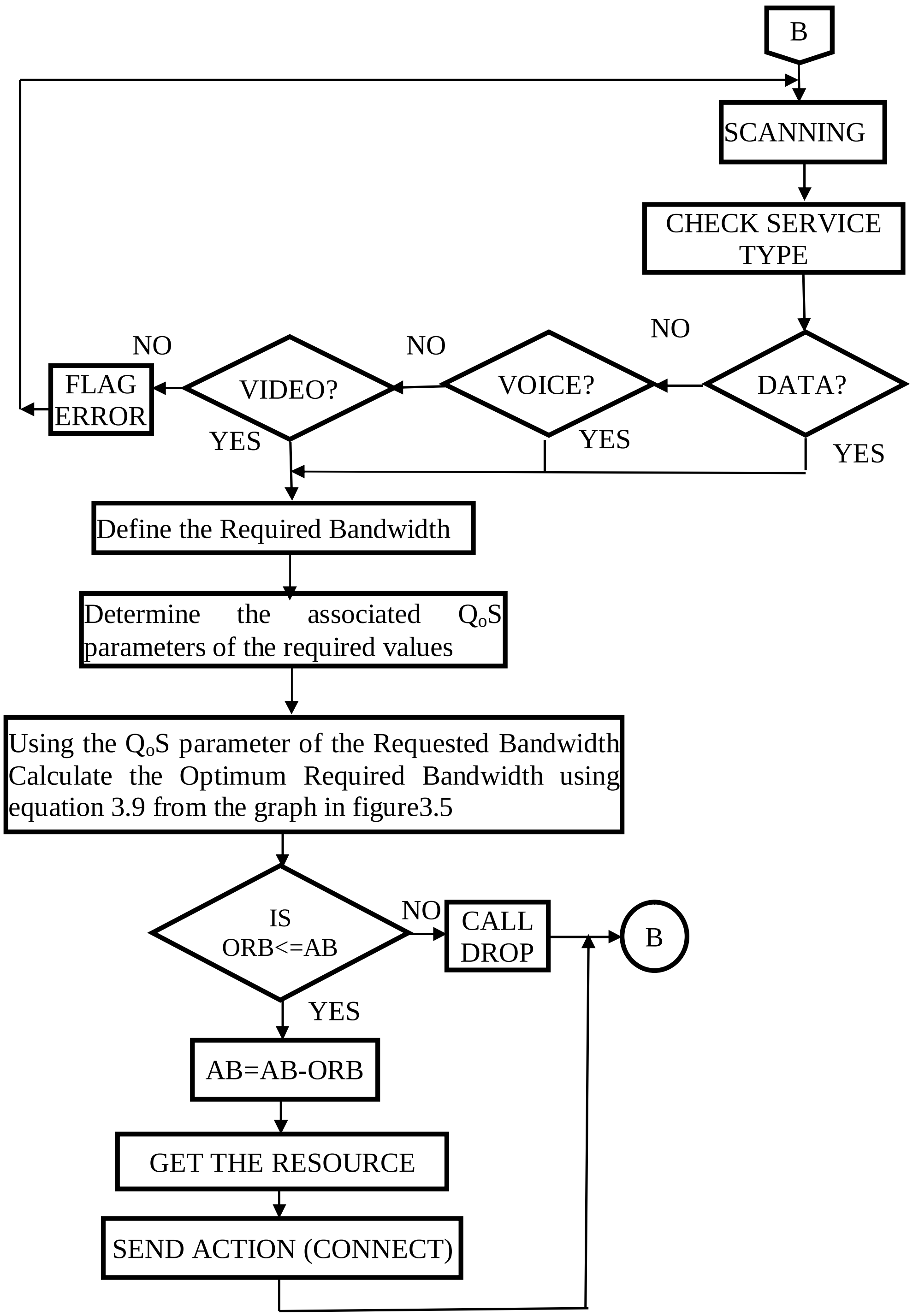


Figure B: Continuation of CMIP flow chart operation for bandwidth allocation

APPENDIX C

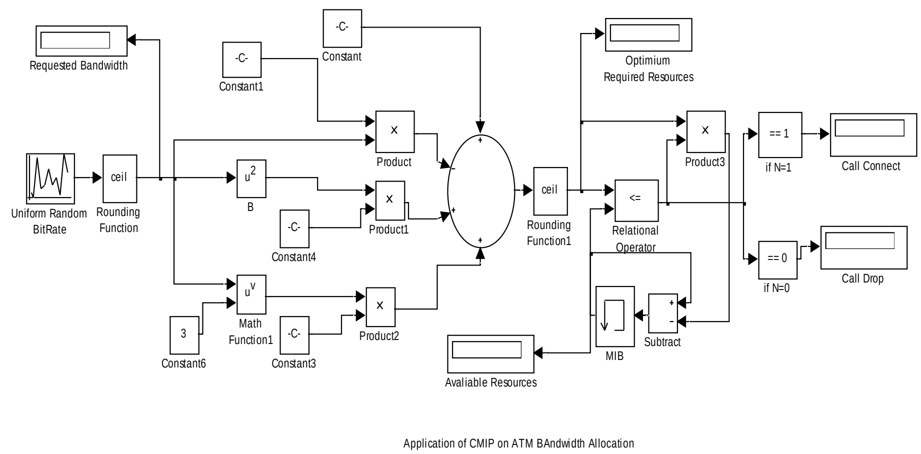


Figure C: CMIP bandwidth allocation in simulink