APPLICATION OF THE SYSTEMS ENGINEERING PROCESS TO DEVELOP A WIDE AREA NETWORK COMMUNICATIONS SYSTEM UPGRADE DESIGN

by

Carl F. Cole

Project and Report submitted to the faculty of the
Virginia Polytechnic Institute and State University
in partial fulfillment of the requirements for the degree of

MASTER OF SCIENCE

in

Systems Engineering

APPROVED:

B.S. Blanchard, Chairman

G.W. Sullivan

H. A. Kurstedt

April 8, 1994

Blacksburg, Virginia

APPLICATION OF THE SYSTEMS ENGINEERING PROCESS TO DEVELOP A WIDE AREA NETWORK COMMUNICATIONS SYSTEM UPGRADE DESIGN

by

Carl F. Cole

Committee Chairman: Professor Benjamin S. Blanchard
SYSTEMS ENGINEERING

(ABSTRACT)

The Systems Engineering Process has been applied to develop a wide area network communications system upgrade design for Alpha Beta Corporation to enhance information exchange and improve productivity.

A feasibility study establishes justification for a system upgrade. Detailed operational and maintenance requirements are defined and documented and a program management plan is formed. An evaluation of technical alternatives, based on life-cycle cost projections and effectiveness factors, is completed after functional analyses are used to allocate system level requirements to the subsystem level. Design team organization, subsystem specifications and system optimization and testing are then addressed. Finally, recommendations for future research are presented.

ACKNOWLEDGEMENTS

I wish to acknowledge the assistance provided by my committee chairman, Dean Blanchard, in completing this project as well as for his guidance and support throughout my graduate career. His extensive knowledge and experience with the systems engineering process proved to be invaluable. I am indebted to Gary W. Sullivan for allocating personal time to serve as a committee member and for assisting me with all phases of this project during the last two months. I'd also like to acknowledge the guidance of committee member Harold Kurstedt. Professor Kurstedt influenced my writing techniques and thought process enhancing the clarity, continuity and quality of this report. Additional thanks go to the Martin Marietta Corporation for their support of higher education and advancement.

Finally, special recognition goes to Nancy L. Rooney for the continuous support, encouragement, and patience she has provided over the three years of this Masters Degree Program.

Table of Contents

Table of Contents, continued

Table of Contents, continued

Table of Contents, continued

List of Figures

List of Figures, continued

1) Introduction

Background Information

In the past five years information technology has exponentially expanded establishing revolutionary computing advancements. In the late 1980's, information technology consisted of proprietary, single application, mainframe computers offering time shared access through dumb terminals. Typically, there were ten users per desk top terminal and system performance was less than 18 kilobits per second (Kbps). Today, information technology involves integration and interoperability of large scale information systems consisting of distributed multimedia applications, powerful desk top work stations, servers, and personal computers. Two desk top computers per user and system performance exceeding 100 Megabits per second (Mbps) is typical. A period of tremendous change and significant growth in communications networks and computing is upon us.

The growth in communications networks and computing technology has dramatically restructured business environments world wide. Businesses now operate in a global market place with wide geographically distributed work groups. Competition is time critical, with increasing priority on shared information across work groups and divisions. Interoperable communications systems are a strategic imperative.

However, the rapidly accelerating complexity of information technology presents a difficult challenge for information system managers. Businesses wishing to replace inadequate legacy systems must do so carefully, only after identifying and reviewing goals and objectives, and establishing and firmly defining system requirements. System planning and architecture design are absolutely essential. As the scale of resources needed to manage communications systems continues to skyrocket, businesses are faced with the dilemma of quickly and effectively implementing new information technology to satisfy growing needs. In this situation, the systems engineering process is a valuable, effective methodology to employ to assist information system managers in developing and upgrading existing communications systems.

An example of this dilemma, faced by many businesses today, forms the basis of this project. Alpha Beta Corporation's (ABC) Information Systems Division is responsible for developing, installing, operating, and maintaining an upgrade design for an existing wide area network (WAN) providing electronic mail (E-mail) communications between ABC's six corporate sites (See Figure 0). The Information System Division program manager and chief engineer are aware of the difficulties involved in completing this task and have requested a systems engineering approach to developing the upgrade design.

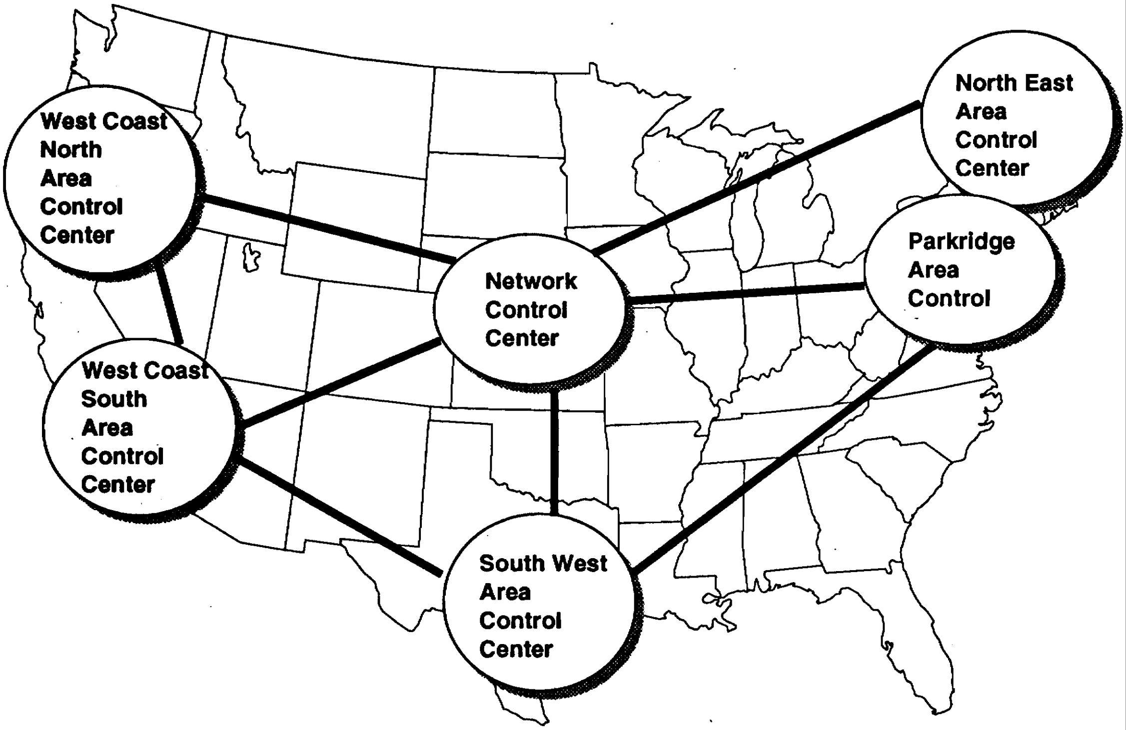

Figure 0. ABC Communications Network

Project Objective

The objective of this project is to apply the systems engineering process as illustrated by Blanchard and Fabrycky in their book, Systems Engineering and Analysis, to develop an upgrade design of the existing ABC wide area network communication system. The four main objectives of the upgrade design are:

Objective 1: Improve User Productivity

Provide a common open operating environment enabling information and software application resource sharing between a variety of hardware platforms.

Objective 2: Enhance Information Exchange

Implement standard communication formats and interface requirements.

Objective 3: Reduce Life-Cycle Costs

Maximize use of COTS products reducing dependence on custom applications and the associated development and maintenance costs. Open systems reduce duplication, increase resource reuse, and provide network scalability and flexibility.

Objective 4: Improve System Management

Control network access and process network audit data from a centralized source.

2) The Systems Engineering Process

Introduction

The systems engineering process uses analytical techniques to establish and continually evaluate a system's design, operation, and support providing a very thorough, logical methodology for effectively developing ABC's communications system upgrade design. The process coordinates engineering and design activities related to the system life-cycle. These activities include the Conceptual Design, Preliminary Design, Detail Design, Construction, Operation, and Retirement Phases of the system life-cycle process as described by Blanchard and Fabrycky. This section outlines the systems engineering approach applied to develop the Conceptual Design, Preliminary Design, and Detail Design Phases of the ABC communications system upgrade as documented in section three of this report.

Conceptual Design Phase

Figure 1 summarizes the activities associated with the Conceptual Design Phase. Information gathering and technology research are an extensive part of the conceptual design phase providing the data required to evaluate the feasibility of implementing an upgrade design, define system requirements, and begin advanced system planning. Information gathering includes performing a needs analysis to document current system inadequacies and future system requirements. Technology research includes identifying technical alternatives through examination

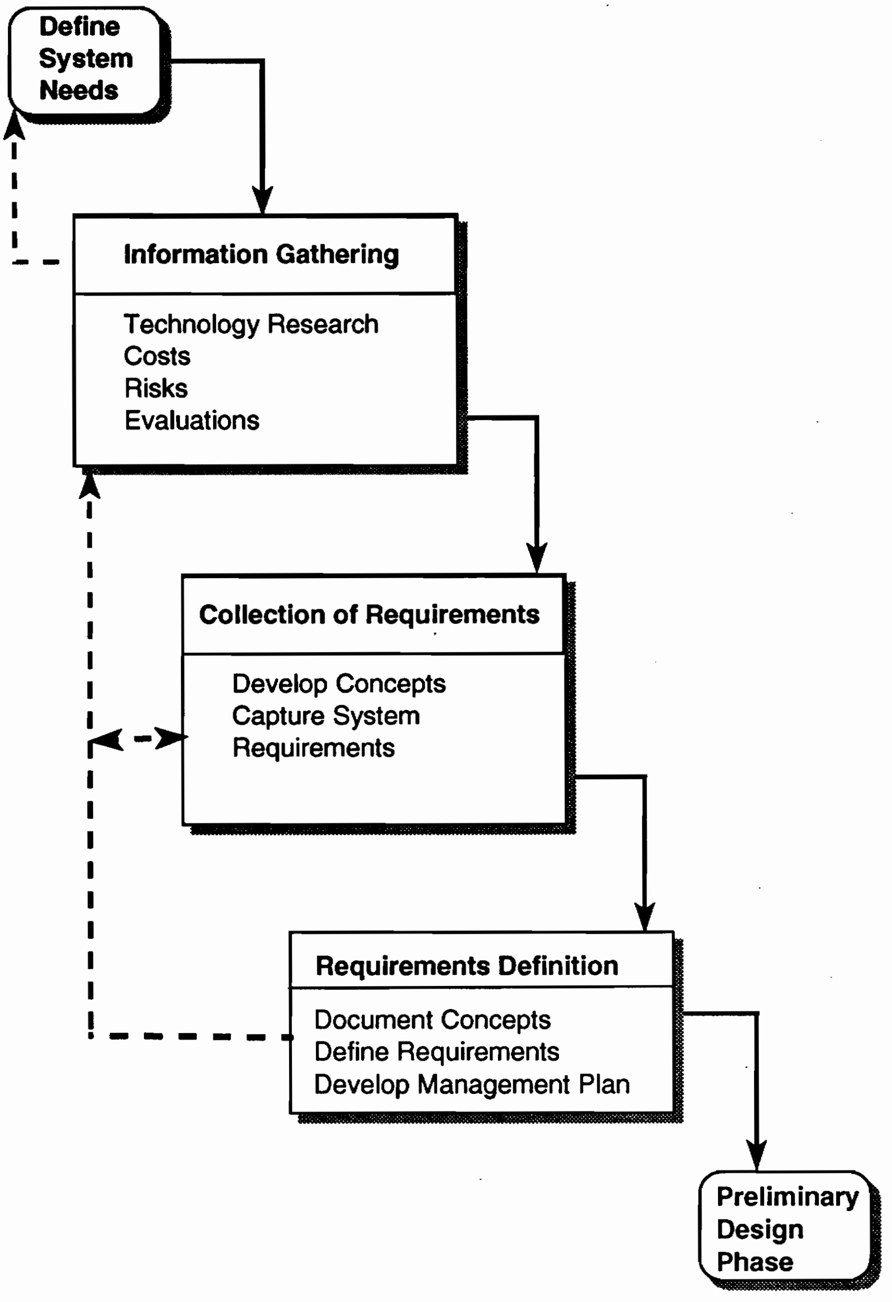

Figure 1. Conceptual Design Phase

and review of current information technology and industry trends. Life-cycle cost data, and any associated risks involved are also collected and considered. Based on the selection and recommendation of the most cost effective and risk free alternative, operational concepts are developed and documented leading to the development, collection and definition of system requirements. Advanced system planning, including organizational, cost, and work breakdown structures along with a project master schedule, is completed in preparation for the preliminary and detail design stages.

Preliminary Design Phase

Figure 2 summarizes the activities associated with the Preliminary Design Phase. Preliminary design begins with the systems technical baseline defined in the Conceptual Design Phase. Refinement of system operational concepts and requirements is accomplished through functional analysis and system requirements allocation. The systems engineering process develops functional requirements in more detail through an iterative analysis incorporating feedback loops as illustrated in Figure 2. Allocation of requirements to the subsystem level provides baseline for the identification of alternative design solutions. System synthesis and optimization is achieved through comparison and evaluation of economic goals and specific functional and operational requirements.

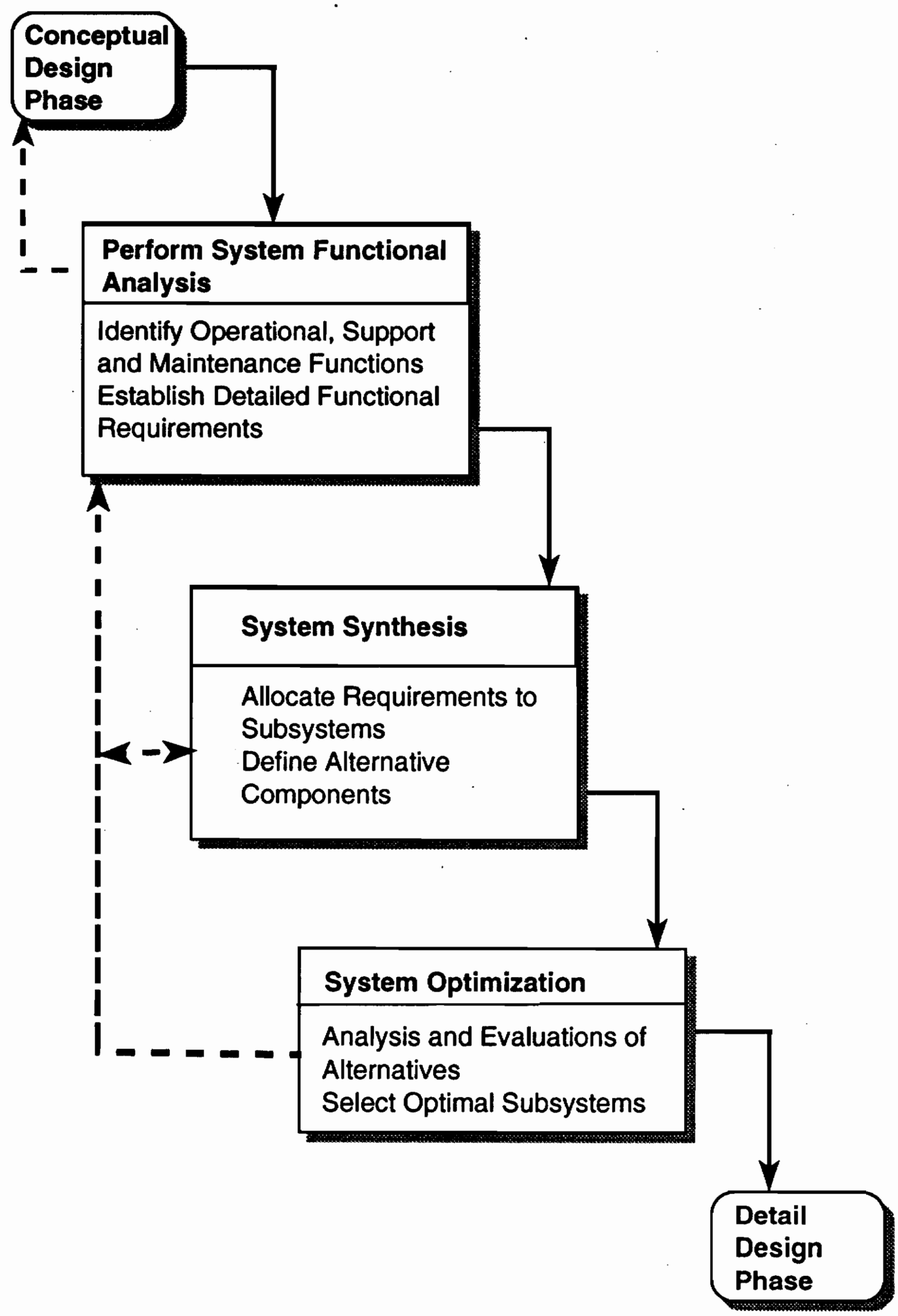

Figure 2. Preliminary Design Phase

Detail Design Phase

Figure 3 summarizes the activities associated with the Detail Design Phase. Detail design begins with the configuration derived in the Preliminary Design Phase and continues further definition of system and subsystem specifications, provides detailed design documentation, and establishes development of a system prototype. Again, as illustrated in Figure 3, continuous evaluation and feedback mechanisms are incorporated into the Detail Design Phase.

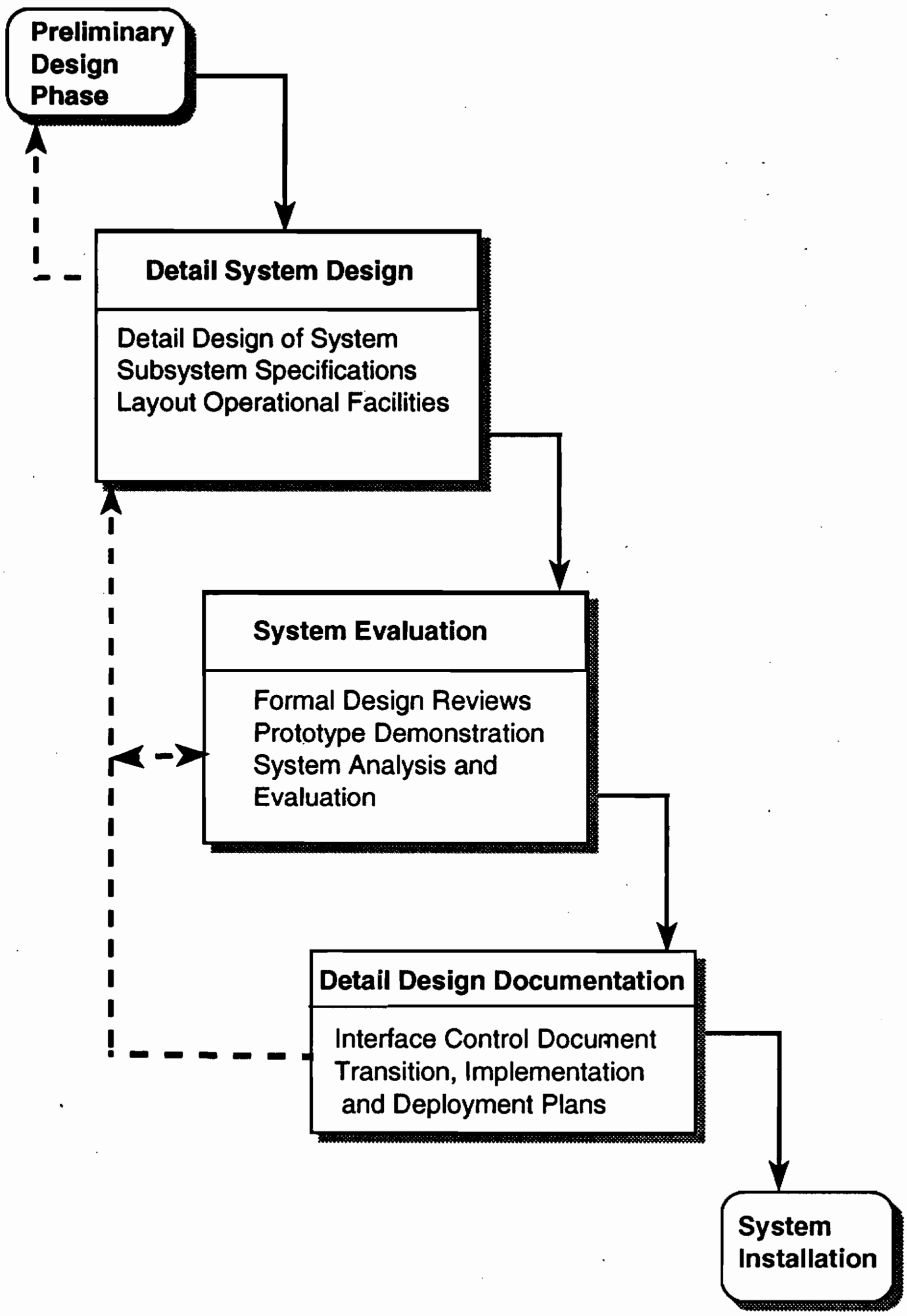

Figure 3. Detail Design Phase

Summary

The system engineering activities outlined in the previous design phases provide high-level guidance to complete the wide area network communications upgrade design for Alpha Beta Corporation. Completing each design phase requires a thorough, concurrent, and most often complicated, analysis involving continual corrective feedback and iterative design and review processes. This report describes a modified application of this process, tailored from Blanchard and Fabrycky, to develop the communications system upgrade Conceptual, Preliminary, and Detail Design Phases. The modified process includes a feasibility study establishing justification for a system upgrade. Detailed operational and maintenance requirements are defined and documented and a program management plan is formed. An evaluation of technical alternatives, based on life-cycle cost projections and effectiveness factors, is completed after functional analyses are used to allocate system level requirements to the subsystem level. Design team organization, subsystem specifications and system optimization and testing are then addressed. Finally, recommendations for future research are presented.

3) Conceptual Design Phase

The intent of the Conceptual Design Phase is to explore, examine, and substantiate information relevant to making effective and knowledgeable design decisions. The information is used to justify the system upgrade, develop system concepts, define system requirements and begin advanced system planning. To that effect, the three major sections addressed in the Conceptual Design Phase are the feasibility study, definition of system requirements, and advanced system planning.

3.1) Feasibility Study

The feasibility study provides justification warranting the ABC communication system upgrade. A definition of needs describes current system inadequacies and outlines future system requirements. An extensive technology research identifies key information technology and services capable of fulfilling primary system inadequacies. Life-cycle cost evaluations, risk assessments, and further recommendations are then completed establishing the decision to proceed with the ABC communications system upgrade design.

Definition of Needs

The objective of this section is to define the business and user needs and expectations; and describe the inadequacies of the existing ABC communications system in qualitative and quantitative terms. The key objectives of the upgrade design are provided below. Key service and technology needs are further examined in the Information Services and Supporting Technology sections that follow.

Objective 1: Improve User Productivity

Provide a common open operating environment enabling information and software application resource sharing between a variety of hardware platforms.

Objective 2: Enhance Information Exchange

Implement standard communication formats and interface requirements.

Objective 3: Reduce Life-Cycle Costs

Maximize use of COTS products reducing dependence on custom applications and the associated development and maintenance costs. Open systems reduce duplication, increase resource reuse, and provide network scalability and flexibility.

Objective 4: Improve System Management

Control network access and process network audit data from a centralized source.

Business Needs

Alpha Beta Corporation needs a standards based E-mail system to enable a modular building block approach for company expansion and to accommodate incremental change and technology expansion. ABC has allocated 8.0 million dollars to implement a new E-mail system linking its six corporate sites. However, ABC will not invest in an E-mail system with an expected life span of less than five years. Also, a goal of ABC is to be able to electronically communicate with its customers, subcontractors, suppliers, and vendors E-mail systems. The ABC E-mail system must provide a directory service structure flexible enough to accommodate anticipated company acquisitions and growth without requiring wholesale replacement of all or large portions of the network. Also, the directory services must be able to expand incrementally in response to the expected 10% per year user growth with no disruption of ongoing network operations. ABC E-mail must be capable of delivering CAD, engineering graphics, and financial graphics files. The E-mail network must provide network monitoring services to provide effective technology resource management and reduce life-cycle maintenance costs. The network monitoring service is needed to document system utilization, and test and optimize system performance. ABC also expects to implement video teleconferencing to improve productivity and quickly communicate business wide best practices. Therefore, the ABC communications network must be capable of supporting multimedia applications.

User Needs

A company wide 1994 software utilization survey indicates an overwhelming (89%) number of employees currently use presentation graphics, word processing, or computer aided design packages not supported by Wang. The ABC mail system must be capable of interoperation with the primary user and subcontractor mail systems:WP Office,NeXT Mail, MS Office, cc:Mail, SMTP Mail, and Quickmail. Also, the ABC mail system shall be capable of providing document conversion for the primary user and subcontractor word processing packages:Word Perfect, Microsoft Word, and Mac Write.

The ABC system will be capable of supporting the expected daily utilization demands as presented in Figure 20. ABC employees work on continuous shifts and need an E-mail system that will be available 24 hours a day 7 days a week. ABC information is time critical. The E-mail system must have a very low failure rate - one system failure per year. System failures must be corrected within the same business day.

ABC user growth estimates indicate a required E-mail capacity capability of 5000 users per node. Additionally, ABC estimates user data transmission rates to increase with the expected multimedia applications. An ABC E-mail system will support WAN backbone data transmission rates of 2 giga bits per second. Users expect to send and receive files within seconds. The ABC network needs to deliver 10 mega bit multimedia documents or files in less than 10 seconds.

Alpha Beta Corporation communications must remain secure. The E-mail system must provide user verification and authentication access controls.

ABC Wang System Inadequacies and Deficiencies

A Wang based wide area network communications system is forcing ABC out of business. The proprietary Wang system, installed in 1988, no longer provides ABC with the technology required to remain competitive. The Wang 150 user maximum capacity per node has stifled ABC growth and will not meet the expected 10% per year employee growth rate through 1999. The current Wang system performance of 9.6 Kbps is not sufficient to meet the estimated 1994 throughput demand of 150 Kbps. Proposed ABC multimedia applications can quickly consume 100 Mbps of local network bandwidth. Wang support and maintenance costs have increased 25% each year for the last three years and are anticipated to continue rising. Expansion costs have increased 50% over the same period requiring vendor specific hardware and software purchases. The outdated Wang components are bulky, requiring large operational space allocations with complex HVAC accommodations and custom structural supports. Also, Wang incompatibility with customer, as well as subcontractor, and supplier mail systems limits ABC flexibility, available services, and engineering output. Employee frustration with the system's slow response time, and system crashes during high utilization periods create user animosity and force high work loads on system administrators.

Information Services

The major components of a communications system are the services it provides to its users and the technology implemented to support those services. This section examines the services provided by the existing Wang communications network. The discussion focuses on the primary services required of any effective communications network. These services include electronic mail (E-mail), file transfer, directory, and network management services. System inadequacies are identified following the description of the services.

Electronic MailServices

The existing communications system is based on the utilization of Wang VS systems and incorporates the memo and package formats featured in Wang Office. Wang Office provides the capability to transfer mail packages, including WP+ documents, memos and files, to other users within a local Wang network. A Wang product called VS Office Connection (VOC) is designed to permit the exchange of mail between two distinct Wang Office local networks. VOC formats mail generated by Wang Office users into VS files and places the files into asynchronous driver ques for delivery across the wide area network.

The Wang VS system provides adequate capability to send and receive text messages. However, the Wang proprietary E-mail platform lacks the flexibility to incorporate advancements in technology and is incompatible with customer, contractor, and supplier E-mail platforms. Flexibility is a critical feature of a successful network mail system. The rate of change in the computing environment has been exponential over the last five years, with corresponding changes in the demands made on telecommunications networks to provide standard E-mail services. The result is an industry wide migration towards standards based E-mail systems to facilitate interoperability between supplier, customer, vendor, and contractor E-mail systems enhancing information exchange. Unlike the proprietary Wang system, a standards based mail system enables a modular building block approach accommodating incremental change and technology expansion.

File Transfer Services

Wang Systems Networking (Netcore) is used to transport Wang Office files over the wide area network. It is also implemented for file transfer in the local area network. Wang Systems Networking (File Transfer Manager) provides the queuing and control mechanism for the transfer of Wang files over Netcore.

The file transfer system is limited to Wang Office file transfers. Word processing documents other than Wang Office WP+, engineering design, CAD/CAM, and graphics files, for example, can't be sent through the network. Once again, a standards based file transfer system would furnish flexibility to implement advancing technology.

Directory Services

Wang Office Directory Services software provides the Wang Office directory interface and directory structure. The software enables manual entry and synchronization of the local network directories. However, all directory changes must be "ferried" by the Network Administrator to all remote networks for inclusion in the remote local directory. Wang Office Directory Services establishes a system addressing scheme to route user to user Wang Office messaging.

In the process of doing business, it is often necessary to expand through the acquisition of another company. Alpha Beta Corporation has done so several times. Unfortunately, the Wang Directory Services structure is proprietary. It is not possible for Wang Directory Services to incorporate or interoperate with any other directory structure. A successful network directory service must be flexible enough to accommodate unexpected developments without requiring wholesale replacement of all or large portions of the network. Directory services must be able to expand or contract incrementally in response to customer demand with minimum disruption of ongoing network operations.

Network Management Services

Currently, there is no capability for network management or network monitoring installed in the ABC network. A system audit capability provides hard copy output recording system errors and file transfers.

Today's networks are increasingly becoming more complex, while management staff is decreasing. This means less people are having to manage more networks. Network management tools are essential to effectively manage information technology assets and personnel time. Standards are evolving in such a way that they are merging toward the same goals.

Supporting Technology

This section examines the technology implemented to support the services described in the previous section. The discussion focuses on the Wang wide area network X.25 communications architecture.

The Wang VS communication technology is based on the CCITT packet-switching standard X.25. X.25, the best known and most widely-used protocol standard, specifies the interface rules and regulations between the ABC network data communications equipment (DCE) and the attached data terminal equipment (DTE). The X.25 standard specifies three levels of communications technology; the physical level, the link level and the packet level. The physical level, CCITT X.21 standard, defines the physical, electrical, mechanical, and functional signal transmission characteristics of the data bit stream. The link level, IEEE 802 High Level Data Link Control (HDLC) standard, provides data encoding, switching and transmission control techniques for single or multiple communications links. Finally, the packet level, referred to as X.25, provides some end to end delivery reliability and error detection capabilities. [1]

X.25 based communications networks consistently provide reliable service. However, advancements in technology are challenging the capabilities of X.25 networks. Take for example, multimedia applications. The integrated use of both text and images in the same program or desk top presentation is a simple form of multimedia application that is in common use today. Most large organizations have separate facilities for video teleconferencing and the integration of full-motion video, text, data, and still imagery is gaining increasing attention. These true multimedia applications are increasingly becoming important in business and government realms to enhance productivity. Multimedia provides the ability to enhance the learning process by seeing, hearing, and doing work simultaneously. Accordingly, multimedia will be to the 90's what the PC was to the 80's, with a "multimedia revolution" already visible on the horizon. As a result, X.25, implemented in 1976 and revised in 1980 and 1984, is being replaced with advanced modular switching, signaling, and transmission techniques capable of handling multimedia data rates ranging from 1.544 megabits to 1.2 gigabits per second.

Identification of Technical Alternatives

The objective of this section is to identify technical alternatives capable of satisfying the needs outlined in the Definition of Needs section. Key service and technology alternatives are examined in the Emerging Services and Technology sections respectively.

There are numerous national and international organizations formed for the primary purpose of defining standards for various aspects of automated information systems. In order to reach a goal of an open system that can be implemented with heterogenous commercial products, it is necessary to carefully select standards that are not only mutually supportive and interoperable, but are endorsed and supported by a broad cross-section of industry. Therefore, it is essential to establish selection criteria to evaluate the costs and benefits of possible standards alternatives. The selection criteria should include functional requirements and industry support. A baseline set of criteria used to evaluate the standards addressed in the Emerging Services and Technology sections are presented in the following paragraphs.

Technical Criteria - Functionality, Compatibility, Stability

Functionality is a measure of the extent to which the standard meets the functional requirements defined for the specific service application. Compatibility considers interoperation with existing standards. The Stability criterion evaluates the standards technology base and capabilities state of development.

Market Factor Criteria - Level of Consensus, Availability, Supportability

Level of Consensus considers the extent to which a standard has been adopted by national and international standards making organizations and by commercial industry. Availability measures the variety of products available from multiple vendors to implement the standard. Finally, supportability evaluates the level of support available from primary hardware vendors with products capable of implementing the standard.

Emerging Services

This section examines the emerging services capable of satisfying ABC communications system needs. The discussion focuses on the primary services required of all effective communications networks. These services include electronic mail (E-mail), file transfer, directory, and network management services. A summary and recommendations section is included concluding each service description.

Electronic Mail Services

Standard E-mail services consist of text-based, store-and-forward messages. However, the growing number of E-mail users on the Internet have demonstrated the importance of E-mail as a means of multimedia information exchange. Already, computer mail applications exist that allow image, audio, and video clips to be attached to text messages or to be sent as the message itself. Video mail will have importance in sales and marketing as well as in engineering and technical design arenas. Today, an electronic mail system must incorporate multimedia technology. E-mail systems capable of providing multimedia services are commonly referred to as message handling systems.

Message Handling Systems (MHS)

Electronic message handling system standards have been around almost as long as E-mail itself. Two emerging E-mail standards, X.400 and Multipurpose Internet Mail Extensions (MIME), are described here. These standards address the incorporation of multimedia technology in electronic messaging. This section compares the virtues and liabilities of the X.400 and the Simple Mail Transport Protocol (SMTP)/MIME multimedia standards, and provides support for the conclusion that the X.400 standard will prevail as the E-mail standard of choice over networks employing Transmission Control Protocol/Internet Protocol (TCP/IP).

A MHS consists of four interconnecting components; a User Agent (UA), a Message Store (MS), a Message Transfer Agent (MTA), and an Access Unit (AU). The Message Store provides storage for mail messages. The User Agent allows users to access the MHS. The Message Transfer Agent is the heart of the MHS providing the store-and forward transfer function. Finally, the Access Unit provides connections to other communications systems. Figure 4 illustrates a Message Handling System (MHS).

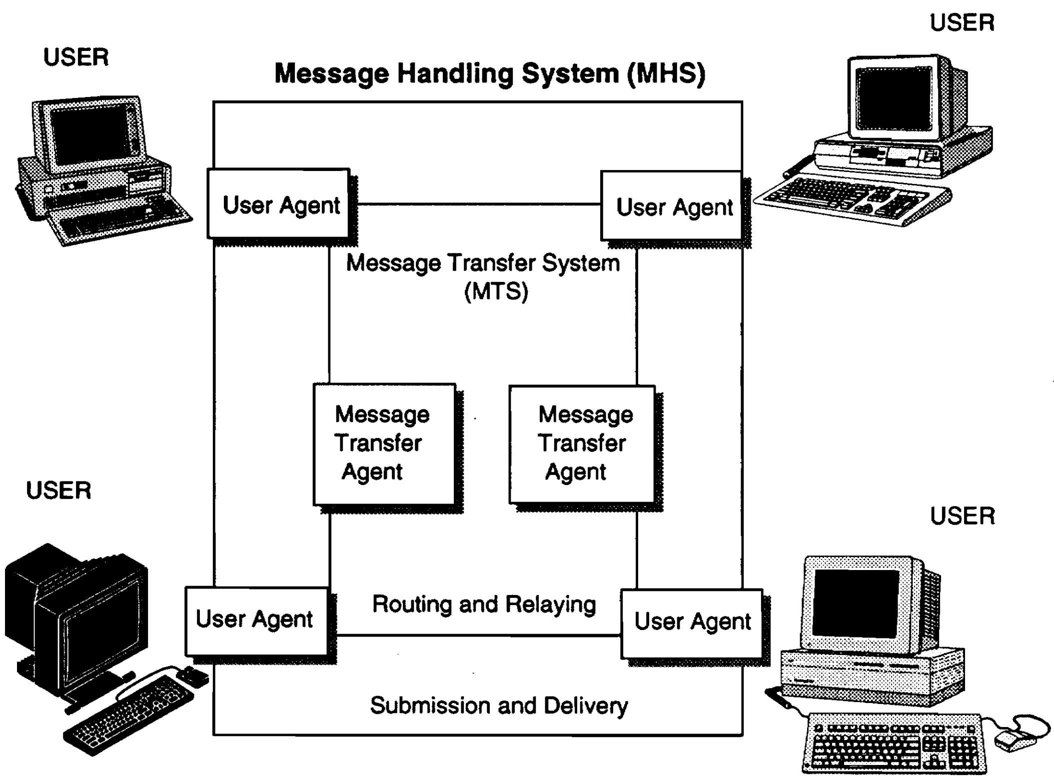

Figure 4. Message Handling System (MHS).

Two standards-making bodies, the International Telephone and Telegraph Consultative Committee (CCITT) and the Internet Advisory Board (IAB), have developed standards for MHS's. CCITT has published the X.400 set of standards, while the IAB developed the MIME specifications that are set forth in RFC 1341. The X.400 recommendations describe specifications for all four components of an MHS. The IAB recommendations specify SMTP as the MTA and MIME as the message format for the Internet. The Internet standard assumes that the other three MHS components are provided by computer operating systems. RFC 1341 defines an additional set of message formats for SMTP. The following sections present summary descriptions of the X.400 and MIME standards.[2]

The X.400 Message Handling System Standard

The CCITT published the X.400 MHS draft standard in 1984 and defined it as a layer 7 specification in the Open Systems Interconnection (OSI) Seven-Layer Reference Model. The OSI Model is a concept for open systems computing and network design that employs layers. Each layer has strictly defined interfaces with the layers immediately above and below it in the OSI protocol stack. This layered approach promotes the interconnection of heterogeneous systems.

Since true network implementations of the OSI protocol stack do not yet exist, the X.400 E-mail standards have been implemented on other types of networks, such as TCP/IP and X.25. RFC 1006 specifically sets forth procedures for the implementation of X.400 over TCP/IP.

The CCITT X.400 committee reconvened in1988 and produced the more robust X.435 standard that includes security-related protocols, EDI support, and multimedia messaging formats. Unless specified otherwise, the X.400 standards referenced throughout this document are based on this1988 specification.[2]

X.400 Security

The X.400 standard supports a number of security features. User authentication, which supports verification of sending and receiving parties, is a major feature. Error checking is also performed to ensure that messages are not altered in transit. Message confidentiality is ensured through optional encryption. Finally, non-repudiation, which allows a third party to verify the message was sent and received, is also supported.

X.400 Multimedia Support

The X.400 standard allows for the transmission and exchange of multimedia messages that can include ASCII and non-ASCII text, audio, voice, images, and data.

X.400 Routing Services

X.400 implementations on Internet TCP/IP networks currently use static routing tables. A standard exists to use the Domain Name System (DNS) for X.400 routing. However, when the global X.500 directory services described later in this document become available, X.400 will be able to use them for routing and mail delivery.

X.400 Products

International Standards Open Communications Resources (ISOCOR) has announced the availability of a suite of end-user products based on OSI protocols. These include X.400 E-mail, EDI, and X.500 directory services. ISOCOR also announced an E-mail gateway that allows coexistence between the OSI X.400 E-mail and the popular SMTP standards for E-mail. Soft*Switch developed an X.400 E-mail gateway that allows users to link different types of messaging systems to others that support the X.400 standards.

Finally, useful software exists in the public domain. For example, Point to Point (PP) is an MTA designed to run under UNIX and is oriented toward full X.400 compliance. It supports all MTA service elements specified in both the 1984 version and the 1988 version of X.400, while also supporting SMTP and RFC 822 protocols. It handles this by converting between X.400 and RFC 822 message structures. It incorporates multimedia message handling and can use either X.500 directory services, DNS, or static routing tables. [3]

The SMTP/MIME Message Handling System Standard

Simple Mail Transfer Protocol (SMTP), as its name implies, is a simple protocol that employs only 14 commands. The vast majority of UNIX systems networked with TCP/IP protocols use SMTP, in addition to the rules for formatting messages set forth in RFC 822.[4]

Security

The SMTP as described in RFC 821 does not employ security specifications. Additional Internet standards that add security on top of the SMTP standard have been developed. These are described in RFC's 1113, 1114, and 1115 as Privacy Enhanced Mail (PEM). Security issues addressed in PEM include message encryption, message authentication, and public key certification.

SMTP MultiMedia

The SMTP standards set allows for the storing and forwarding of ASCII-only text. MIME, the new Internet draft standard described in the following paragraphs, has been developed to allow the transmission of multimedia messages over SMTP. This new draft standard is currently referenced as RFC 1341.[4]

SMTP Routing Services

SMTP uses either DNS or static routing tables to provide mappings between hosts and network addresses. SMTP will be modified to use X.500 directory services when they are deployed. Another RFC will be published to describe the mappings between X.500 and the current SMTP routing services.

SMTP Products

Most versions of UNIX have E-mail message handling systems compatible with SMTP standards. There are also many Disk Operating System (DOS) and OS/2-based E-mail products that can read and write SMTP messages via gateways to the Internet.

Multipurpose Internet Mail Extensions (MIME)

MIME is a message format specification based on SMTP protocols that can be implemented easily over existing, widely-deployed standards.

MIME Security

Like SMTP, MIME E-mail messages can be protected using the PEM standards. MIME does not address any additional security capabilities.[5]

MIME Multimedia

MIME specifies the following three new header fields that allow for multimedia message transmission: MIME-Version, Content-Type, and Content Transfer-Encoding.

The "MIME-Version" header field determines whether a message complies with the version of MIME on the recipient's system. If the message lacks the field, the E-mail application knows the message originated from a system lacking the MIME standard and processes the message accordingly.

The "Content-Type" header field is used to label the message content as something other than ASCII text. Image, audio, video, message, application, and multipart body types can be specified using the Content Type header. Each of the types can also specify "sub-types" that indicate a specific media format or program in the body of the message.

The third header field is "Content-Transfer-Encoding." This specifies the technique used to encode the data so that it passes correctly through other mail transport mechanisms that may have character or data set limitations.[6]

MIME Routing Services

MIME/SMTP currently use DNS and static routing tables in lieu of directory services. When X.500 directory services become widely deployed, SMTP will have the capability to make use of this standard for mail routing.

MIME Products

Bell Communications Research (Bellcore) recently released version 2.2 of Metamail. Metamail is simply an add-on software patch to UNIX systems running E-mail based on SMTP. Bellcore hopes to pave the way for future E-mail innovations and is therefore offering Metamail in the public domain on Internet. Bellcore is also testing another MIME-based product, which should reach the market later this year.

Also in the public domain, PP (described above under X.400 Products) will incorporate MIME functionality later this year, according to its author, Steven Kille. Marshall Rose's new version of his public domain software, MH, and Mark Crispin's latest release of IMAP currently use MIME for multimedia messaging.

In the marketplace, Innosoft Corporation has released a MIME-based E-mail distribution and routing application named PMDF for Digital's Virtual Memory System (VMS) operating system. Other vendors have also announced plans to release MIME-based E-mail products this year.[7]

E-mail Recommendations And Summary

The X.400 standard is recommended as the E-mail standard of choice over networks employing Transmission Control Protocol/Internet Protocol (TCP/IP). Overall both standards are very capable and accepted. This explains why SMTP/MIME and X.400 are primary considerations for E-mail standards. However, the supportability of the SMTP/MIME standard is questionable. Although MIME makes multipart messages mailable, it doesn't automatically mean your systems are ready to handle MIME. There are no MIME compliant user agents available to support MIME. Systems frequently lack the hardware capability necessary for MIME applications. Also, only one MIME user agent and one MIME gateway are being developed. At the same time, the Government Open Systems Interconnect (GOSIP) X.400 directive has accelerated X.400 development and industry acceptance. A second X.400 development strength is the complementary X.500 suite of directory service standards.

Over the next five years, SMTP may remain the basis for some E-mail systems, particularly on the Internet, and the MIME extensions will be used for multimedia messaging. However, X.400 will continue to be used for messaging applications with accelerated development and international acceptance. The X.400 standard is becoming the true OSI future mail standard.

File Transfer Services

Two emerging file transfer standards, Electronic Data Interchange (EDI) and Continuous Acquisition and Life-Cycle Support (CALS) are described here. These standards address file transfer standards for electronic messaging. This section compares the virtues and liabilities of EDI and CALS standards, and provides support for the conclusion that the CALS standard will prevail as the file transfer standard of choice.

Electronic Data Interchange (EDI)

The American National Standards Institute (ANSI) Committee X.12 is responsible for developing EDI standards to encode and exchange business data. These standards specify the formats for the electronic exchange of information within specific industry contexts. For example, the ANSI Transportation Data Coordinating Committee has defined standards for the bills of lading, packing slips, purchase orders, confirmations, etc. used by the transportation industry. Other committees are setting EDI standards for the grocery industry, insurance companies, banking, and other industries.[8]

The real value of EDI is realized with electronic data transmission. EDI data exchanges can be treated as E-mail messages, an approach that takes advantage of E-mail systems already in place. In message handling systems, a user agent places a message in an electronic envelope that is relayed through a series of MTAs for delivery to recipients. The MTAs look only at the envelope to make their routing decisions; the envelope can contain any kind of data, within limits.

Using an application-level protocol such as X.400 has certain advantages over using lower-level protocols on X.25 networks. System security and administration are improved and the use of X.400 allows the same EDI document to be sent to multiple recipients simultaneously.

Recent additions to the X.400 standard have increased its utility for EDI transmission. X.435, which was published in 1990, defines standards for "EDI Messaging System and Services." It defines a new message content type labelled P35. The P35 content type consists of a heading and a body. The heading contains several data fields, such as the name of the sender, the recipient, and a time stamp. The body contains the EDI data and may be divided into several components containing different data types. For example, one part might be an invoice, another an engineering diagram, and another a data sheet. The data types of the different components are recorded, allowing recipients to search for specific data types within messages. The X.435 specification also enhances X.400 reliability and security by defining a set of receipt notices. These notices include positive, negative, and forwarding notices, and the specification describes when and how each should be used. X.435 also allows EDI information to be exchanged between applications without manual intervention. For example, data contained in an EDI message could be entered automatically into a database upon receipt.

EDI applications are being actively developed by a number of Government agencies, including the Internal Revenue Service, the General Services Administration, the Veterans Affairs Department, the Customs Service, and the Environmental Protection Agency.

The Department of Defense (DOD) adopted EDI as a policy in 1988 and about 100 EDI projects are currently underway. Ultimately, all proposals, purchases, receipts, invoices, and bills of lading are supposed to be exchanged electronically with DOD suppliers. So far, DOD purchasing and logistics message formats have been converted to X12 variable-length formats, and transaction sets have been submitted to the ANSI Accredited Standards Committee for adoption as X12 standards. The DOD is also working with NIST to develop a FIPS for public key encryption. These efforts require considerable interaction with industry representatives because most of the anticipated EDI traffic will occur not within DOD agencies but between those agencies and industry contractors.[8]

Continuous Acquisition and Life-Cycle Support Standards

EDI functionality conforms closely to the goals of the DOD's Continuous Acquisition and Life-Cycle Support (CALS) program. A dramatic increase in DOD technical documentation led to development of the CALS program, which is designed to replace paper documents with electronic documentation and information distribution. The CALS program began as a joint DOD and industry effort in 1985. CALS objectives include reduced lead times, reduced costs, and greater efficiency in systems acquisition, manufacturing, research and development, and logistics. These objectives are to be attained by replacing paper-based technical documentation with computer-based databases and by distributing data in digital format on electronic media. Ultimately, CALS implementation will enable contractors and DOD agencies to engage in interactive videoconferencing and online electronic modification of charts and drawings.

A primary CALS activity is development and promotion of standards and specifications that will ensure interoperability and compatibility among industry and DOD automation equipment and information distribution systems. Specific attention is being paid to industry standards and technological developments for incorporation into the CALS standards. This approach allows the DOD to take advantage of the economies inherent in using COTS hardware and software and ensures that the resulting standards do not obsolete contractor investments in automation systems.

CALS standards and specifications implement existing and emerging national and international standards and are the result of extensive coordination between the National Institute of Standards Technology (NIST), National Science Industry Association (NSIA), Automakers Industry Association, Electronic Industry Association (EIA), and user groups such as Manufacturing Automation Protocol (MAP), and Technical Office Protocol (TOP). The standards described in the following sections are the principal components of CALS and are subject to continuing review and revision.[9]

MIL-STD-1840A

This standard, titled "Automated Interchange of Technical Information", is the parent document for a family of military specifications through which the CALS standards will be published. It provides the "enveloping" rules for organizing files of digital data into a complete document, such as a technical manual composed of MIL-M-28001 text, MIL-D-28003 vector graphics, and MIL-R-28002 raster graphics.

The 1840A standard is currently undergoing revision and is expected to be replaced by version 1840B in the spring of 1994. The draft 1840B document adds CD-ROM and MS-DOS diskette formats to 9-track tape as acceptable media for the distribution of CALS data. Other recommended additions include acceptance of the IP, TCP, and FTP formats from the Internet suite of protocols for CALS communication networks.[10]

MIL-D-28000A (Amendment 1)

This standard, titled "Digital Representation for Communication of Product Data: IGES Application Subsets," defines subsets of the Initial Graphics Exchange Specification (IGES) for technical illustration, engineering drawings, electrical/electronic applications, and numerical control manufacturing. IGES is a neutral format for the digital interchange of Product Definition Data between dissimilar computer-aided design systems.

MIL-M-28001A (Amendment 1)

This standard, titled "Markup Requirements and Generic Style Specifications for Electronic Printed Output and Exchange of Text," defines standard DOD requirements for each step involved in the automated publishing of page-oriented (i.e., printed) technical publications. For exchange of source data (prior to document composition), it defines a common implementation of the Standard Generalized Markup Language (SGML). For composition processing functions, it defines an Output Specification of typographic tags and format rules. For display of the composed document, it provides options for use of commercial Page Description Languages (PDLs).[11]

MIL-R-28002A

This standard, titled "Requirements for Raster Graphics Representation in Binary," defines DOD technical requirements for raster (bit-map) graphics that have been compressed to reduce file size and transmission time. CALS must apply raster graphics to both office documents and facsimiles, and for engineering drawings and other oversize documents. An option is included to use tiling, in which the raster image is divided into a series of tiles that can be individually processed to reduce throughput and terminal storage requirements.

MIL-D-28003A

This standard, titled "Digital Representation for Communication of Illustration Data: CGM Application Profile," defines use of the Computer Graphics Metafile (CGM) for two-dimensional vector (line segment) picture descriptions or illustrations in technical manuals. Whereas IGES has its principal use within computer-aided design, CGM is becoming widely available for authoring and graphic art work stations.[12]

Other CALS Standards Initiatives

Additional CALS standards under development include the Interactive Electronic Technical Manual (IETM), which is designed to replace paper technical manuals with contractor-maintained databases that are accessible over telecommunications networks and that can be distributed on electronic media. Initial efforts include the use of a variety of authoring software packages that provide interactive text search and image handling capabilities using optical storage media.

In a parallel development, the Contractor Integrated Technical Information Service (CITIS) specification will define the structure of a contractor-maintained database that will contain all drawings, reports, test procedures, test requirement documents, Logistics Support and Analysis (LSA)/LSA Records (LSAR) data, and technical publications relating to a specific procurement. Subcontractors and the Government will have either read/write or read only online access to the database.

CALS Products

CALS Products emphasize the digital capture, transfer, and delivery of text and graphics in conformance with the MIL-D-2800X series of specifications. The increased graphics capabilities of workstations should stimulate industry interest in the CALS IGES and CGM standards for graphics representation.

Demand for the addition of audio and video data to technical documentation is anticipated as multimedia applications mature. The video/image industry is advancing toward integration of voice, video, graphics, and images all in one "box." The goal is to be able to capture video, edit it, and electronically mail it. In the area of standards, video transmission formats are in transition from traditional analog techniques to new digital technology. Also in transition are proprietary compression and decompression algorithms that are giving way to International Standards Organization (ISO) and Telephone and Telegraph Consultative Committee (CCITT) standards. The Joint Photographic Experts Group (JPEG) and the Motion Picture Experts Group (MPEG) standards are displacing proprietary algorithms in stored interactive video applications. The term "Joint" in the title of JPEG emphasizes that JPEG is a collaboration between CCITT and ISO.[13]

Video/Image Transmission Formats

Digital video will be transported at various resolutions and bit rates over various channels connecting computers and television receivers. Advances in display technology are needed along with standards for interoperability among these differing systems. The existing formats for analog television are National Television Standards Committee (NTSC), Phase Alternating Line (PAL), and Sequential Color And Memory (SECAM). NTSC is the current standard for television. Proprietary and standardized digital formats that have the capability for digital imagery and full motion video are in use today. Examples are Intel's Digital Video Interactive (DVI), Phillips' Compact Disk Interactive (CD-I), and Kodak's Photo-CD. The High Definition Television (HDTV) format is a new standardized format that many industry experts believe will unseat NTSC as the industry standard for common television receivers. Other video formats for lower resolution transmission include Common Intermediate Format (CIF) and Quarter Common Intermediate Format (QCIF).

File Transfer Services Summary and Recommendations

EDI was formally made a part of the CALS program in 1991. The incorporation of EDI into the CALS standards and the inclusion of TCP/IP standards makes extensive commercial offerings of these protocols available to the CALS community. The danger inherent in any standards-making process is that the standards will inhibit further technological development. CALS standards-making, however, appears to be an evolutionary process with considerable industry input. If that process continues, the CALS standards should be flexible enough to accommodate technological innovations and evolving user needs.

Directory Services

A directory or naming service is a necessary part of any computer and communications network. Every computer and communications component within a network needs a name and those names must be mapped onto corresponding addresses in a lookup table or directory. This type of service is essential for any activity involving interactions between two or more components, such as E-mail, file transfers, inter-process communications, and network management.

A number of naming technologies and approaches have been developed for specific applications. The primary examples are the Internet's Domain Name Service (DNS), which is used on the Internet to provide mappings between hosts and network addresses, and CCITT's X.500 Directory Services standards. This section examines DNS and X.500 standards, and provides support for the conclusion that the X.500 standard will prevail as the directory service standard of choice.

Domain Name Service (DNS)

DNS is a standard TCP/IP protocol suite application layer service that associates information with objects. DNS obtains and provides information about hosts on a network by querying and answering queries. Domain Name Service performs naming between hosts within your local administrative domain and across domain boundaries and is distributed among a set of servers commonly called name servers. At the client, the service is implemented through the resolver, which resolves user queries. The resolver must know the address of at least one name server to resolve queries and distribute network data. DNS names have hierarchial organization, consisting of domains nested within one another. The DNS hierarchy reflects your place in the overall domain structure and provides guidelines for naming other domains, hosts and zones. A zone is a hierarchial community of hosts administrated by a single authority and served by a set of name servers. The root of the DNS hierarchy is controlled by the Network Information Center (NIC). Each domain must have a unique name and be properly registered within its level of network hierarchy. DNS establishes the mechanisms and controls to provide mappings between hosts and network addresses.[14]

The X.500 Functional Model

In the X.500 model information objects are represented by entries in the Directory Information Base (DIB). Entries consist of one or more attributes and each attribute consists of an attribute type with at least one value for that type. An attribute's type defines the characteristics of the attribute, compares the characteristics of two or more attribute values, and determines if more than one attribute value is to be allowed.

An entry is named hierarchically according to its position in a Directory Information Tree (DIT). The unique name for an entry, which is called its Distinguished Name (DN), is formed by tracing a path from the root of the DIT to the entry and adding the Relative Distinguished Name (RDN) at each branch. For example the DN of the operations manager at ABC might be; countryName "US", organizationName "ABC", Unit Name "Operations", commonName "Manager".

The global X.500 DIB is designed to be distributed among different locations. For example, different companies, organizations, or geographic regions could maintain their own local X.500 DIBs, which would be tied together by a global network to form the global X.500 Directory. Each DIB has a Directory Service Agent (DSA), which is responsible for processing search requests, directory updates, and other operations. Users looking for an address access the Directory by means of their own Directory User Agent (DUA), which connects with a local DSA. Figure 5 shows a diagram of the X.500 functional model. The DSA can search its own DIB

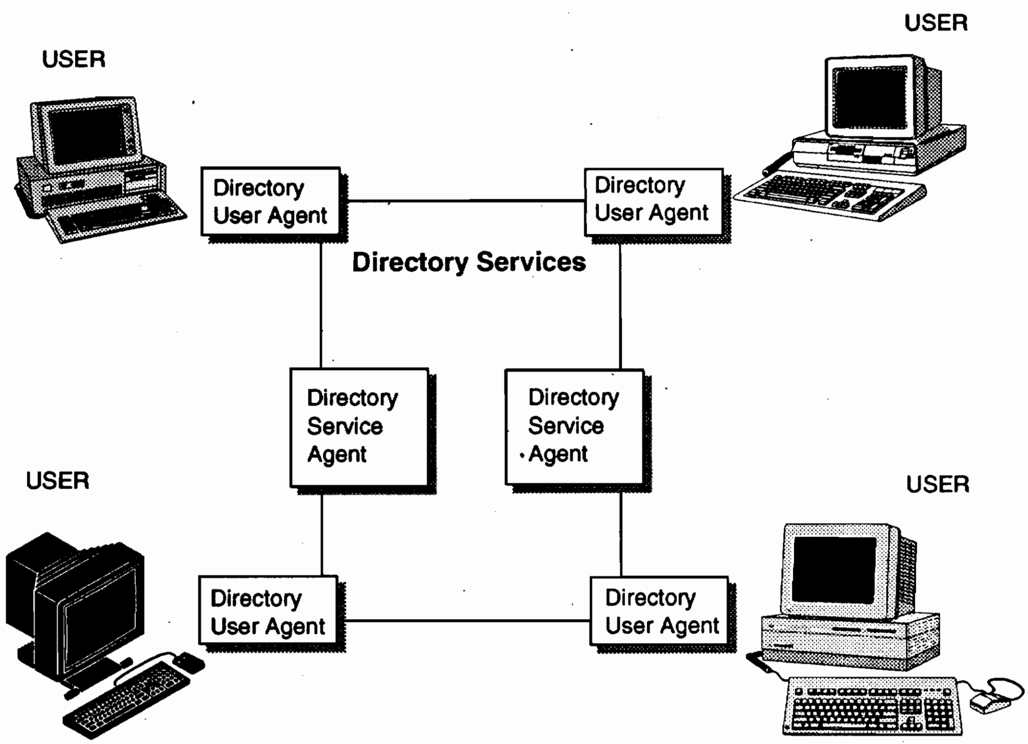

Figure 5. X.500 Directory Service Model

but does not have direct access to other DIBs. If the information requested is in another DIB, the DSA may refer the DUA to another DSA that has the information. Alternatively, information may be passed internally between DSAs and passed on to the DUA through the local DSA.

An international group of researchers created an X.500 service named Paradise, which consists of more than 360 DSAs in 28 countries. The number of entries in the Paradise directory has increased during the past year from 310,000 to more than 800,000. Universities operate most of the Paradise DSAs, but a number of corporations and government entities also use the directory.

The 1988 X.500 standard does not deal specifically with authentication, authorization, access control, or other security issues. The North American Directory Forum has led the effort to include a greater number of security features in an updated version of the X.500 standard that will reportedly provide a full set of access control features.[15]

Directory Services Summary and Recommendations

The DNS approach works well within centrally controlled networks, but the growing emphasis on open systems and distributed networking favors implementation of the CCITT X.500 series of recommendations. X.500 has strong acceptance within the commercial industry as the future directory service standard. The X.400 protocol suite complements X.500 implementation strengthening both standards. Unlike other directory services, X.500 is infinitely scalable and allows public directory services and corporate directories to be linked to form a single, global distributed directory. A research group at University College London developed and tested a complete implementation of the OSI Directory based on the 1988 X.500 recommendations. It has been tested by groups in the United States, Europe, and Asia and is considered the directory standard for open systems interoperable networks.

Network Management Services

The accelerating growth and complexity of communications networks necessitates implementation of network management tools. This section provides a summary of the primary commercial-off-the-shelf (COTS) network management products, and provides support for the conclusion that the Simple Network Management Protocol, SNMP, standard will prevail as the network management protocol standard of choice.

Network Management Products

The capabilities of five primary network management software packages are summarized. The packages include; Sun's SunNet Manager, Hewlett Packard's OpenView, AT&T's Accumaster Integrator, Lexcel's Lance+, and Harris's Interactive Networking Tools (HINT). Hewlett Packard's SNMP based OpenView product is recommended as the overall best network management product.

Sun's SunNet Manager

Sun's Sun Net Manager is a Simple Network Management Protocol (SNMP) based local area NMS that runs on a Sun platform (UNIX operating system). SunNet Manager uses Sun's Openlook graphical user interface. It has autodiscovery capabilities and features customized maps. It also includes a DBMS for historical traffic and event reporting, and it has traffic analysis and histogram tools. Users can download over 30 precompiled MIBs from an E-mail server free of charge.

Hewlett Packard's (HP) OpenView

OpenView runs on HP, Sun, and IBM workstations over the UNIX operating system. OpenView is also available in DOS format for PCs. It uses the OSF/MOTIF graphical user interface and employs INGRES as its database management system (DBMS) for reporting and storing historical network data. It also has a MIB compiler to create a management information base for network nodes that do not already have the MIB information, as well as the capability of importing third-party MIBs (i.e., MIBs already resident on a node). In addition, traffic reports and histograms can be generated and management functions are segmented to enable network management systems to communicate and manage each other.[16]

AT&T's Accumaster Integrator

AT&T has its own network management protocol that provides a common means of communicating the information and instructions needed for integrated, end-to-end, multidomain network management among the systems it manages. Alarms are monitored through an Element Management Systems (EMSs), and Accumaster can detect the most probable cause in a multipoint failure. AT&T has EMSs with expert system capability to automatically analyze faults, initiate repairs, and clear alarms. Accumaster can talk to SNMP-based EMSs through an interface, thus allowing the management interconnectivity of several SNMP-based LANs.

Accumaster can handle up to 12 EMSs and 30,000 managed objects. It uses an Informix DBMS and allows for security through partitions of network duties.

Lexcel's Lance+

Lexcel's Lance+ is a LAN management system built for Sun (UNIX operating system) and VAX (VMS operating system) platforms. Lance+ features a hierarchical map, traffic statistics, and reports over an X-Windows-based graphical user interface. Lance+ can also create MIBs with its MIB compiler, or it can import third-party MIBs. In addition, Lance+ can store historical data through its own DBMS. Finally, Autodiscovery will be featured in a release later this year.

Harris Interactive Networking Tools (HINT)

The final NMS product discussed here is the Harris Interactive Networking Tools (HINT) from the Harris Corporation. Harris' HINT is a wide area SNMP-based Enterprise Manager sold as value-added software bundled with the networking devices developed by Harris. HINT runs on Pyramid, Sun, and Intel 386/486-based platforms (UNIX operating system) and uses MOTIF features over an X-Windows graphical user interface.

HINT performs alarm reporting and incorporates a top-down progression of network maps to aid in pin-pointing the alarms. It also features auto trouble ticketing, which is built into a helpdesk system, and it includes an Oracle DBMS for historical data capture and reporting.

Network Management Summary and Recommendations

The best example of an SNMP based product, HP's OpenView, is an effective monitoring device that provides autodiscovery and hierarchical map drawings of network nodes. OpenView runs on HP, Sun, and IBM workstations over the UNIX operating system and is also available in DOS format for PCs. The other net managers require specific or proprietary hardware/software platforms. Also, Lance+, and SunNet Manager allow SET operations (service primitive to reconfigure device), thereby putting sensitive configuration information at risk if used. Accumaster does not encrypt its network commands, and also has some security concerns. HP implements its "Extensible SNMP" agent, which remotely manages software applications such as print queues and databases. Because HP is deeply immersed in Open Software Foundation's (OSF's) progress on Distributed Management Environment (DME), they have the advantage of being at the forefront of standards and are poised to give their customers these standards this year. Many other companies, such as Network Equipment Technologies (NET), license the HP OpenView software and sell it under their own product name. NET's SNMP Manager is precisely this, and NET plans to migrate to the new standards along with HP. Even the ATM Forum has endorsed SNMP as the interim local management interface for high speed networks based on ATM transmission. Network management standards will move towards SNMP the network management standard.[16]

Supporting Technology

This section examines the telecommunications technology capable of handling ABC communications system needs and advanced services addressed in the previous sections. The discussion focuses on two key emerging telecommunication technologies, Distributed Systems and Asynchronous Transfer Mode switching.

Distributed Systems

Network technologies that were expected to meet demand for the next 10 years are becoming obsolete only a few years after they are introduced. Some network demands that will be made over the next five years can be predicted, while others can only be surmised. Future network architectures cannot rely on technological solutions that require forklift upgrades every few years. Modularity is an essential feature of a communications network architecture. Network planners cannot afford to let local distribution bandwidth limitations inhibit the introduction of new desktop applications. The network architecture must minimize the choke point created by the interface between local distribution and long distance transport networks. One way to overcome this limitation may be to extend backbone technologies and protocols to the desktop, eliminating the distinction between backbone and local networks. This is known as employing a "Distributed System" communications architecture because the processing power of the network is "distributed" to the desktop. Since computer costs are decreasing much more rapidly than communication costs, it makes economic sense to distribute wide area network functionality as close to the user as possible. Also, distributed systems offer component parts or modules that interact through standardized interfaces. This modularity permits incremental growth and the implementation of system upgrades without disrupting ongoing operations. The distributed systems approach provides modularity, built-in redundancy, and tolerance of single-point failures.

Asynchronous Transfer Mode (ATM)

Another area in which wide area network flexibility is of critical importance concerns transmission of the different data types used in multimedia applications. For example, text and numerical data can tolerate a certain amount of network delay, but error detection and correction are critically important. Conversely, video and voice transmission and some real-time telemetry applications can tolerate a certain number of errors without affecting program material, but network delays must be minimized. The network architecture must be able to accommodate varying data requirements by establishing different priorities and different handling procedures for different data types.

Traffic composed of different data types tends to be bursty. The network architecture must be able to allocate bandwidth where and when needed. This requirement is related to the need for efficient bandwidth use. Fiber has been described as supplying almost "infinite" amounts of bandwidth. However, that bandwidth is going to fill up rapidly as multimedia applications put greater demands on the network.

The network requirements described in the previous paragraphs have been anticipated by leading edge communications planners. The CCITT has proposed the Asynchronous Transfer Mode (ATM) as the transport mechanism for Broadband Integrated Support Digital Network (BISDN). ATM has the potential for meeting most, if not all, of these requirements.

An ATM network contains three types of components; the transport, statistical multiplexers, and ATM switching equipment. The transport maps ATM cells into Synchronous Optical Network (SONET) payloads using statistical multiplexers to concentrate signals for more efficient bandwidth sharing. The primary advantage of ATM switches is that they do not use the shared-medium bus architecture that most switches, multiplexers, and routers use today. This type of architecture is adequate for the kinds of data rates used in networks today but will become too impractical to implement as backplane speeds that surpass 1 Gbps.

The ATM format's primary advantage is that the same ATM switch can handle voice, data, image, and video traffic. The minimal processing needed for ATM routing reduces delays through the network, which is particularly important for real-time voice and video transmission. The fixed cell size also reduces delay by simplifying cell processing at nodes and by reducing the number and size of buffers.

A second advantage of the ATM approach is that the use of small cells and the ability to multiplex different types and rates of traffic over the same channel promote more efficient bandwidth use. A third feature of the ATM protocol that enhances its flexibility is its ability to carry a variety of non-standard data rates. The protocol responds to different data rates and bursts of data by sending more or fewer cells.

Finally, ATM terminal equipment will have a simple and flexible design. The same interface unit will receive video, data, and voice traffic and will simply route cells to video, data, and voice processors based on cell service type.[17]

Life-Cycle Cost Evaluations

A high level life-cycle cost analysis provides estimated net present value costs required to implement an ABC communications system architecture based on the recommendations described in the previous section. The cost data enables ABC to consider the rough order magnitude financial commitment necessary for the upgrade during the feasibility evaluation.

The life-cycle cost data were generated through cost analysis of similar sized networks implemented by other companies offering similar services with comparable supporting technology and also through analysis of past and present ABC network costs. The costs are broken down into research and development costs, acquisition costs, installation costs, operation and support costs, and system retirement costs. A five year useful system life-cycle is assumed. Research and Development (R&D) costs over the system life-cycle include an initial year long, eight person, intense effort with continued resources allocated for the system life time. R&D costs also include system prototype development and testing. Acquisition costs are based on estimating message handling system hardware, software and infrastructure costs. Installation costs include labor, transportation, and training during system installation. Operation and support costs include inventory, maintenance, system administration, program management, administration support, and training costs. Retirement costs include system dismantling labor hours, handling equipment, and transportation costs. Figure 6 provides a summary of the life-cycle costs.

R&D Costs $1.4M

Management	$100,000
Feasibility	$50,000
Planning	$50,000
Research	$400,000
Equipment	$100,000
Design	$600,000
Documentation	$50,000
Testing	$50,000

Operation & Maintenance Costs $5.0M

Personnel	$2,100,000
Maintenance	$500,000
Equipment	$200,000
Supplies	$100,000
Training	$50,000
Documentation	$2,000,000

Acquisition & Installation Cost $1.8M

Procurement	$1,100,000
Planning	$50,000
Travel	$40,000
Training	$10,000
Personnel	$600,000

Retirement Costs $55,000

Personnel	$50,000
Handling	$5,000

Total System Cost **$8,200,000**

Figure 6. Projected Life Cycle Costs

Risk Assessments

For any design, an assessment and evaluation of associated risks should be completed. Any consequences or uncertainties involved in proceeding with the recommended design should be documented and communicated to management. This section identifies problems associated with X.400, X.500, ATM, and distributed computing. As with all new technology there is an inherent risk of design and development delays. Cutting edge technology availability is often promised only to end up significantly delayed. Program management should be aware that product availability dates most likely will be delayed and should recognize the need to incorporate delay factors into the design schedule. Also, actual system costs could be much greater than the projected life-cycle costs. This is again an inherent risk associated with implementing leading edge technology. There are hidden costs involved that we simply can not estimate because we are not aware of them.

Problems with X.400 Implementations

The X.400 standard does not cover all that is necessary for routine multimedia messaging. In particular, standard interchange formats have not been agreed upon slowing widespread adoption of X.400 multimedia mail. This means that different vendor products cannot exchange multimedia mail because the formats are incompatible. Without a standard format, users cannot be sure that multimedia mail transmitted between differing vendor products will be readable at the receiving end.

Another not-so-easily-solved incompatibility problem deals with the multitude of OSI lower-layer protocols. X.400 was designed to run over all of them, but this capability could be a problem. X.400 implementations from two vendors that run over two different transport stacks (e.g., connection-oriented X.25 and connectionless datagram services) most likely will not be interoperable. The problem is not in X.400 but in the lower level OSI protocols. RFC 1006, which allows OSI applications to run over the transport layer of TCP/IP, may alleviate this problem in the TCP/IP realm. Until standards for transport protocols under messaging systems are defined and made readily available, X.400 products over OSI could be plagued with incompatibility problems.

TCP/IP and SMTP have a large installed base in the data communications industry and have been universally accepted in the UNIX and Internet community. This could inhibit the acceptance of X.400 over a large industrial base.

MIME defines a standard mechanism for labeling data and combining it into multipart messages rather than defining a standard data format. This simplicity will facilitate quicker adoption of MIME by the SMTP community. The MIME standard alters the "store-and-forward" paradigm of the other E-mail standards. For large objects, such as video or complex imaging, a mechanism exists in MIME by which data are passed by reference rather than by including the whole data object in the message. MIME works because it is simple. It was designed to be compatible with both SMTP and X.400 transport standards.[18]

Since MIME will coexist with X.400 standards, some industry experts believe SMTP-based products using the MIME extensions will initially compete with X.400 products but ultimately will become the standard for multimedia mail.

Problems with X.500 Implementations

The OSI Directory, as defined in the CCITT X.500 Recommendations, does not use distributed database technology for historical and political reasons. It has been argued that, as a result, the X.500 Directory will suffer unduly from consistency problems, naming conflicts, and inefficient query implementations.[19]

Also, the 1988 X.500 Recommendations are incomplete and do not deal with issues such as replication and access control. The 1992/93 extensions focus on these shortcomings, however, industry has been reluctant to commit development time and resources to a standard that may be changed. Some vendors, such as DEC and Novell, have announced X.500 directory services, but these function within proprietary networks and there is no guarantee that they will interoperate with a global X.500 directory service. In Europe, France Telecom has a public X.500 service and several other European companies are using a subset of X.500 to automate cross-border directory inquiries. However, the lack of access control in particular has prevented adoption of X.500 by organizations reluctant to allow access to their local directory from the global network. More specifically, companies favor a directory structure that gives unlimited browsing access to company employees and global access to marketing and sales personnel.

Problems with Network Management

A project to develop an international network management standard is in progress. The International Standards Organization (ISO) is working to develop Common Management Information Protocol (CMIP) and Common Management Information Services (CMIS) protocol suites. The availability of CMIP/CMIS standards is not expected before 1995. HP Openview is a proprietary software package based on the Simple Network Management Protocol (SNMP). ABC should be aware of the possibility of migrating to CMIP/CMIS standards in the long term.

Problems with ATM

While the ATM format can accommodate a variety of different types of program material, this flexibility has a cost. A protocol designed to handle different types of traffic is generally not as efficient as a protocol designed to handle one specific kind of traffic. For example, IBM researchers reportedly feel that ATM uses too much overhead when transmitting SDLC packets. Considerable bandwidth is also wasted by constant-length ATM cells in distributed computing environments. Messages between processors in distributed computing systems are typically only one or two bytes long. The messages must be transmitted quickly and cannot wait for an ATM cell to fill up. Consequently, a 43-byte cell must be used to transmit a one or two byte message.[20]

Problems in Developing Distributed Systems

The most significant difficulty in designing distributed systems is the complexity that results from the interaction of a number of different components, which may produce unexpected behaviors and problems. The causes of these problems can generally be categorized as resulting from interconnection, interference, propagation effect, scale effects, and partial failures.

The interactions of two or more components in a system may exhibit unpredictable and unwanted effects. One example is the software problem that disrupted AT&T's long-distance service several years ago. The SS7 software at one node was not clearing completed calls, which resulted in complete blocking of the node. The problem propagated to other nodes, which brought down most of the system. The Internet was also severely affected a few years ago when an E-mail message was sent instructing nodes to replicate the message and send it to other nodes. This flooded the network. The episode was created intentionally by taking advantage of an idiosyncrasy of the Unix operating system.

Another pitfall in designing distributed computer operating systems is the problem of scaling. While modular hardware components can be added to a distributed system, algorithms used in the operating system or in applications may not scale up with the rest of the system, thus causing a bottleneck. The need to maintain system state and the replication of files and other system resources are only two of the tasks involved in meeting this requirement.[21]

Recommendations

The approach that appears to be the most beneficial to the organization incorporates a strategy that is based on government standards dealing with the various aspects associated with information systems and services. The ABC enterprise message capability will utilize a wide area backbone based on the X.400 standard for global electronic messaging. X.400 is a vendor independent, industry standard for cross-platform messaging and comprises a set of network level protocols within the Open Systems Interconnection (OSI) model. Because of its wide acceptance and implementation across government and industry and government level endorsement, X.400 is the most viable and potentially has the longest life expectancy for electronic messaging. Two additional specifications, X.500 addressing directory synchronization and maintenance standards, and X.509 addressing network security issues, will be incorporated into the enterprise message specification. The long term strategy for the consolidation of electronic messaging services will provide a reliable integrated E-mail transport system and attachment formats. The design goal is to utilize international standards with COTS hardware and software to minimize costs and maximize service support to the users. The implementation of connectivity standards and strategy will facilitate the operation of a single system that will support a heterogeneous user community. Therefore, the ABC communication network information services should also include file transfer systems based on Continuous Acquisition and Life-Cycle Support (CALS) standards which incorporate Electronic Data Interchange (EDI) standards. CALS standards are globally accepted, commercially available, and thoroughly tested. The accelerating growth and complexity of ABC communications networks necessitates implementation of a network management tool. Hewlett Packard's OpenView network management application software package provides the greatest functionality, security and vendor support. These services should be provided using a distributed computing technology approach to provide modularity, built-in redundancy, and tolerance of single-point failures. Asynchronous Transfer Mode (ATM) switching and Synchronous Optical Network (SONET) transmission infrastructures should be implemented to handle the expected voice, data, image, and video communications traffic. Figure 7 provides an illustration of the recommended system.

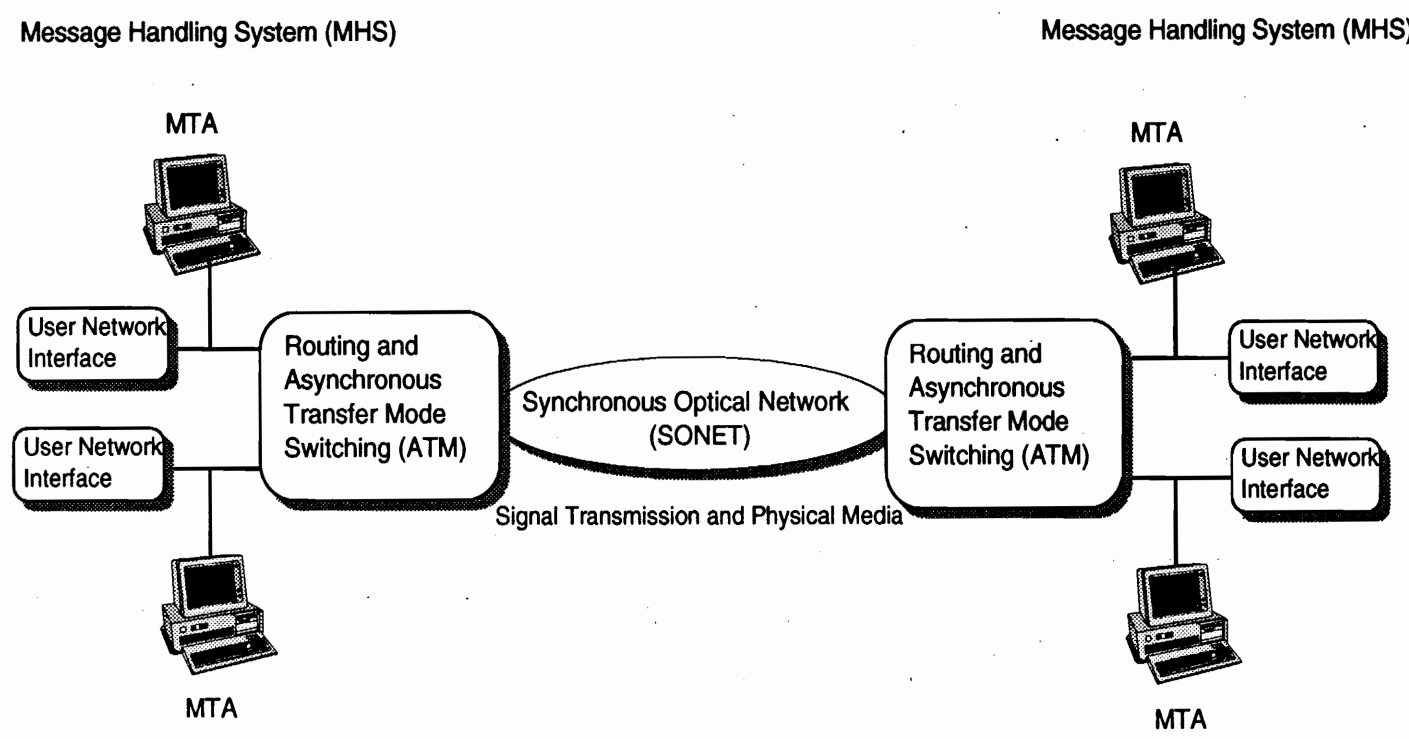

Figure 7. Recommended Design

3.2) Definition of System Concepts

System Concepts

System operation, system maintenance, system logistics and support, and system test and evaluation concepts are presented in the following sections.

System Concept of Operations

The MINWK WAN Mail Handling System conceptual diagram is shown on the previous page in Figure 7. The long term strategy for the consolidation of electronic messaging services will provide a reliable integrated E-mail transport system with standard attachment formats. The MINWK design goal is to utilize international standards with COTS hardware and software to minimize costs and maximize service support to the users. The implementation of connectivity standards and strategy will facilitate the operation of a single system that will support a heterogeneous E-mail community. The MINWK enterprise message capability will incorporate a wide area backbone based on the X.400 standard for global electronic messaging. The complimentary X.500 specifications, addressing directory synchronization and maintenance standards, will also be incorporated into the enterprise message specification. ABC communication network information services will implement file transfer systems based on Continuous Acquisition and Life-Cycle Support (CALS) standards which incorporate Electronic Data Interchange

(EDI) standards. The network management strategy will be accomplished using Hewlett Packard's OpenView network management application software package. Asynchronous Transfer Mode (ATM) switching and Synchronous Optical Network (SONET) transmission infrastructures will implemented to handle expected voice, data, image, and video communications traffic.

Network Operation

A system user sends an E-mail message, with the assistance of a user agent to help address the message in the proper format, to the LAN/WAN interface router. The router sends the message to a mail gateway for translation from its native mail format (if not X.400) into the X.400 standard format. The Message Transfer Agent (MTA) insures the integrity of the X.400 message, and inventories and packages the message for delivery to a remote MTA. Figure 8 shows the expected network utilization.

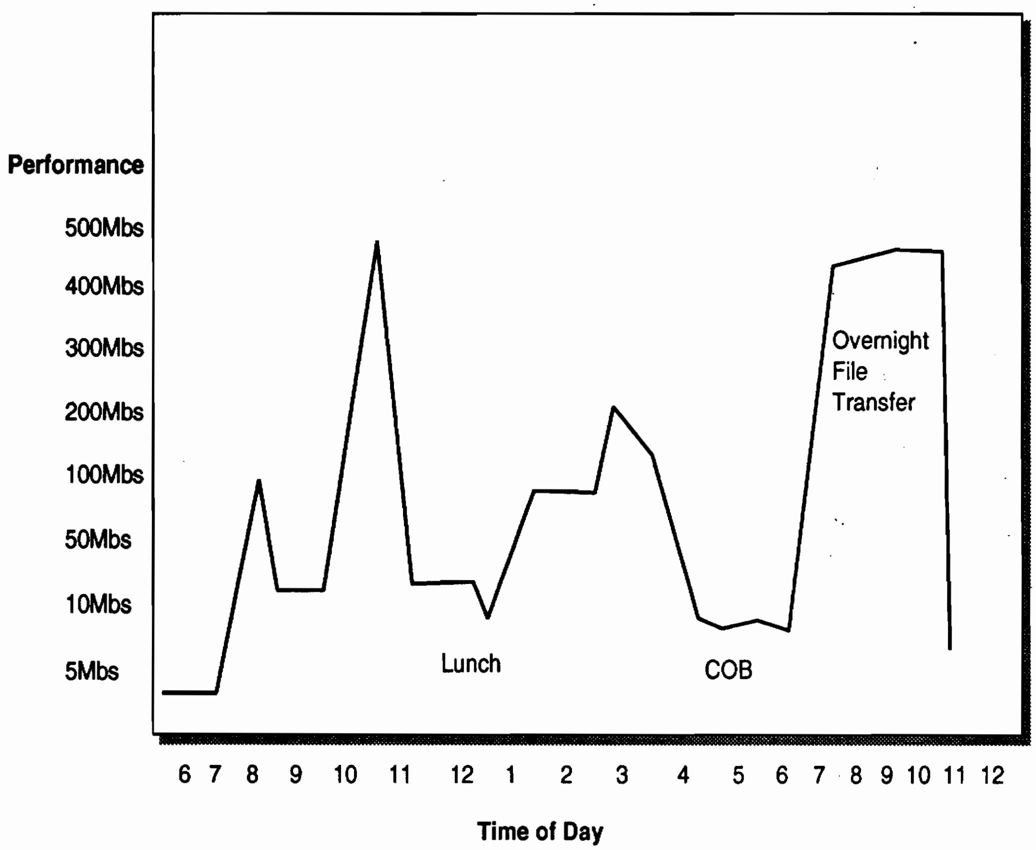

Figure 8. System Utilization

System Maintenance Concept

The MINWK system will be supported with three levels of maintenance: Organizational, Intermediate, and Vendor. MINWK Area Control Center (ACC) personnel are responsible for the organizational level of support which will be provided at each ACC. The Network Control Center (NCC) administrators will be responsible for the intermediate level of support which will be provided both at the ACC's as well as in the NCC lab. The individual vendors of the system's various products will be responsible for vendor level of support which will be provided both on-site and at the vendor's servicing facilities. See Figure 9 for the system operation and support flow. Figure 10 outlines the maintenance concept flow, and Figure 11 describes the major levels of maintenance.

Organizational Support

The organizational support will provide both corrective and preventive maintenance. Preventive maintenance activities include visual inspections of the MTA's, workstations and any peripheral devices attached to the workstations, replace/replenish basic operating supplies, performing system backups, maintaining data/user security, handling user accounts, as well as system software training and assistance. Corrective maintenance activities include limited repair/replacement of workstation and MTA equipment, loading/upgrading workstation software, and reporting any break in the WAN communications to the NCC. The organizational level personnel support all the WAN software and hardware excluding the cable infrastructure. The organizational support will try to isolate system faults and repair the fault if possible. However if further service is required the ACC personnel will contact the NCC personnel or the vendor as appropriate.

Organizational support will consist of two support people for each ACC. One person will provide MTA expertise while the other will provide router and networking expertise. The organizational personnel will require intermediate skill levels emphasizing familiarity with MTA and network hardware and software operations.

Intermediate Support

The intermediate level supports the entire MINWK WAN network. Preventive maintenance activities include optimization of WAN communications and maintaining security of network access. Corrective maintenance activities include network fault isolation to the component level using the network management tool, replacing faulty components when appropriate, network analysis and testing, and some limited calibration. Intermediate level support will consist of two network administrators.

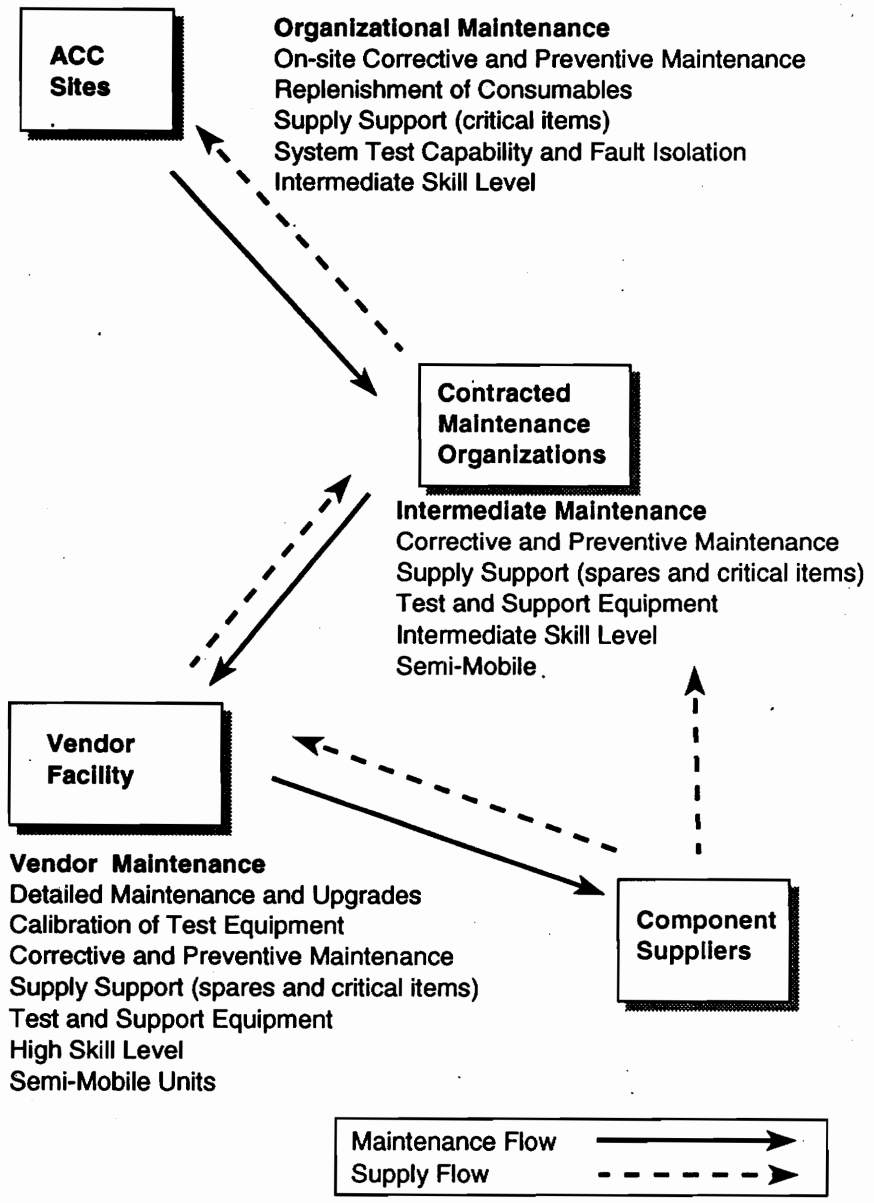

Figure 9. System Operation and Support Flow

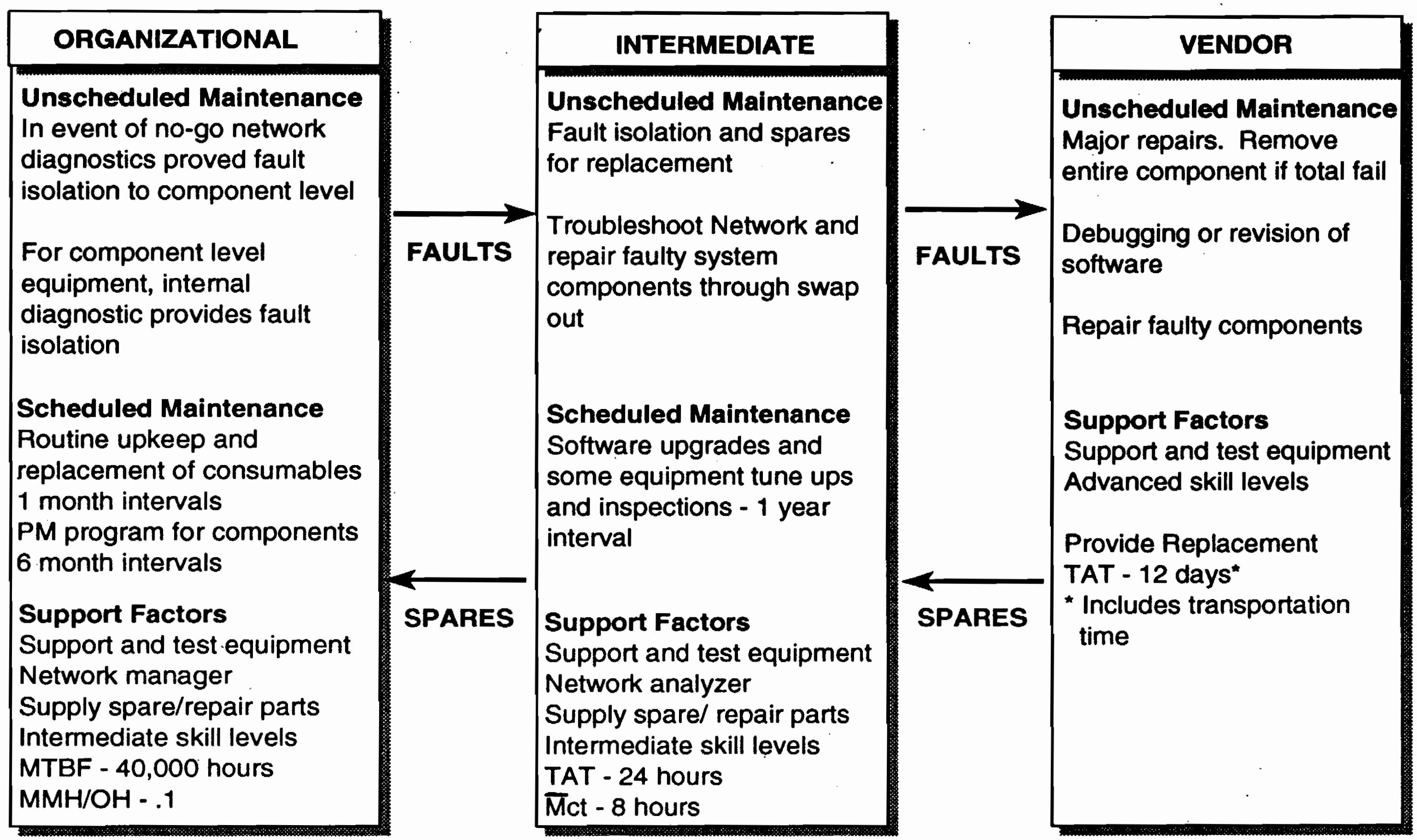

Figure 10. Maintenance Concept Flow

Criteria	Organizational Maintenance	Intermediate Maintenance	Vendor Maintenance
Done Where?	Operational Sites	Operational Sites	At Vendor Site
Done by Whom?	MINWK Personnel Intermediate Skills	Semi-mobil units with Intermediate Skills	Vendor High Skilled
On Whose Equipment?	MIWK's	MINWK and Vendor	Vendor
Type of Work ?	Visual Inspection and Checkout Minor Service Adjustments, Calibration, Replacement	Overload from Organizational Upgrades	Overhauls and Rebuilds Major Service and Repair Complicated Upgrades and Adjustments Detailed Inspection

Figure 11. Major Levels of Maintenance

Vendor Support

The wide area network communications system will primarily consists of Commercial Off The Shelf (COTS) products. Failure of these products or components will be repaired by the vendors. The vendor level supports include component overhauls/rebuilds, major on-site servicing, complicated component adjustments/calibrations, and complex system upgrades. ABC is responsible for arranging and maintaining maintenance and warranty contracts with vendors.

System Logistics and Support Concept

System support is an integral part of all aspects of system planning, design and development, test and evaluation, acquisition and installation, operations and system retirement. The system logistics and support concept identifies critical support elements which must be developed throughout the systems life-cycle. These include maintenance planning, supply support, test and support equipment, transportation and handling, personnel and training, documentation, and computer software.

Maintenance planning should continue throughout the system life-cycle and includes the maintenance concept, logistic support analysis, and procurement and acquisition of support items. Supply support includes all spare units, assemblies, modules, repair parts, consumables, and special supplies needed to support primary system equipment. Test support and equipment requirements at each level of maintenance and special transportation or handling equipment must be identified. The personnel and training requirements necessary for system installation and verification must also be identified. Finally all system installation, operating, and maintenance procedures and drawings must be developed and documented.

Figure 12 shows the logistic support data required for system planning and operation. Figure 13 shows the wide area network support functions.

Maintenance tasks and levels
- sequences
- time
- frequency

Facilities
- special equipment
- utility requirements
- costs
- HVAC

Test and support equipment
- quantity and type
- utilization
- availability/reliability
- cost

Transportation and handling
- equipment
- quantity, type, location
- containers
- packing and shipping

Personnel and training
- quality and skill level
- labor rates and hours
- overhead costs
- training costs
- replacement costs

Supply support
- repair levels/location
- repair parts/consumables
- spare quantity and type
- critical items
- wear out rates
- lead time

Additional factors
- MTBM, MTBF,MLH/OH
- MLH/year
- Logistic support cost factors

Figure 12. Logistic and Support Data

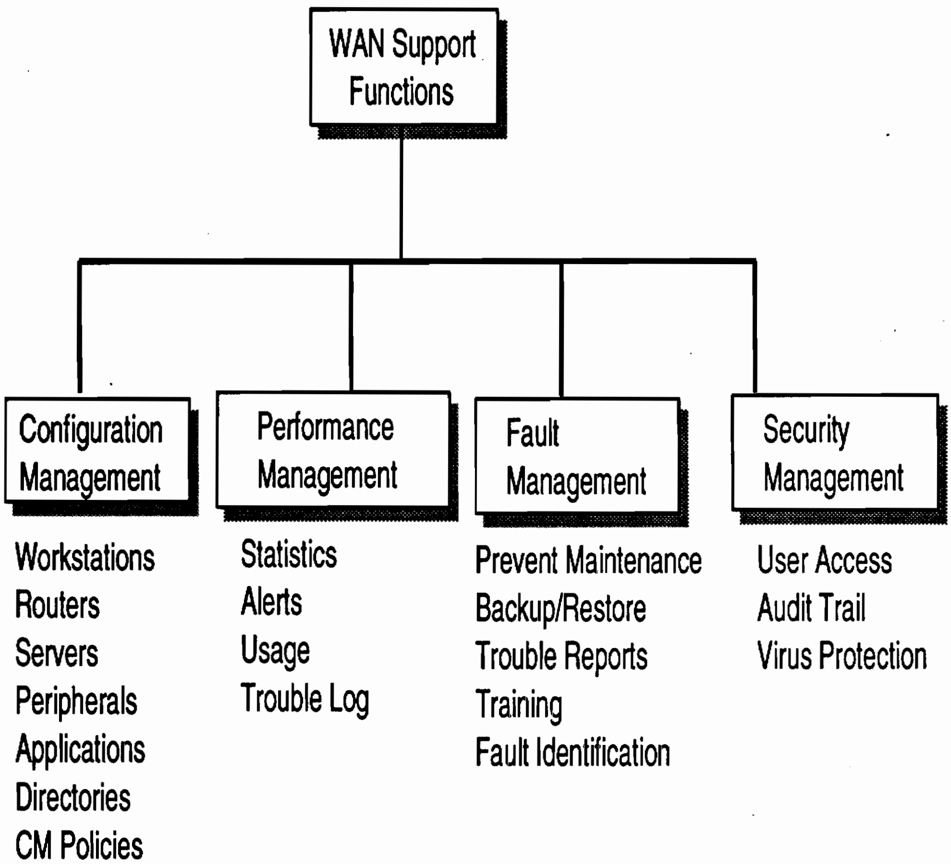

Figure 13. WAN Support Functions

System Test and Evaluation Concept

A system test and evaluation concept should be developed early in the system design stage and continue through the completion of the design. Thinking about system testing early in the design will stimulate design questions and provide significant design improvements that most likely would have gone undetected. An initial test plan format and concepts are presented in the following sections

I. Introduction

The MINWK (Management Information Network) System will be upgrading all sites from a proprietary (WANG) mail system to the recommended CCITT X.400 mail standard and X.500 directory services. Asynchronous Transfer Mode (ATM) switching with Synchronous Optical Network (SONET) infrastructures will also be installed. The upgrade has been designed to minimize the impact on the user nodes. The majority of the changes will occur at the Network Control Center and the Area Control Centers.

II. Scope

The Test and Evaluation Concept describes the testing that will take place at each site after installation of the upgrade and prior to "going live." After installation and upgrade the test and evaluation plans which follow will be used to verify operational status and identify system deficiencies. Review of the summary by authorized personnel will determine whether the site will go operational.

III. Test Environment

Test procedures will be done and results recorded for each portion of the system. System level tests will be from end user to end user. The portion of the system which is being tested is not tested in isolation. Other parts of the system should be installed and operational for system testing. Each site will have its own unique set of test procedures depending on the numbers and types of hardware and software platforms, mail systems and gateways.

IV. Test Plan

For each portion to be tested the following areas will be done as appropriate:

1. Power Up (This is also an operational procedure but doubles to test that all connections are working.)
2. Initial Communications
3. Send and Receive Mail
4. Network Monitoring Functionality
5. Directory Synchronization

For each site, a detailed diagram will describe the configuration including both hardware and software as well as communications network numbering. Each test procedure will be documented. Standard test forms will be created to facilitate documentation of system testing.

3.3) Advanced System Planning

Management Scope

The focus for this project is to provide a path for the consolidation of various heterogeneous E-mail messaging systems. The MINWK system will be designed to provide a balance between costs and benefits. The design approach incorporates a strategy that is based on government standards to provide a transport mechanism for the exchange of messages and E-mail attachments between sites using COTS hardware and software. This architecture will maximize the use of E-mail (X.400) standards; Electronic Data Interchange (CALS) standards; Directory Service (X.500) standards. High level functions to be accomplished include: design and implement the system; identify and consolidate requirements; identify security requirements and constraints; and define interface specifications.

Project Management Process

A conceptual system design will be developed which provides a baseline architecture for testing; and which accommodates all required and desired functionality of the system. An Initial Design Review (IDR) will be held, and, if the outcome of the IDR is favorable, an initial prototype will be developed. A demonstration of the initial prototype will be conducted, and limitations and concerns will be documented and addressed in the Preliminary Design Review (PDR). If the outcome of the PDR is favorable, a final prototype will be developed. Limitations and concerns noted during the final prototype demonstration will be documented and addressed at the Critical Design Review (CDR). Critical system design issues will be reviewed at the CDR and the decision to proceed with full system implementation will be made.

To accomplish formal system acceptance a preliminary test plan will be developed and a review will be conducted after the completion of the initial prototype. A final test plan will be developed and review will be conducted after the completion of the final prototype. Initial Validation, Verification, and Acceptance (Initial VV&A) testing will be conducted after the initial system delivery, and will be the formal mechanism by which the Initial Operational Capability (IOC) of the system is accepted. Final Validation Verification, and Acceptance (Final VV&A) testing will be conducted after the final system delivery, and will be the formal mechanism by which the Full Operational Capability (FOC) of the system is accepted.

Project Management Policies

Engineering Review Boards

An Engineering Review Board (ERB) will be established in support of and convened at the request of the project manager. It is composed of senior technical personnel from the functional engineering organization to provide technical oversight and assistance to the project manager. The ERB will be convened to fact find and provide recommendations on technical changes to controlled systems.

Project Management Reviews

A Project Management Review (PMR) will be convened at the request of senior management to review and approve the high level project decisions, schedules, funding commitments and strategic directions. The PMR will provide incremental or full authorizations to proceed to a FOC system. The contents of Life-Cycle project reviews are shown in Figure 14. This project accomplishes the project initiation design review and addresses all stages of the conceptual, preliminary, and detail design reviews. Figure 15 provides a project documentation checklist. Guidelines for the program management plan, operational concepts document, systems requirements document, and the configuration management document are presented following the project documentation checklist.

Configuration Control

The program manager is the executive agent and manager for Configuration Control for the MINWK effort. The specific configuration management duties and processes that apply to the MINWK effort includes software version control; hardware baseline control; requirements traceability; action item tracking; document control; and change control.

MINWK Life-Cycle Project Reviews

1. Program Plan Review
- Conduct Management Support Staff concept review
- Create user requirements statement
- Define initial system concept (budget, schedule and resource estimates)
- Develop initial system acquisition plan
- Establish acquisition strategy (staffing, contracting, and resources)
- Conduct trade study
- Analyze technology drivers

2. Project Initiation Review
- Conduct Program Review Board decision briefing
- Establish project work agreements (GO/NO GO decision)
- Define project requirements management
- Establish verification and validation approach
- Establish project team identification
- Create Work Breakdown Structure and budget allocations
- Create project products list and fact sheets
- Develop detail schedules with resources required
- Perform critical path identification and schedule risk analysis
- Establish risk management approach
- Develop control systems, visibility systems, status systems
- Establish leadership approach

3. System Requirements Review
- Conduct user requirement statement summary
- Develop system requirements document
- Create requirements models
- Perform requirements analysis
- Perform operational environment studies
- Establish concept selection criteria
- Perform trade study
- Identify technology drivers

Figure 14. Life-Cycle Project Reviews

4. Preliminary Design Review
- Develop design-to performance specifications
- Develop requirements traceability results
- Conduct risk assessment (based on design feasibility modeling and testing)
- Define architecture
- Define performance specification
- Develop project schedule
- Develop verification plan
- Develop integration plan
- Develop deployment plan
- Develop initial operator's and user's manual
- Documentation audit

5. Critical Design Review
- Create "Built-to" design documentation (drawings, process specifications)
- Create "Code-to" design documentation (development folders and manuals)

6. Test Readiness Review
- Implement test plans, procedures and configurations, test equipment/facilities
- Establish personnel responsibilities and qualifications
- Define completion date, expected results, acceptable results, and methods
- Establish security testing procedures
- Implement quality assurance methods
- Analyze test failure procedures, data analysis plans and procedures
- Analyze test site and preparation status

Figure 14 cont. Life-Cycle Project Reviews

7. Validation Readiness Review

- Establish validation plans and procedures
- Validate test configuration and equipment
- Implement security validation procedures
- Hardware configuration audit
- Software configuration audit
- Develop software QA plan
- Analyze technical justification for the design
- Establish trade-off analysis results and design feasibility model results
- Establish requirements and design traceability
- Develop preliminary system verification procedures

8. Acceptance Review

- Preform verification of requirements
- Document test results
- Capture demonstration and inspection results
- Conduct analysis and create lessons learned

9. Deployment Readiness Review

- Evidence that the system is capable of being deployed and operated as
- specified
- Analyze resolution of all discrepancies since System Verification

10. Operational Readiness Review

- Develop operational demonstration procedures
- Develop operational and maintenance procedures

11. Operational Acceptance Review

- Implement operational demonstration procedures
- Document operational Test Results
- Capture corrective action results for discrepancy reports
- Create operational readiness certificate

Figure 14 cont. Life-Cycle Project Reviews

Project Documentation Checklist

- PROJECT INITIATION REQUEST
- PROJECT MANAGEMENT PLAN
- CONFIGURATION MANAGEMENT PLAN
- SYSTEM REQUIREMENTS DOCUMENT
- OPERATIONS CONCEPT DOCUMENT
- SYSTEM DEVELOPMENT PLAN
- PROJECT SCHEDULE
- SECURITY PLAN
- COMMERCIAL OFF THE SHELF (COTS) EVALUATION
- INVESTIGATIVE REPORT
- SYSTEM DESIGN SPECIFICATION
- DATA DEFINITION DOCUMENT
- INTERFACE CONTROL DOCUMENT
- REQUIREMENT VERIFICATION TRACEABILITY MATRIX
- INTEGRATION TEST PLAN
- ACCEPTANCE TEST PLAN
- TRANSITION PLAN
- TRAINING PLAN
- FACILITY INTERFACE DRAWINGS
- INTEGRATION TEST PROCEDURES
- ACCEPTANCE TESTING PROCEDURES
- USER MANUAL
- OPERATOR MANUAL
- PROJECT CLOSURE MEMO
- INTEGRATION TEST REPORT
- ACCEPTANCE TEST REPORT
- VERSION DESCRIPTION DOCUMENT

Figure 15. Project Documentation Checklist

Project Management Plan

Policy Summary

MINWK will be managed according to a Project Management Plan. It shall be prepared by the Project Manager during the Conceptual Design Phase. The Project Management Plan is used to define the management environment throughout the life-cycle for the project.

Guidance

The Project Management Plan is used to specify the project life-cycle in terms of Periods and Phases, along with the products and reviews associated with each. The management organization, policies, and procedures to be used on the project are specified in this document. The main function of the document is to ensure that the management aspects of the project are addressed. It can be used to coordinate the interrelated activities of various organizations supporting the project.

This document can be baselined as early as the Preliminary Requirements Review and is updated as required through the Implementation and Integration Period.

Operational Concepts Document

Policy Summary

The Operations Concept Document is used to describe major operational activities, sequences of events, timelines, and interaction of interfaces.

Guidance

The Operations Concept Document is used to describe the planned environment that will exist when the project has transitioned to the operational mode. The audience is the user, the customer, and the O & M personnel. It helps them understand what the developer envisions the system doing then final operational capability is achieved.

The Operations Concept Document is baselined at the System Requirements Review and is maintained throughout the rest of the life-cycle.

Configuration Management Plan

Policy Summary

Configuration Management is the process of ensuring the integrity and traceability of products by identifying the configuration of the "system", "subsystem", "component", or other "products" at discrete intervals of the life-cycle, and controlling all changes to that configuration.

Guidance

A Product Assurance Program is the planned, systematic process of establishing requirements, standards, and procedures to ensure the quality, reliability, and maintainability of products being acquired or developed; and ensuring conformance to these established standards and procedures. There are three functional aspects to product assurance:

- Configuration Management - the process of ensuring the integrity and traceability of products by identifying the configuration of the system, subsystem, component, or product at discrete intervals of the life-cycle and controlling all changes to that configuration. The process of configuration management is documented in the Configuration Management Plan.

- Quality Assurance - the process of ensuring that all products and the processes that produce or acquire them conform to documented standards, policies, and procedures. The standards are documented in the System

Requirements Document, System Development Plan, and the System Design Specification. The process of quality assurance is achieved by generation and execution of Test Plans and Procedures, execution of a Configuration Management Plan.

- Verification and Validation - the process of ensuring that all requirements are complete, correct, and testable, and that each requirement has been satisfied by an end product. Validation is accomplished by evaluation, integration and test activities conducted to ensure conformance of products to user needs as recorded in the System Requirements Document and the various Design Documents. Verification is accomplished by analysis of the test reports to ensure intended functionality has been delivered, and the Requirements Verification Traceability Matrix.

The Configuration Management Plan can be baselined as early as the Preliminary Requirements Review and is maintained through the Implementation and Integration Period.

System Requirements Document

Policy Summary

The System Requirements Document specifies the complete and detailed requirements (functional, interface, security, and performance) of the system, subsystem, and components.

Guidance

The purpose of the System Requirements Document is to provide a basis for a mutual understanding between users and designers as to the definition of the products and operational aspects of this project. The System Requirements Document contains all requirements imposed on the project. This includes such areas as security requirements, design standards or manufacturing practices to be followed in developing the system, subsystems, or components, as well as those requirements that all final products are expected to meet.

The System Requirements Document is developed during the Conceptual Design Phase of the System Life-Cycle. The document presented at the System Requirements Review by the project manager is briefed to the customer and put under formal configuration control. The document is maintained through the Acceptance Test Period.

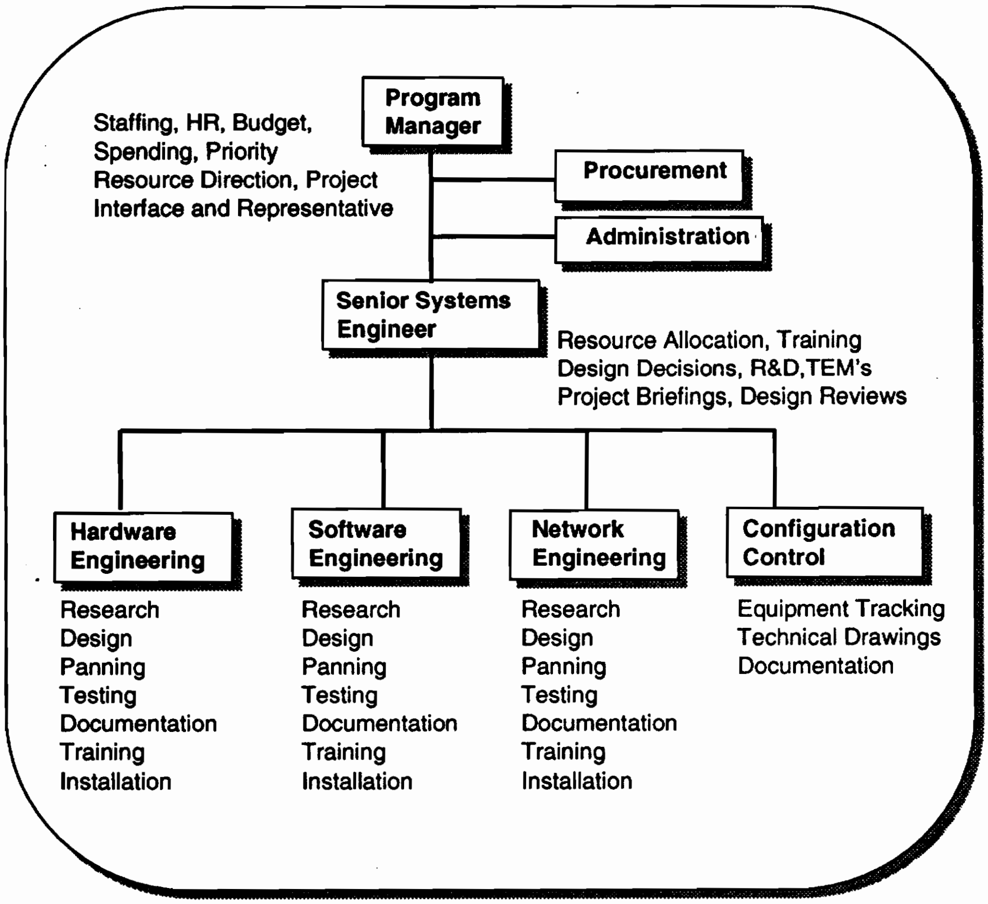

Figure 16. Work Breakdown Structure

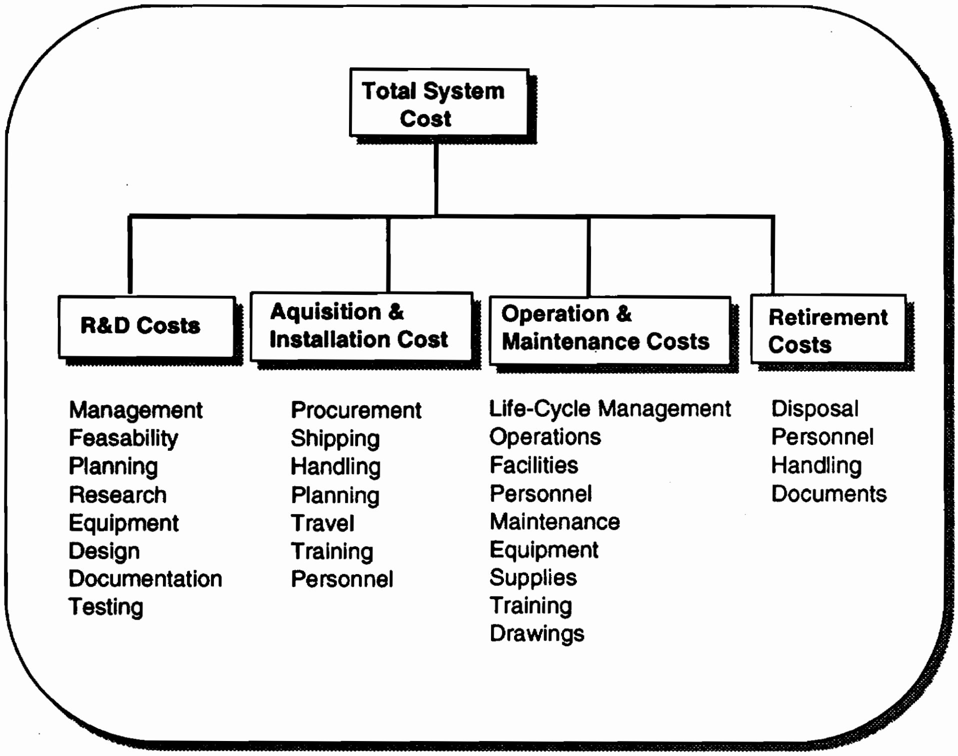

Figure 17. Cost Breakdown Structure

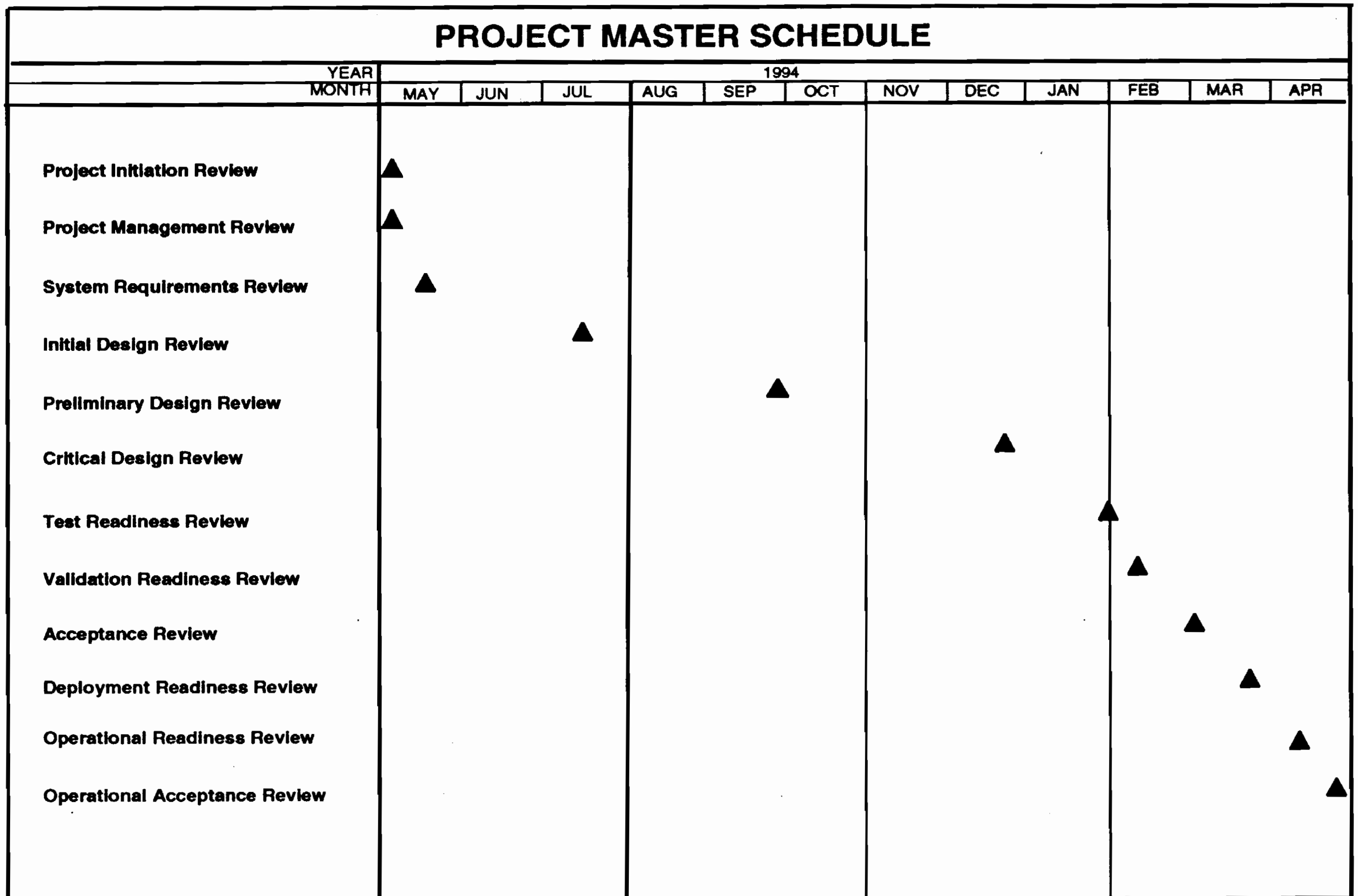

Figure 18. Project Master Schedule

3.4) Definition of System Requirements

Mission Statement

The MINWK communications system will implement X.400, X.500, CALS(EDI), and SNMP standards with ATM switching and SONET infrastructures to accomplish the four primary objectives described below.

Objective 1: Improve User Productivity

Provide a common open operating environment enabling information and software application resource sharing between a variety of hardware platforms.

Objective 2: Enhance Information Exchange

Implement standard communication formats and interface requirements.

Objective 3: Reduce Life-Cycle Costs

Maximize use of COTS products reducing dependence on custom applications and the associated development and maintenance costs. Open systems reduce duplication, increase resource reuse, and provide network scalability and flexibility.

Objective 4: Improve System Management

Control network access and process network audit data from a centralized source.

Operational Life-Cycle
MINWK will be operational by July 1995, with an expected life time of 5 years.
The SONET infrastructure shall have an expected useful life of at least 10 years.
The ATM switching shall have an expected useful life of at least 10 years.
MHS, Router, and Management software shall be system life time upgradable.
MHS, Router, and Management hardware shall have an expected life of five years.

Functional Requirements
Provide multimedia electronic mail to include: audio, image, graphics, video, and text

Costs
The Life-Cycle cost of the MINWK system will be less than $8,000,000.

System Capacity
Support local network node capacities up to 5000 users.

Security
Provide physical access controls to area control centers.
Provide user verification and authentication system access controls.

Performance Requirements
MINWK will support data transmission rates of 2 giga bits per second, and deliver 10 mega bit multimedia documents or files in less than 10 seconds.

Figure 19. System Requirements

Network Management
The MINWK system will provide status, audit, traffic, and history data; remote configuration capabilities; and fault detection for primary system components.

System Utilization
The MINWK system will be capable of supporting daily utilization demands as presented in figure 20.

Availability
The system will be available 24 hours a day 7 days a week.
Handle peak utilization periods at 75% capacity.
Handle short term bursts (less than 4 hours) of 200% of the projected utilization.

Reliability
The network shall be operational at least 98% of non-scheduled maintenance time.
Provide power failure transfer (UPS) for primary equipment.
The MTBF of the system shall be 40,000 hours.

Maintainability
Preventive maintenance routines shall not exceed 2 hours.
The mean preventive maintenance time ($\overline{M}pt$) shall be less than 2 hours.
The mean time to repair (MTTR) shall be less than 6 hours.
The MTBM of the system shall be one year.
The mean maintenance time shall not exceed 0.1% of operational time. (MMH/OH)

Figure 19 cont. System Requirements

Environment
System components will operate in standard (OSHA defined) office environments.
The system shall implement automatic controlled shutdown if the environment reaches 95% of specified ranges.

Software Compatibility
The system shall be capable of interoperation with the primary user and subcontractor mail systems:WP Office,NeXT Mail, MS Office, cc:Mail, SMTP Mail, and Quickmail.

The system shall be capable of providing document conversion for the primary user and subcontractor word processing packages:Word Perfect, Microsoft Word, and Mac Write.

Software Maintenance
Automatic tape backup of MHS system files will be performed weekly.
Version control and upgrade procedures will be developed.

System Retirement
System components will be donated to local elementary schools after the usable life.

Physical Characteristics
Primary system components will be easily accessible and reasonably sized.
Installation of electrical wiring and network cabling as required by all County and State codes and regulations.

All equipment shall be powered by either 120 or 240 VAC power.

Figure 19 cont. System Requirements

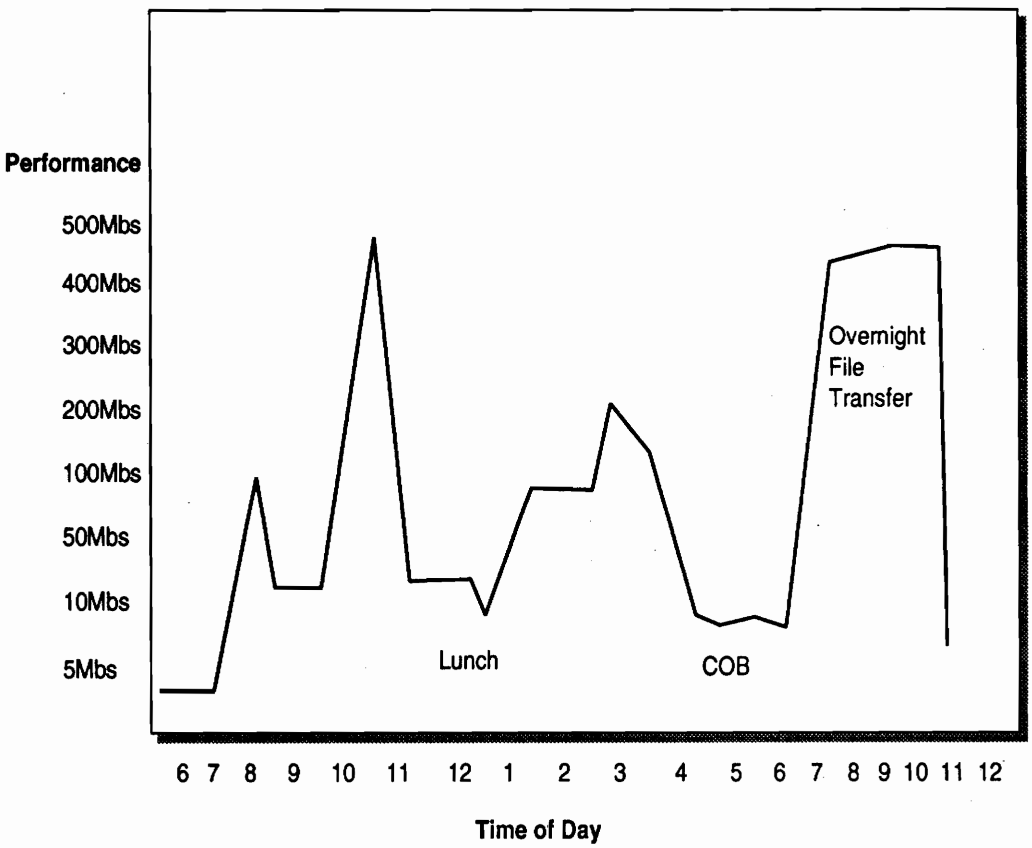

Figure 20. System Utilization

4) Preliminary Design Phase

Preliminary design begins with the systems technical baseline defined in the Conceptual Design Phase. Refinement of system operational concepts and requirements is accomplished through functional analysis and system requirements allocation. Allocation of requirements to the subsystem level provides a baseline for the identification of alternative design solutions. System synthesis and optimization is achieved through comparison and evaluation of economic goals and specific functional and operational requirements.

4.1) System Functional Analysis

Functional analysis is described as the systematic approach used to design and develop a system. It is intended to facilitate the design process in a logical and complete manner. The functional analysis is based on the operational concept and the maintenance concept. Functional flow diagrams provide the methodology to structure system requirements into functional components. If used properly, functional flow diagrams define mission objectives, performance parameters, user requirements, operational deployment, operational life, effectiveness factors, and expected operating environment. MINWK operational and maintenance functional flow diagrams to three levels are shown in Figures 21 through 25. The functional analysis identifies five primary functional components (Addressing, Packaging, Routing, Handling, Monitoring) right away. System requirements can now be allocated into these functional areas establishing hardware, software, or component level requirements. Figure 26 shows MINWK system requirements allocated to the identified functional components. Continuing the analysis will further define requirements for each functional component. Functional analysis and functional flow diagrams prove to be an effective design development tool.

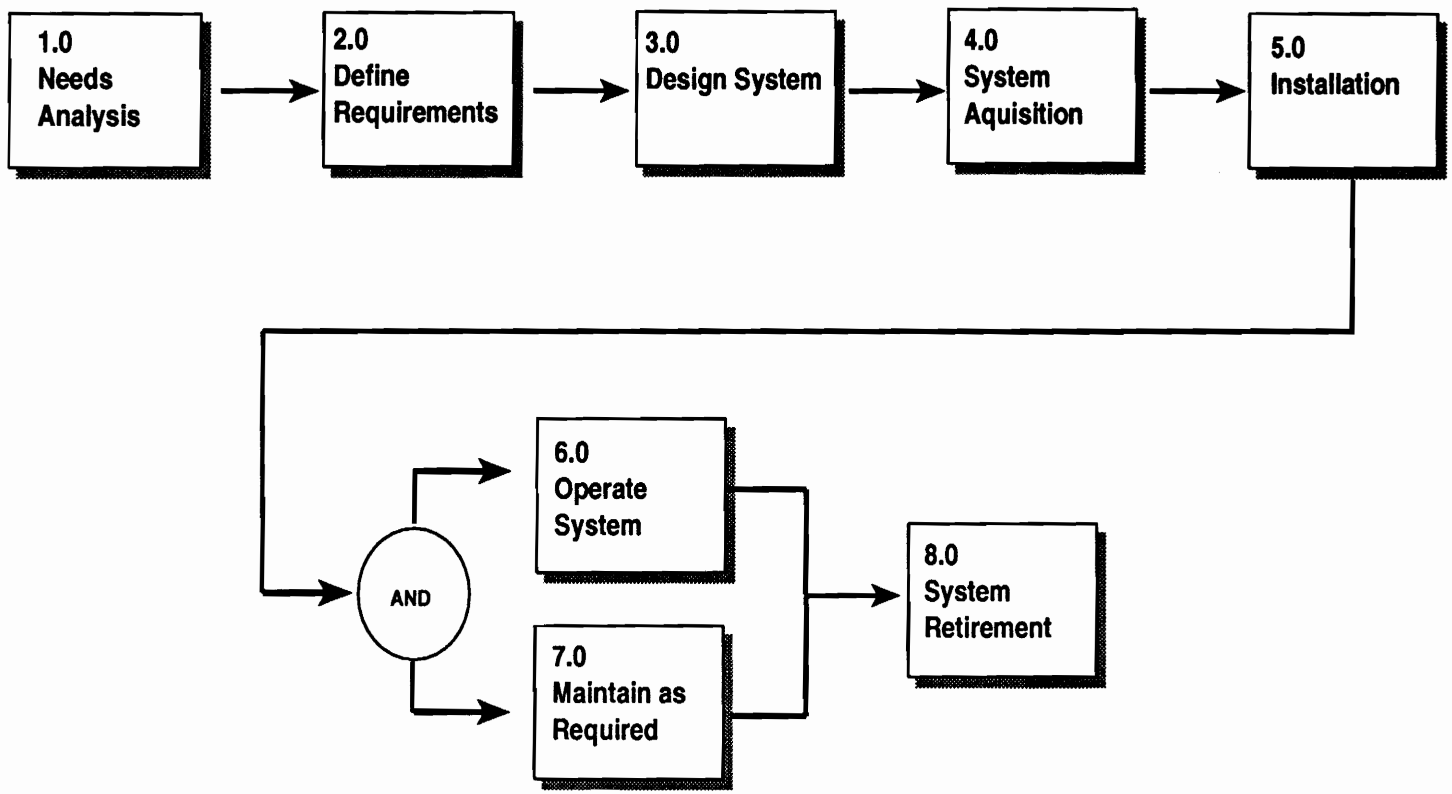

Figure 21. 1st Level Functional Flow Diagram

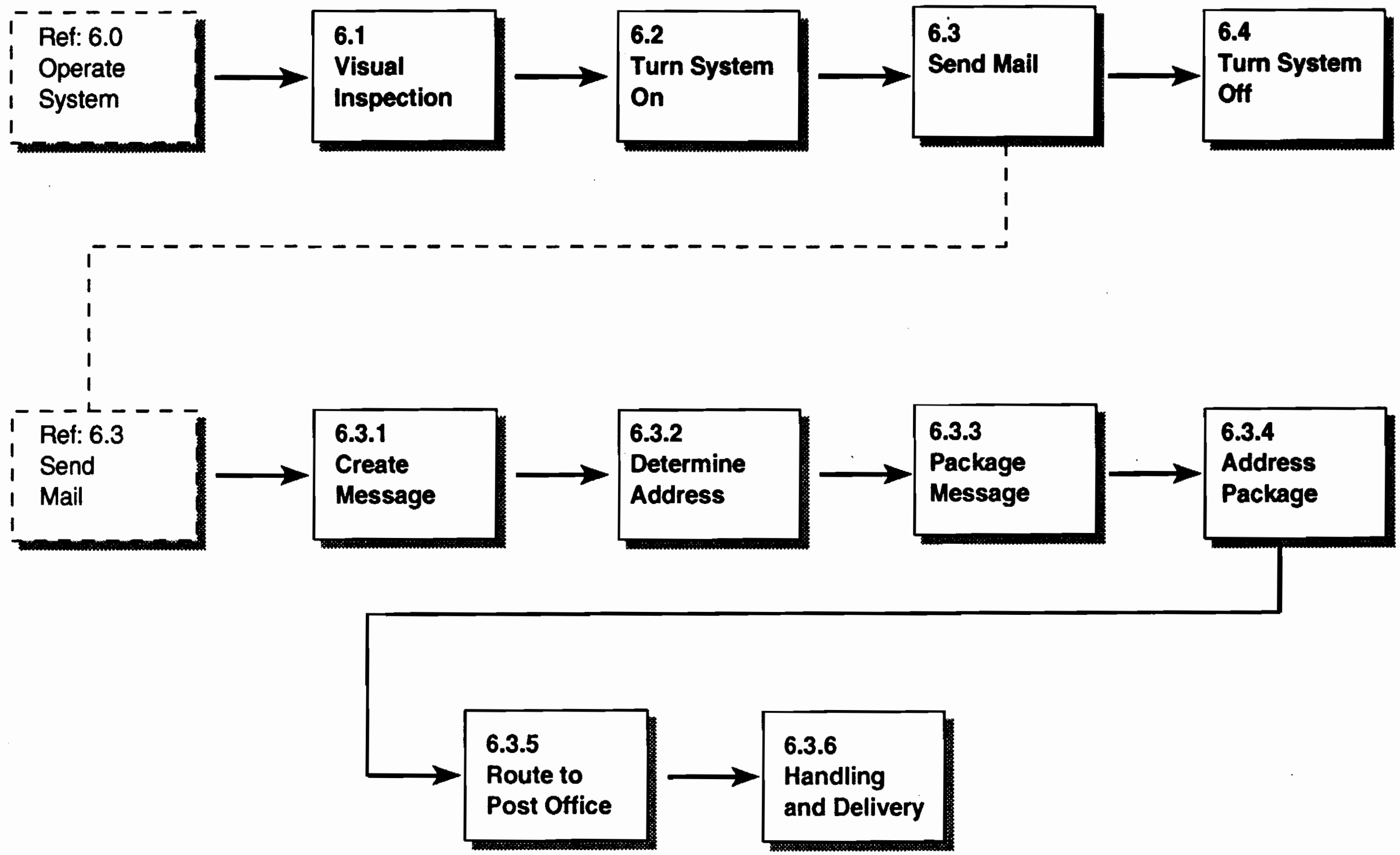

Figure 22. 2nd and 3rd Level Operational Flow

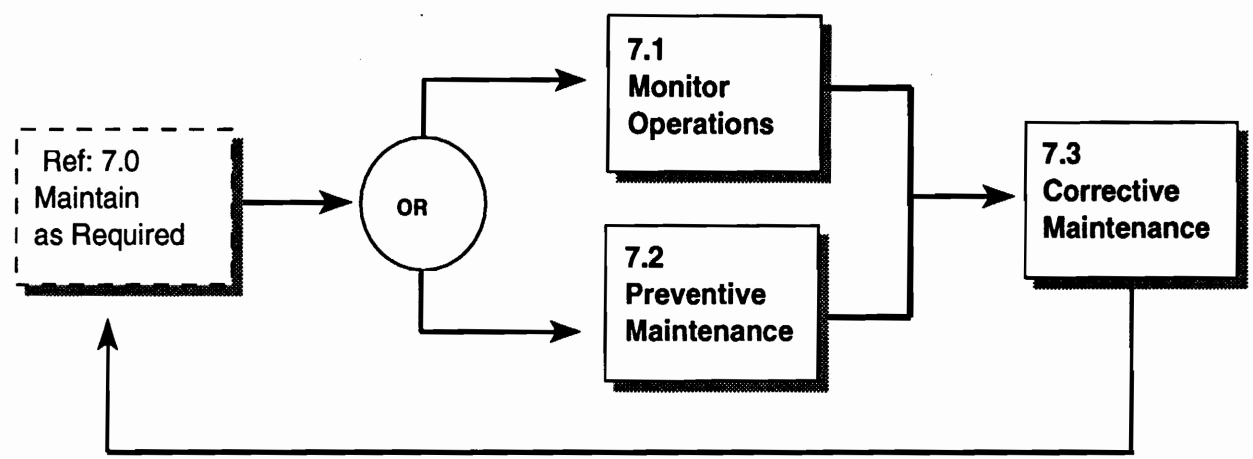

Figure 23. 2nd Level Maintenance Functional Flow Diagram

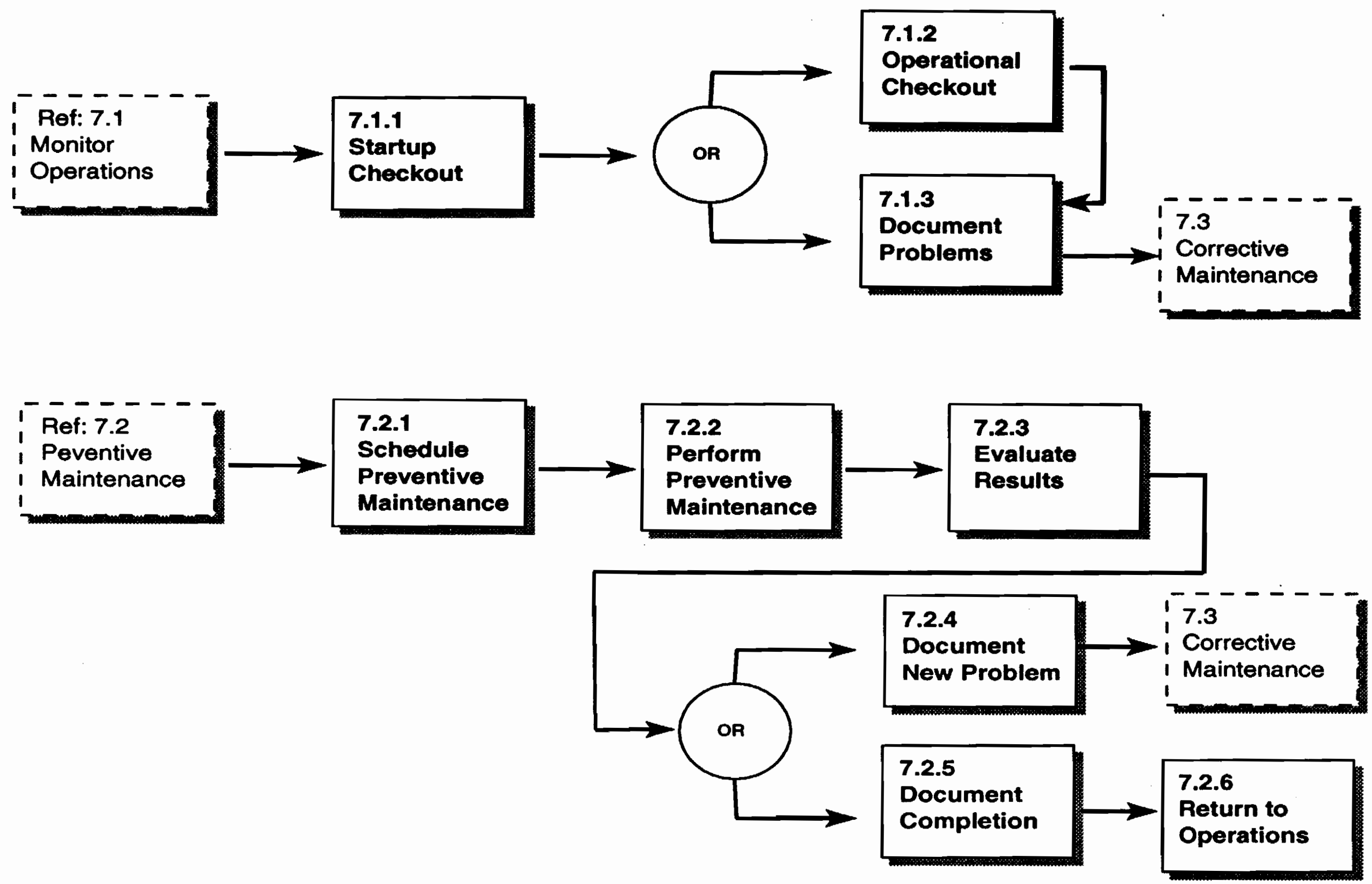

Figure 24. 3rd Level Functional Flow Diagram

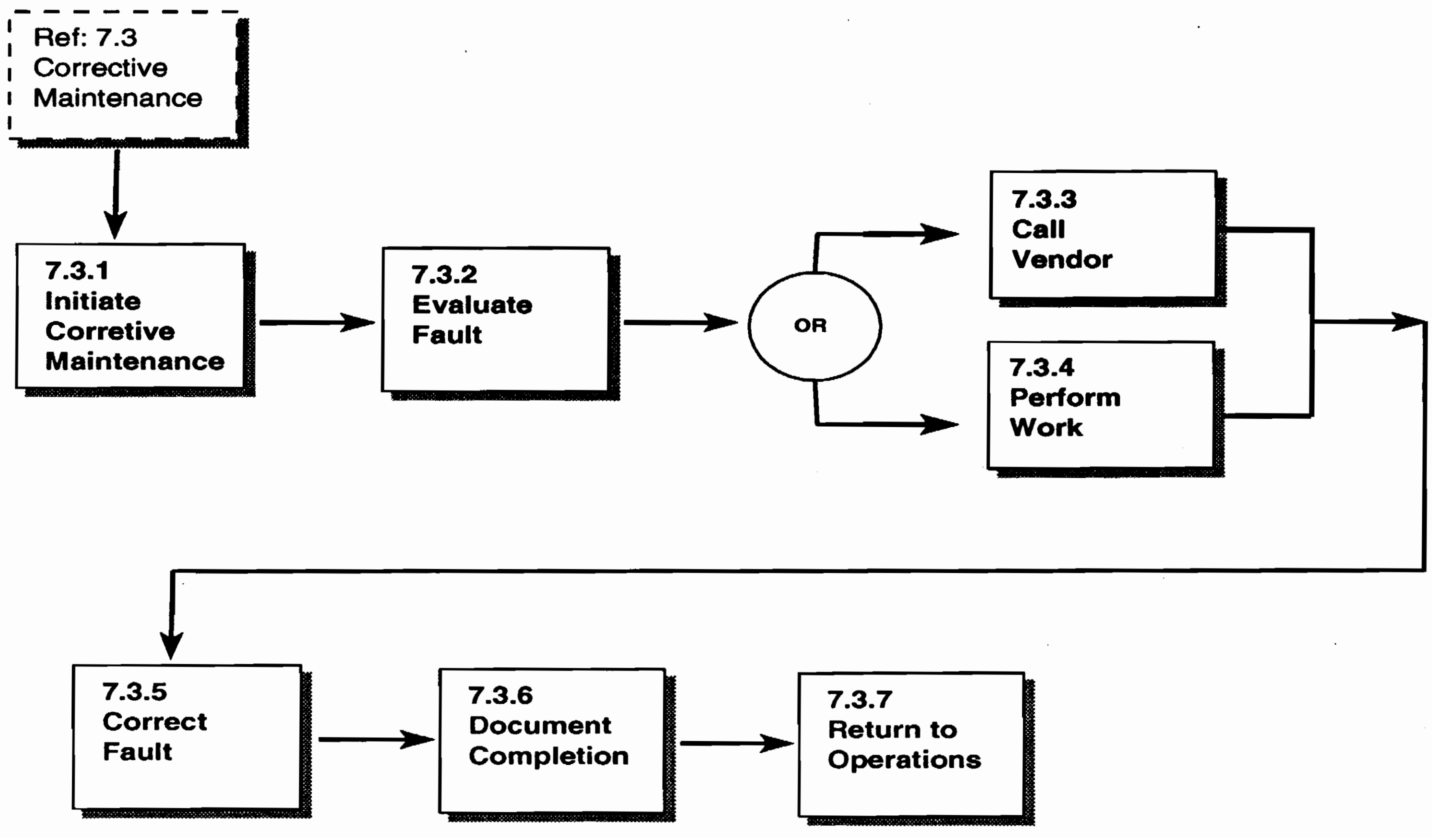

Figure 25. 3rd Level Maintenance Flow Diagram

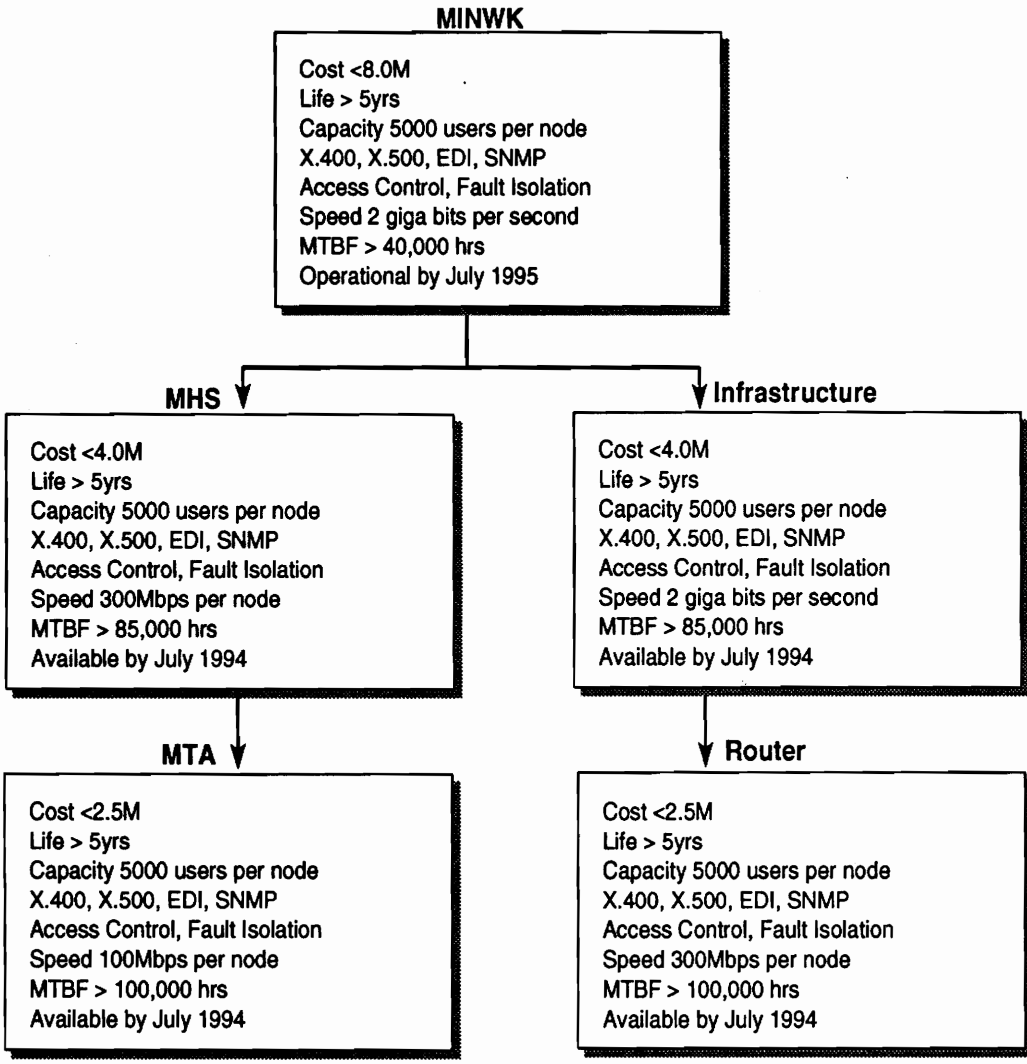

Figure 26. Component Level Requirements Allocation

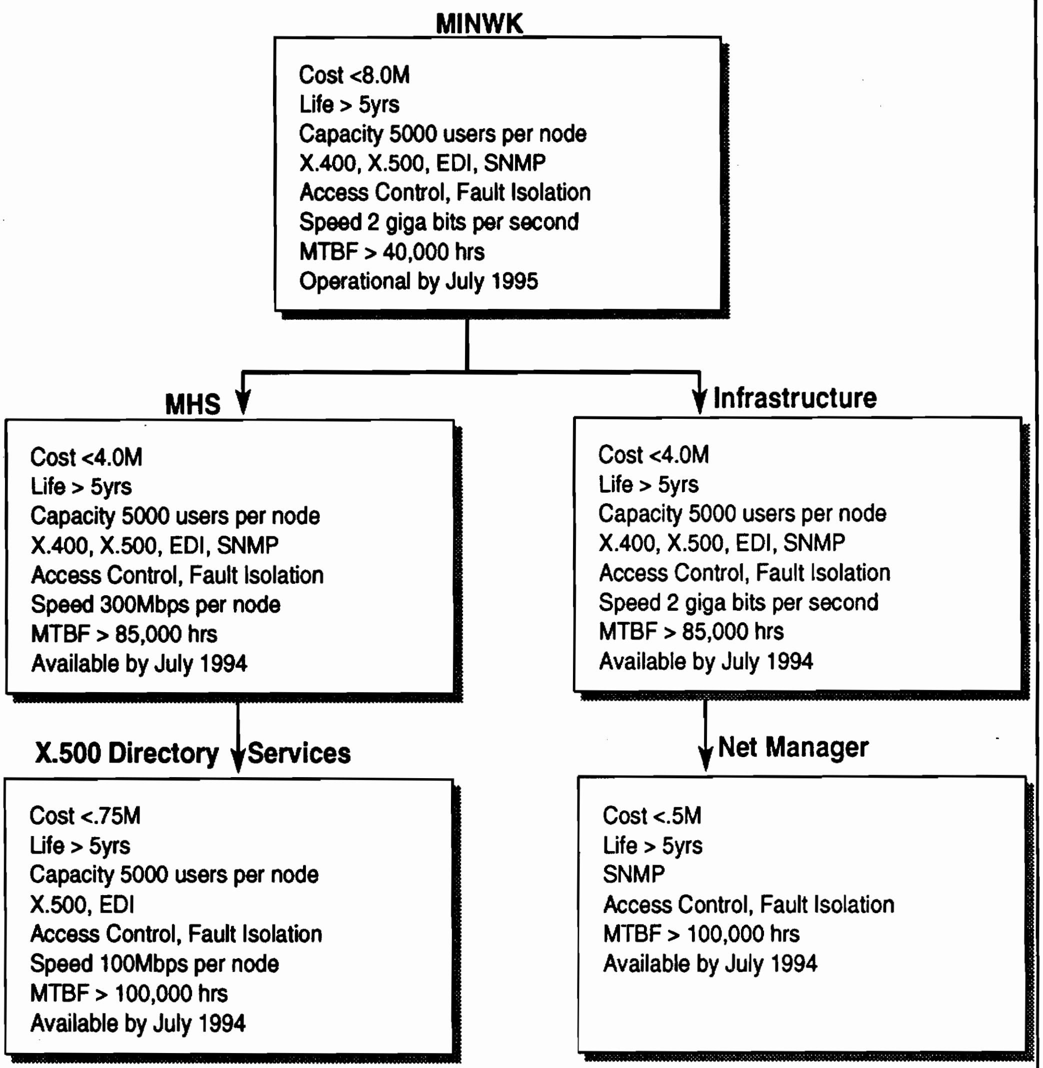

Figure 26. Component Level Requirements Allocation

4.3) Analysis and Evaluation of Alternatives

Based on the allocation of system requirements, component level alternatives can be evaluated. Critical system requirements such as cost, performance, and maintainability were used as attributes to compare the top router, MTA, and ATM product alternatives. The evaluation identified Cisco Systems routers, ISOCOR's ISOPLEX X.400 MTA, and GTE's Spanet ATM switch as the component alternatives of choice for the MINWK network. Figures 27, 28, and 29 summarize the evaluation criteria and rating of each of the components.[22]

Criteria	Cisco Systems AGS+	Wellfleet Backbone
Life-Cycle Costs	$55,000	$49,000
Performance	4.6 Mbps	4.6 Mbps
Expandability	To four ATM interfaces	To four ATM interfaces
Availability	Now	Now
Reliability	Tested	Tested
Maintainability	Low maintenance skills	Low maintenance skills
Market Share	75%	15%
Reputation	Top of the line Router	Top of the line Router
Supported Protocols	IP, BR, IPX,OSI	IP, BR
Processing Speed	Max. Latency < 1.39E-05	Max Latency < 1.38E-05
Service	Cisco Smartnet Support	Wellfleet Support
Resident Expertise	Two installed	No experience
System Compatibility	Yes	Yes
Risks	None	None

Figure 27. Component Evaluation: Cisco vs. Wellfleet Routers

Criteria	ISOCOR X.400 MTA	Retix X.400 MTA
Life-Cycle Costs	$200,000	$230,000
Expandability	Software upgradeable	Software upgradeable
Availability	Now	Now
Reliability	Tested	Tested
Maintainability	Intermediate Skills	Intermediate Skills
Market Share	35%	20%
Reputation	One of top vendors	One of top vendors
Supported Gateways	6-8 Well Known	2-3 Well Known
Service	ISOCOR Support	Retix Support
Resident Expertise	Yes	Yes
System Compatibility	Yes	Yes
Risks	None	None

Figure 28. Component Evaluation: ISOCOR vs. Retix MTA

Criteria	GTE Spanet	Fore System
Life-Cycle Costs	$355,000	$490,000
Performance	6 Gbps	4 Gbps
Expandability	10 - 600 Mbps interfaces	8 - 300 Mbps interfaces
Availability	Now	Now
Reliability	Tested	Tested
Maintainability	High maintenance skills	High maintenance skills
Market Share	10%	10%
Reputation	Not established	Not established
Supported Interfaces	WAN, Campus, LAN	Wan, Campus, LAN
Service	GTE Support	Fore System Support
Resident Expertise	NO	NO
System Compatibility	Yes	Yes
Risks	New technology	New Technology

Figure 29. Component Evaluation: GTE Spanet vs Fore System

5) Detail Design Phase

The Detail Design Phase begins with the configuration derived in the Preliminary Design Phase and continues further definition of system and subsystem specifications, provides detailed design documentation, and establishes development of a system prototype.

5.1) Detail Design Team

The detail design team is responsible for component research and development, system integration and planning, capability assessment, configuration and testing, and system technical documentation. Each member of the team will be responsible for the development of system components as shown in the design team organization Figure 30. The two senior systems engineers will coordinate resources, initiate design review activities, and insure a systems design approach is followed.

5.2) Detail Design Specifications

Before any system can communicate, system addressing schemes must be developed. The following sections present router network numbering schemes and MTA directory structuring schemes for MINWK.

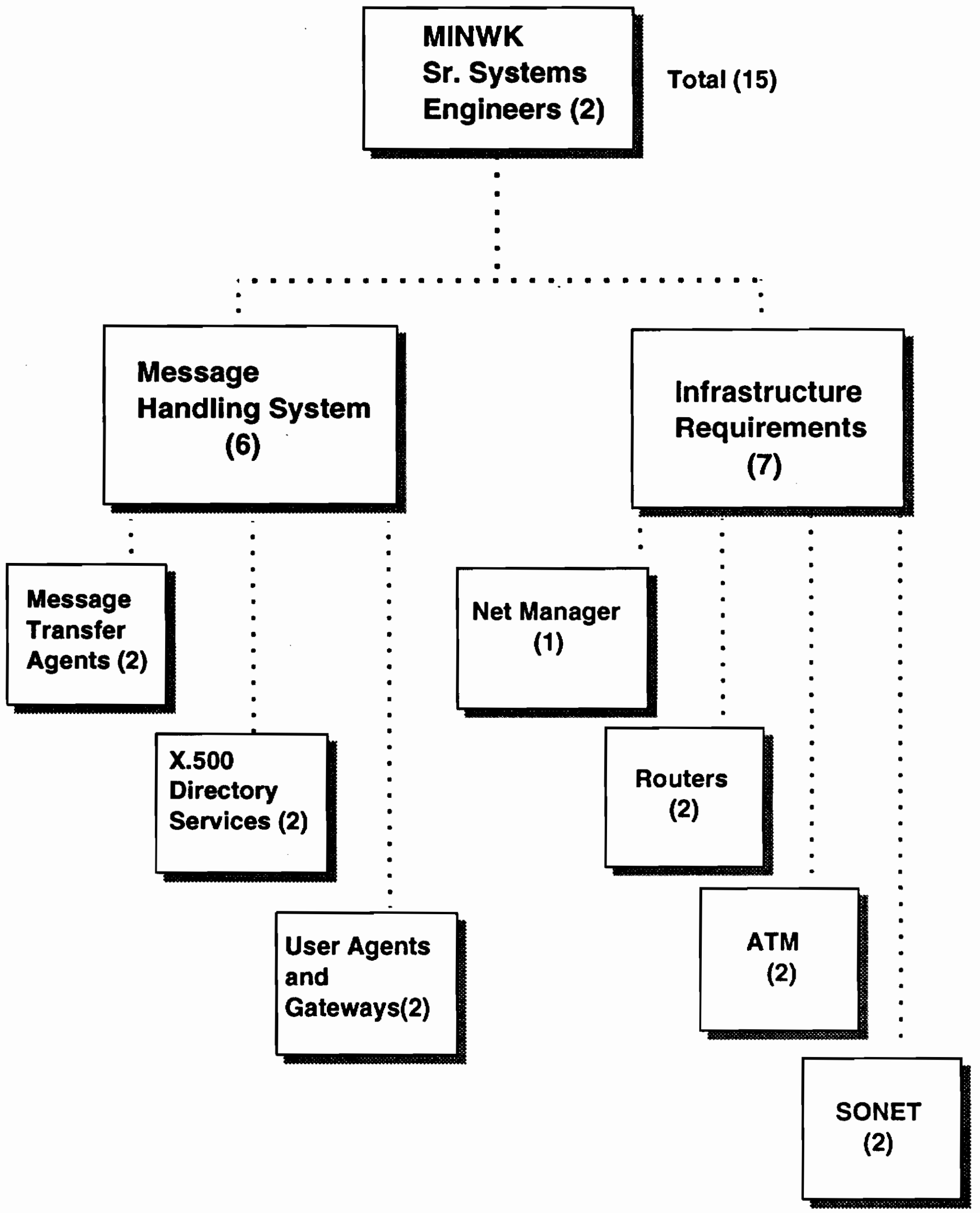

Figure 30. Design Team Organization and Research Areas

Router IP Numbering Scheme

Figure 31 outlines the IP numbering scheme for the MINWK system. An explanation of the MTA Directory Structure follows directly after. In the IP addressing scheme, ranges of host ID's are reserved for different devices in order to make debugging simpler. With this addressing scheme, MINWK can have 64 subnets per node with 1022 hosts per subnet. The IP addresses have been assigned in a manner that will allow an administrator to identify the location of a problem with just the IP address.

5.3) Detail Design Drawings

Area Control Center configuration diagrams are shown in Figures 32 through 37. A system prototype will be developed using two of the WAN nodes. The preliminary Test Plan follows the ACC diagrams.

HOST #	RESERVED FOR DEVICE TYPE
11 - 30	AGS Routers
31 - 130	IGS Routers
131 - 150	MTAs
151 - 160	Hubs
161 - 200	File Servers
201 - 350	Sun Workstations
351 - 500	PCs
501 - 650	MACs
651 - 800	NeXT
801 - 950	WANGs
951 - 1022	Misc devices

AGS Router #		Location	Connections between ACC's :
11		NCC	
12	NEACC	NCC to NEACC	189.11.4
13	PKACC	NCC to PKACC	189.11.8
14	SWACC	NCC to SWACC	189.11.16
15	WCSACC	NCC to WCSACC	189.11.32
16	WCNACC	NCC to WCNACC	189.11.64

Figure 31. Network Addressing Schemes

PKACC

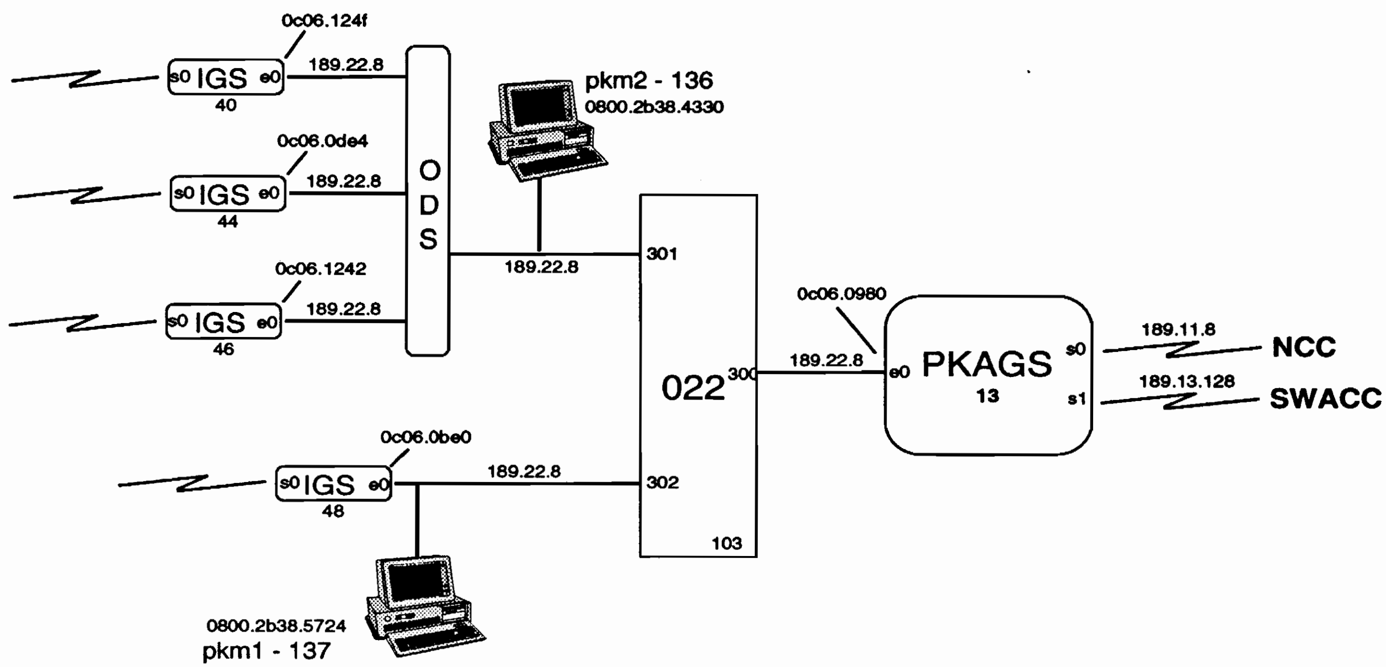

FIGURE 32. PKACC

NEACC

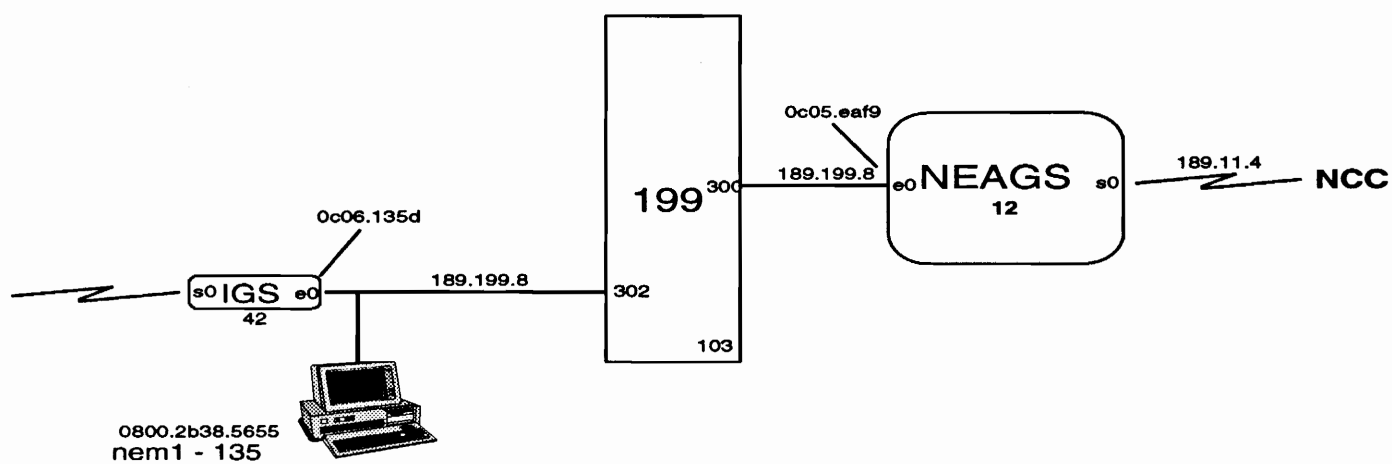

FIGURE 33. NEACC

WCNACC

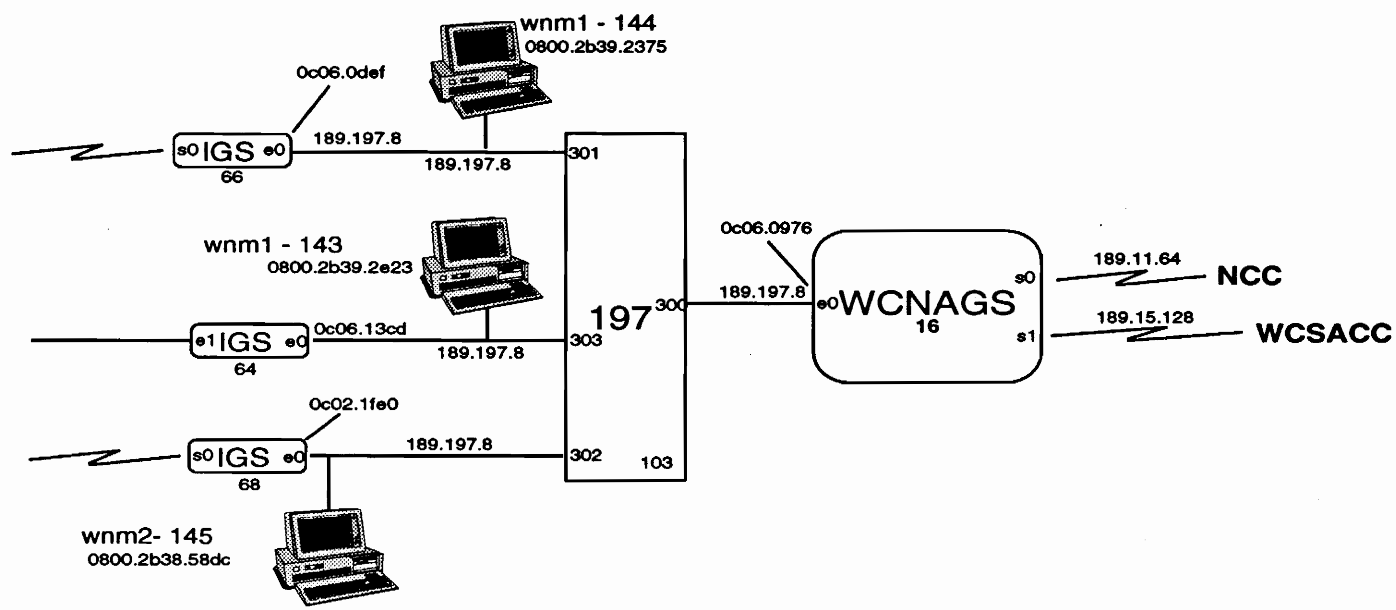

Figure 34. WCNACC

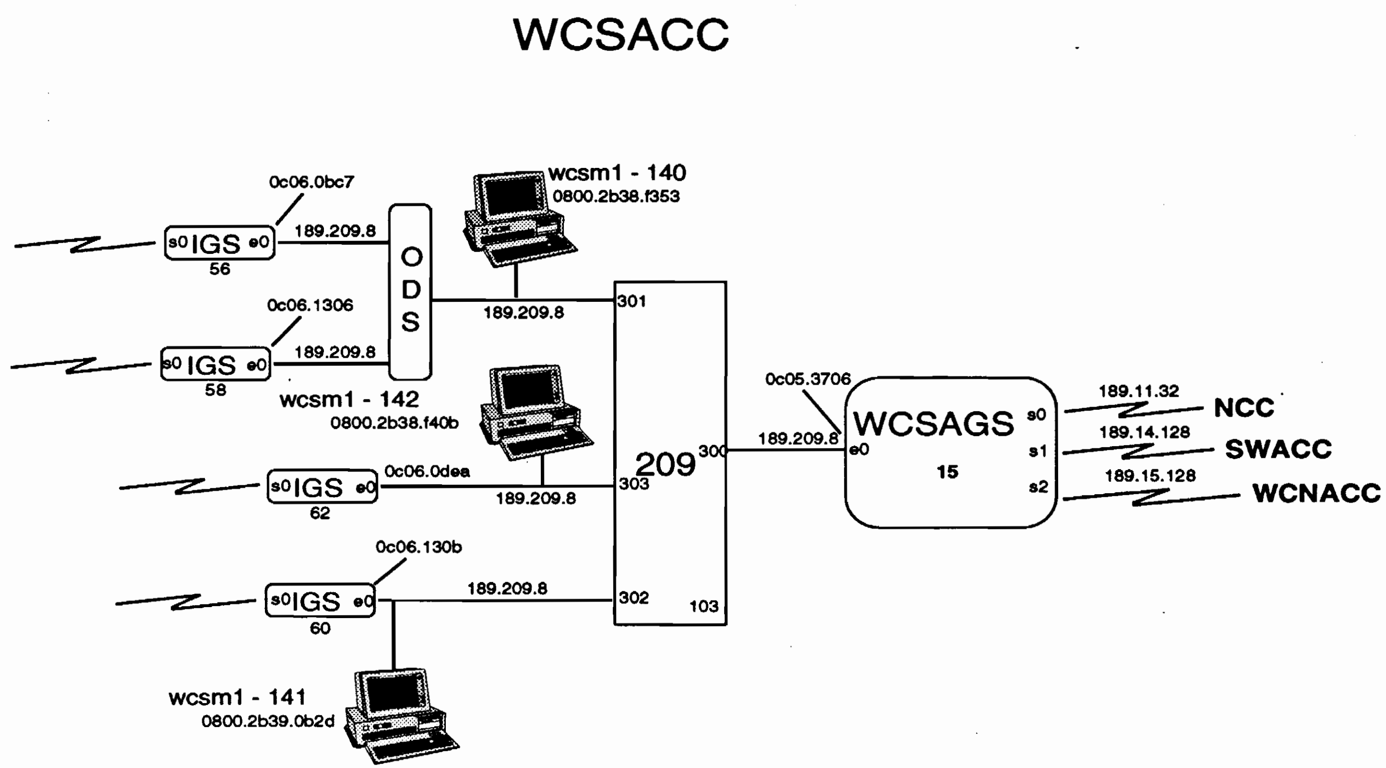

Figure 35. WCSACC

SWACC

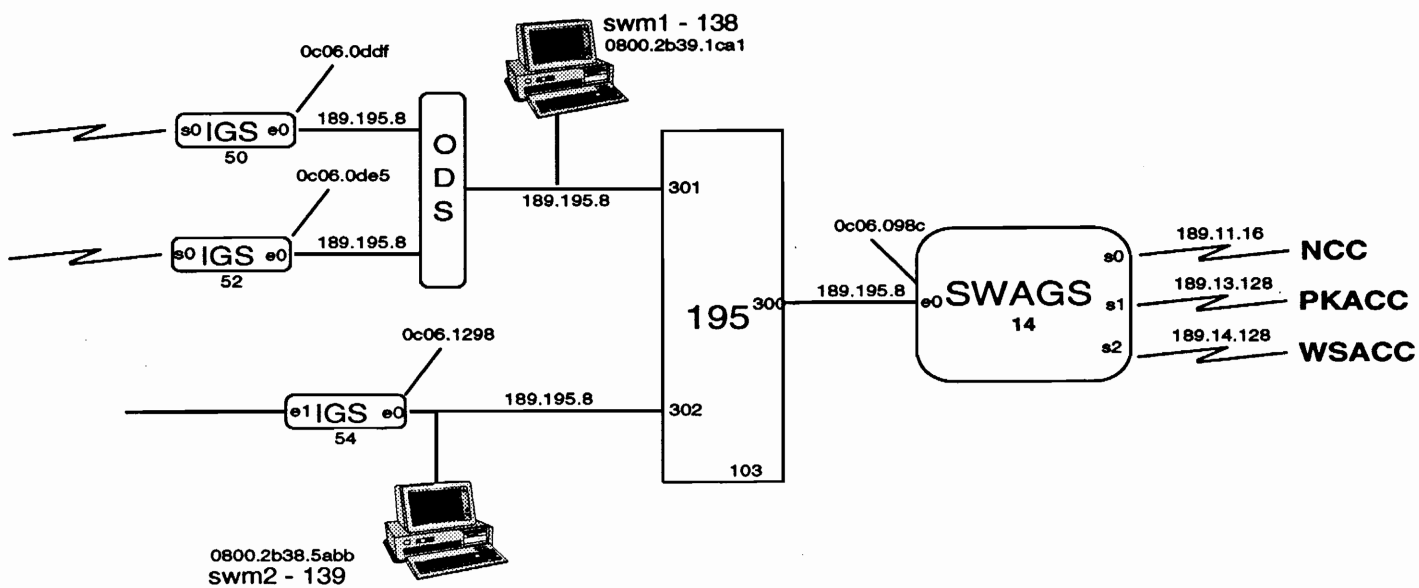

Figure 36. SWACC

NCC

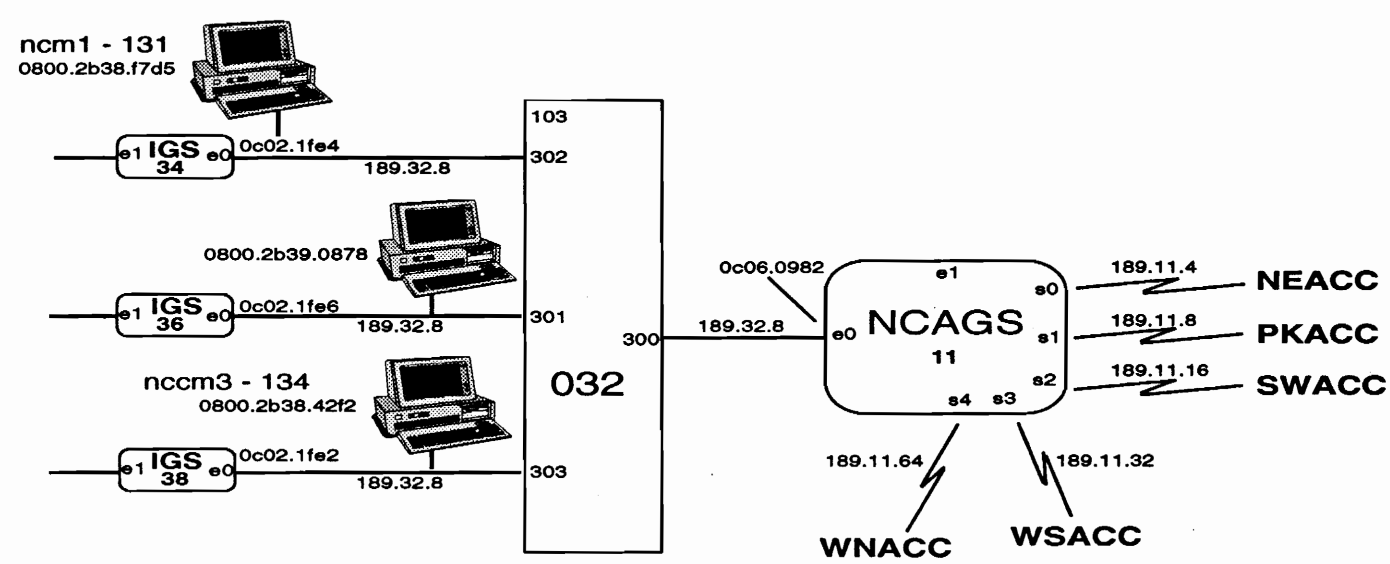

FIGURE 37. NCC

X.400 MTA Directory Addressing Scheme

The following paragraphs describe table based and rule based X.400 MTA directory addressing schemes. Directory services facilitates exchange of mail between sites. The directory management scheme provides an organized means of identifying and tracking system users. Additionally, this scheme provides a means of managing the relationship between X.400 O/R (Originator/Recipient) addresses and their associated aliases. Directory management implementation eliminates the need for the end user to have knowledge of X.400 addressing schemes or to remember lengthy, complicated user address strings.

There are two types of addressing schemes, table-based address translation and rule-based address translation.

Table-based address translation requires that the system administrator establish and maintain a table of alias records which consists of O/R names and associated aliases for each gateway user. One O/R name and one or more aliases are matched in an alias record. With table-based address translation, each user may have multiple aliases, each in the format of a different LAN E-mail system, so that a message originator may address mail using the alias format that is compatible with his own native E-mail system. Since each alias for a given user corresponds to only one O/R name, a local gateway user may have many addresses by which he can be reached.

Rule-based address translation requires that the system administrator establish and maintain a correspondence between an O/R name and an alias according to a pre-defined set of rules. The primary advantage to this type of addressing scheme is that it does not require the administrator to maintain a table of aliases and O/R names for each individual user. Instead, the administrator maintains a table of locator records, each of which consists of a partial O/R address and a locator name, to identify a particular E-mail location. The administrator also establishes a set of address translation rules by which a user's name is converted into X.400 format. The user name and locator are joined together to construct a rule-based alias. The address translation rules and locator records are used to map this alias to an appropriate X.400 O/R address.

The MINWK system will employ table-based address translation for local users and rule-based address translation for remote users. This scheme allows the system to provide maximum flexibility for local user addresses while minimizing the administrative burden of establishing and maintaining lists of remote user names.

5.4) Development of System Test Plan

Router Test Plan

I. Introduction

The MINWK Phase III network will use Cisco AGS+ routers to establish the Wide Area Network (WAN) communications backbone. Cisco IGS routers will be used to establish communications from the individual nodes to the Cisco AGS+ WAN interface at each ACC. These routers have the ability, through access lists, to permit or deny specific protocols and/or processes. Testing is done to ensure communications have been properly established and to verify the completeness of the access lists.

II. Scope

The router must first be configured with the basic startup configuration. The start up configuration simply defines the communication protocols and assigns network addressing schemes to be used. The configuration files for each router are unique and thus each router must be tested independently. A complete router configuration file contains access lists that permit or deny specific protocols and/or processes on a source address/destination address basis. The testing will determine whether the desired permit/deny objectives have been achieved.This is accomplished by intentionally violating the access list and observing the result. If the access lists are working properly, any violation attempt well be unsuccessful.

III. Test Environment

Each Area Control Center (ACC) will have a Trusted Guard front-ended by a Cisco AGS+ Router. Each compartment on the back side of the Guard will have at least one Cisco IGS Router. Each compartment will also have a Mail Transfer Agent (MTA) on it.

IV. Test Plan

Preliminary testing will be done to verify that data can be transmitted and received by the routers over the communication line or lines. An Internet Control Message Protocol request packet (ICMP Request commonly referred to as a PING) is addressed to the remote router and transmitted across the communications line by the local router. If the routers are able to communicate over the communication line the local router will receive an ICMP Response from the remote router. If a PING is successful, data can be transmitted over the communications line. Each access list will then be individually tested to ensure the desired permit or deny requirements have been met.

Message Transfer Agent (MTA) Test Plan

I. Introduction

The ISOPLEX 800 Message Transfer Agent (MTA) is a message handling system that conforms to worldwide X.400 standards and exploits the benefits of Open Systems through implementation of the Open System Interconnect (OSI) model. Interoperability and connectivity are accomplished through the compliance with OSI, therefore, providing worldwide networking capabilities to any system that is fully conformant with OSI.

II. Scope

This test plan will test the ISOPLEX 800 MTA for MINWK Phase III. This test plan will demonstrate that the MTA will allow the exchange of messages with other MTA's and X.400 users of any computer system as well as provide an accurate report of any invalid transactions.

III. Test Environment

At each Area Control Center (ACC), the hardware test environment will consist of at least one 486 DEC PC, one DEC 1.05GB external SCSI hard drive, one DEC 1/4 inch external tape drive, and one Advanced Gateway System (AGS) router. The software test environment will consist of DEC SCSI hard drive fully configured with SCO OPEN DESKTOP/SCO UNIX, ISOCOR X.400 MTA (88'), and ethernet driver routines.

IV. Test Plan

Before testing of the MTA can commence, preliminary testing will verify that there is communication between the Network Control Center (NCC) and the local ACC site.

The system administrator will install a test user account for the ISOMAIL 800 mail system and organize any necessary login scripts that are needed to access the mail system. The test will include the following functionalities:

- The sending and receiving of simple text messages from the local MTA to the MTA at the NCC.
- The sending and receiving of text message with attachments from the local MTA to the MTA at the NCC.
- Replying to a message.
- The sending and logging of error generated messages.

After testing has completed a summary of the test results will be fully documented.

System Level Test Plan

I. Introduction

The MINWK (Management Information Network) System is upgrading its E-Mail communications backbone from a proprietary (WANG) mail system to the X.400 standard established by the International Standards Organization (ISO). X.400 provides a standard transport for E-Mail across the Wide Area Network (WAN) enabling users with different mail packages to communicate. Each individual component will have been tested prior to the system level test plan.

II. Scope

The System Level Test Plan is written to test end user to end user E-mail functionality. This test plan will verify that end users with different mail packages can successfully communicate and will provide an accurate report of any discrepancies that need to be resolved.

III. Test Environment

At each Area Control Center (ACC), the hardware test environment will consist of at least one 486 DEC PC, one DEC 1.05GB external SCSI hard drive, one DEC 1/4 inch external tape drive, and one Advanced Gateway System (AGS) router. An IGS router will be installed and configured between the end-user workstations and the MTAs

The software test environment will consist of a DEC SCSI hard drive fully configured with SCO OPEN DESKTOP/SCO UNIX, ISOCOR X.400 MTA (88'), and one or more of the following gateways: SMTP, SMTP with NeXT Message Handler, cc:Mail, QuickMail, and Microsoft Mail. The routers will be configured to allow static and/or RIP routing,TCP/IP and/or CLNS.

The end-user platforms appropriate to the site will also be necessary, with the electronic mail system for that platform installed.

IV. Test Plan

End user to end user mail testing will be performed between each supported mail system at each node and the mail systems supported at the NCC. The test procedures are designed to test the following electronic mail functionalities:

Test Send and Receive For

- Simple text message
- Simple Text message with attachments
- Message with cc: recipients
- Message with bc: recipients
- Return Receipts

Each function will be tested by sending mail from an end user on every supported mail system to an end user on every supported mail system at the NCC. This procedure will be repeated for each ACC. After testing is complete, test results will be summarized and fully documented.

6) **Future Recommendations**

Continue development of Preliminary System Design and complete a formal preliminary design review. The functional flow diagrams should be developed to further define requirements for each functional component. Additional requirements are necessary to establish reliable, quantifiable, and distinguishing evaluation criteria. The evaluations presented in the Preliminary Design Phase are based on life-cycle cost and one or two other critical factors. A more detailed evaluation could be warranted.

Many techniques exist for performing multiattribute system hardware or software evaluations. The Sequential and Weighted evaluation techniques are briefly described here. Sequential elimination uses a choreographed process of elimination with multiple comparisons of alternative to alternative and attribute to attribute to identify the most preferred alternative. Weighted evaluation techniques involve ranking and weighing attributes, normalizing and pairwise comparisons. Multiattribute decision analysis techniques could be applied to evaluate the primary (router, MTA, gateway, network manager, ATM) components of the network.

Continue further development of Detail System Design and complete formal design reviews with ACC administrators. Begin to develop Detail Design documentation such as Interface Control Documents, Implementation Plans, and Deployment Plans. Finally, performance testing and analysis and system loading should be completed and the results documented.

7) Conclusions

The systems engineering life-cycle process appears to work very well in this application to develop a wide area network communications system upgrade design. The Conceptual Design Phase established high level direction to implement X.400, X.500, CALS(EDI), and SNMP standards with ATM switching and SONET infrastructures. Project management, system maintenance and support, and system requirements documents were created detailing design goals and positioning company resources. The Preliminary Design Phase allocated system requirements to the component level where an evaluation of alternatives established a preliminary system configuration. The Detail Design Phase continued design development providing detail design drawings, specifications and component level test plans.

Future recommendations include performing detailed evaluation of technical alternatives, holding engineering and design review meetings between sites, and developing Interface Control, Implementation, and Deployment documentation.

As you can see, the systems engineering process provided a logical and systematic approach to design a communications system upgrade design for ABC corporation.

GLOSSARY

ABC	Alpha Beta Corporation
ACC	Area Control Center
AGS	Advanced Gateway Server
ANSI	American National Standards Institute
ATM	Asynchronous Transfer Mode
ASCII	American Standard Code for Information Interchange
CAD	Computer Aided Design
CALS	Continuous Acquisition and Life-Cycle Support
CAM	Computer Aided Manufacturing
CCITT	International Telephone and Telegraph Consultive Committee
CDR	Critical Design Review
CGM	Computer Graphics Metafile
CMIP	Common Management Information Protocol
CMIS	Common Management Information Service
COTS	Commercial Off The Shelf
DBMS	Data Base Management System
DIB	Directory Information Base
DIT	Directory Information Tree
DN	Distinguished Name
DNS	Domain Name System

DOD	Department of Defense
DOS	Disk Operating System
DSA	Directory Service Agent
DUA	Directory User Agent
EDI	Electronic Data Interchange
E-Mail	Electronic Mail
FTP	File Transfer Protocol
FOC	Final Operational Capability
Gbps	Giga bits per second
IAB	Internet Advisory Board
IETM	Interactive Electronic Technical Manual
IGS	Integrated Gateway Server
IGES	Initial Graphics Exchange Specification
IP	Internet Protocol
IOC	Initial Operating Capability
ISO	International Standards Organization
ISOCOR	International Standards for Open Communications Resources
LAN	Local Area Network
Mbps	Mega bits per second
MHS	Message Handling System
MIB	Management Information Base

MIME	Multipurpose Internet Mail Extension
MINWK	Management Information Network
MTA	Message Transfer Agent
NCC	Network Control Center
NIC	Network Information Center
NIST	National Institute of Standards and Technology
NMS	Network Management System
NTSC	National Television Standards Committee
O/R	Originator / Recipient
OSI	Open Systems Interconnection
PEM	Privacy Enhanced Mail
PDR	Preliminary Design Review
RDN	Relative Distinguished Name
RFC	Request for Comments
SDLC	Synchronous Data Link Control
SMTP	Simple Mail Transfer Protocol
SNMP	Simple Network Management Protocol
SONET	Synchronous Optical Network
TCP/IP	Transmission Control Protocol/ Internet Protocol
UA	User Agent
WAN	Wide Area Network

REFERENCES

1) Blanchard, Benjamin S. and Wolter J. Fabrycky. Systems Engineering and Analysis. Prentice Hall: New Jersey. 1990.

2) Bradner, Scott. Router Tests V.6. Harvard University, 1993.

3) Data Communications. "ATM Networking" October 1993.

4) Electrical Communication. Volume 64, Number 2/3 1990.

5) Enck, John. A Managers Guide to Multivendor Networks Professional Press Books: Horsham, PA. 1991.

6) Lanz, C., Lubich H., and Plattner B. X.400 Message Handling. Addison-Wesley: New York. 1992.

7) McClain, Gary R. International Connectivity Standards Van Nostrand Reinhold: New York. 1990.

8) Robison, Phillip. Delivering Electronic Mail M&T Books: San Mateo, CA. 1992.

9) Stallings, William. Handbook of Computer Communications Standards Macmillan: New York. 1992.

10) Stallings, William. Data and Computer Communications 3rd Edition Macmillan: New York. 1993.

11) Steedman, Douglas. X.500: The Directory Standard and Its Application
Technology Appraisals Ltd.: Twickenham, UK. 1993.

12) Tanenbaum, Andrew S. Computer Networks 2nd Edition
Prentice Hall: New Jersey. 1990.

13) Uyless, Black. TCP/IP and Related Protocols
McGraw-Hill: New York. 1992.

FOOTNOTES

[1] Stallings, William. Data and Computer Communications pg. 424-442

[2] Lanz, C., Lubich H., and Plattner B. pg. 50-55

[3] Ibid., pg 63

[4] Ibid., pg 66-70

[5] Uyless, Black. pg. 271

[6] Ibid., pg 272-280

[7] Robison, Phillip. pg 90

[8] Lanz, C., pg. 148-158

[9] Electrical Communication., pg 105

[10] Ibid., pg 111

[11] Ibid., pg 124

[12] Ibid., pg. 148

[13] Ibid., pg. 209

[14] Uyless, Black., pg. 77-80

[15] Steedman, Douglas, pg. 10-22

[16] Enck, John., pg. 95-107

[17] Data Communications. pg. 66-82

[18] Lanz, C., pg. 163-165

[19] Steedman, Douglas., pg. 3

[20] Data Communications. pg. 66

[21] Electrical Communication., pg. 73

[22] Bradner, Scott., pg. 1-8

[23] Data Communications., pg. 69