A SYSTEMS ENGINEERING PLAN FOR PROVIDING EXTERNAL COMMUNICATIONS CONNECTIVITY TO A SMALL COMPANY

by

Jennifer E. Marsh

Project and Report submitted to the Faculty of the

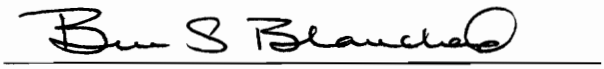
Virginia Polytechnic Institute and State University

in partial fulfillment of the requirements for the degree of

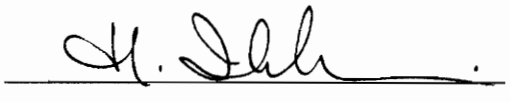
MASTERS OF SCIENCE
in

Systems Engineering

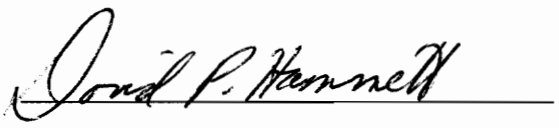
APPROVED:



Dean B.S. Blanchard, Chairman



Dr. H. Ibrahim



Mr. D. Hammett

May, 1996
Blacksburg, Virginia

Key Words: Network Architecture, Internet, Systems Engineering

c. 2

LD
5681.1
V251
1996
M-17
c. 2

A SYSTEMS ENGINEERING PLAN FOR PROVIDING EXTERNAL COMMUNICATIONS CONNECTIVITY TO A SMALL COMPANY

by
Jennifer E. Marsh

Committee Chairman: Benjamin S. Blanchard
Systems Engineering
(ABSTRACT)

This project addresses the issue of providing external electronic communications capability via the Internet to a small company with an existing Local Area Network in place. A contractor will assist the company in deriving system requirements, evaluating various technologies and design alternatives, creating the network architecture design, and finally implementing and testing the complete system. The systems engineering lifecycle is followed, with the results of the first phases of conceptual, preliminary, and detail design presented within this report. Additional phases of the project, such as implementation, test, and training are beyond the scope of this project and are therefore described and scheduled but not executed. Project management takes place throughout all phases.

The goals and requirements of the AmeriClean corporation lead to a network design which integrates a combination of commercial components into a system which builds upon the existing communications infrastructure. The addition of a dedicated Internet access line, the security of an Internet firewall, and hardware and software which provide access to Internet applications provide enhanced capabilities while retaining the look and feel of the current Windows NT LAN. A balance is achieved between providing ease of use and administration, and providing advanced technological capabilities which improve AmeriClean's business position in the marketplace.

Acknowledgment

I would like to extend my thanks to my parents, for teaching me from an early age how to persevere and do a job well. They always have had confidence in my abilities.

I never could have survived the Advanced Courses without the support of my classmates and friends. Thanks for the academic and moral support, and for the sanity checks that confirmed there really is life outside of work and class! Thanks to the Advanced Education office; Dave, Christina, and most especially Bev; for guidance and smoothing the logistics of part-time graduate education.

Thanks Mike for putting up with my stress and complaints for three years. You were always full of encouraging words, and ready with a study break when I really needed it.

Thanks to all of you for making this accomplishment possible.

Table Of Contents

Table of Figures

Table of Tables

1. Introduction

1.1 Situational Background

The AmeriClean Corporation sells a variety of domestic and commercial cleaning products to wholesale and retail outlets all over the country, and in a limited number of foreign markets. The company consists of approximately 50 employees in positions of manufacturing, sales, marketing, management, and administration. They currently have a Local Area Network set up at the home office in Northern Virginia which supports a corporate database which tracks product orders, inventory, and records of communications with customers. This network is used daily by most employees, but has no external connections to any data sources outside of the company facilities. The LAN consists of 40 personal computers, Intel 486 and Pentium compatible, running the Microsoft NT operating system and using the Microsoft Office suite of data processing tools as shown in Figure 1-1. One full-time system administrator operates and maintains the network. He is kept extremely busy maintaining connectivity, administering the e-mail post offices, training new employees and answering user questions. On occasion, as when a software upgrade must be installed, he has part-time assistance from another employee who is a computer hobbyist and has taught himself some of the technologies in his spare time.

The company employs 15 sales representatives who spend about 75% of their time traveling to the various customer locations, gathering information about current satisfaction levels with the products, attempting to sell new products to existing customers, and looking for potential new customers of the product line. Currently, this sales force records data from the two to five day trips using paper forms and writing in travel journals. No data is entered into the corporate databases until the employee returns to the home office, or unless she has made arrangements with one of the headquarters employees to enter data that is transmitted back from the trip by telephone or by fax. The fact that orders are not being placed until the sales person returns to headquarters up to a

week after the order was requested is causing unnecessarily long lead times for filling orders.

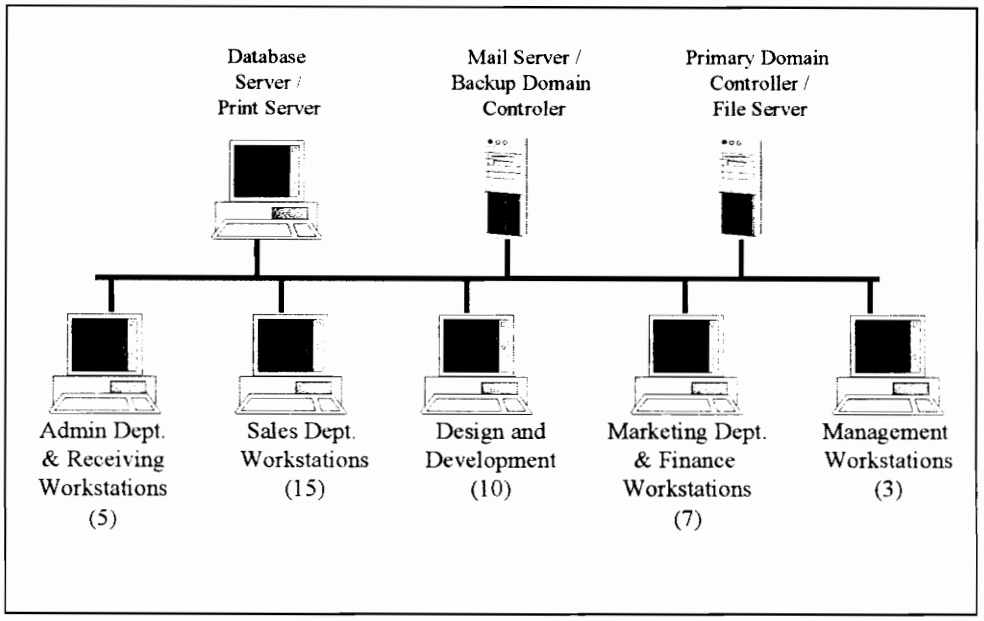


Figure 1-1: AmeriClean Corporation Network Architecture.

In addition, employees located at headquarters have remote communications needs as well. Corporate management has heard significant information and read articles about the usefulness of the Internet and the World Wide Web. They can see countless applications for this means of accessing and researching information, and would like to be able to research competitors so as to stay abreast of the latest developments. They need to send e-mail to suppliers to track resource shipments, and would like to have a customer support e-mail address instead of the current telephone hot line.

1.2 Problem Statement

The AmeriClean Corporation would like to employ a systems engineering approach to develop a plan for achieving external connectivity with other corporations and with the traveling salespeople via the Internet. Connectivity shall include a means for headquarters employees to utilize the Internet for information gathering and for communications with other companies and customers. Salespeople shall posses both the

ability to access the Internet while away from headquarters on business, and to remotely access the corporate database so that they can input or query information during those times.

This plan shall include a detailed analysis of the company's communications requirements, to ensure that all user needs are met, but that no excessive capabilities are designed or purchased that are not really needed. The assumption is being made that a telecommunications contractor shall be hired to execute the effort. A general network architecture shall be developed based on these requirements, with types of components required identified. As requirements are allocated to those components, specific products shall be selected which best meet the requirements. As necessary, alternate designs will be evaluated and the best selected. The remaining phases of the project (installation, testing, project management, etc.) will be described in detailed plans and schedules but will not be executed in the scope of this project. The details of the systems engineering process to be followed are found in Section 2.

1.3 Issues to be Considered:

Ease of Use - The corporation is not very computer literate. None of their current computer systems are really state-of-the-art, but all follow tried and true methods of transaction processing and office automation. The solution should keep the capabilities of the users in mind.

Cost vs. Capability - It would be easy to implement an option to provide them with the "kitchen sink" or a standard package of Internet connectivity and services which contains everything a company "should" need. The corporation is concerned that all money spent on the system be justified as meeting a real need.

Privacy - The corporation keeps new product formulas on the LAN, as well as sensitive financial and contracts oriented data. They want to make sure that developing an external connection does not allow competitors or others to access this data.

Room for Corporate Growth - Over the lifetime of the enhanced network, the company expects to grow in business and employees. Therefore design of an architecture and selection of components should allow room for corporate expansion.

System Reliability and Supportability - Once the external electronic connection is established, employees will come to depend on it for job performance. It is important that the reliability rate remain high, requiring low levels of maintenance from the over-tasked administrative staff.

Types and Volumes of Communications Required - The initial steps of gathering user requirements are important because they will dictate what equipment and performance levels are required of the system as a whole.

2. Overview of the Systems Engineering Process

2.1 Introduction to Systems and the Systems Age

The world in which we live consists of a never-ending hierarchy of interconnected systems. Both in nature, and in the man-made world, anything that may be experienced may be decomposed into multiple layers of subsystems and components, and then analyzed in great detail. In simple terms, a system is a set of interconnected components working together to achieve a common objective. A system may be conceptual, such as a system for constructing governmental policy; or extremely concrete, as in the physical system of forces and materials making up a bridge span. It is obvious that in using such a general definition, an infinite number of diverse systems may be studied and understood using the general methodology.

While it now appears obvious that we are surrounded by a multitude of systems, and therefore much effort should be applied to their understanding, this was not the case until very recently. For most of the scientific and industrial ages, those who sought to understand and improve on their environments devoted much effort into breaking everything down into the smallest possible components and then performing analysis on those components. In the industrial age, these low level components were replaced by machinery whenever possible in a search for efficiency of performance. Little effort was placed on the understanding of the interactions and dependencies of these components and the systems they form. In the second half of the twentieth century, this school of thought began to change. Scholars and scientists realized that similar principals could be applied to elements of nature as to elements of machinery, and they began to look at objects and components as parts of the larger system that contains them. This approach takes into account the interrelationships between all components, and ensures that desired performance improvements can be optimized across an entire system rather than for one component at the expense of another.

When this systems approach to understanding problems is applied to traditional engineering realms, it has yielded a formal analysis process called the Systems Engineering

Methodology. The beauty of this methodology is that it can be scaled to be applied to any problem, large or small, and ensures that no important aspect of design is forgotten. The methodology will be described in the following sections, and applied throughout this project to a problem of telecommunications technology.

2.2 The Systems Engineering Lifecycle

The process of performing systems engineering may be broken down into several distinct phases which span the time period from the initial idea for a project through its design and development, to the final phase of supporting and maintaining the resulting system throughout its useful life and through its eventual retirement. (Blanchard) The entire process rests on the foundation of the need for a particular system. A problem or deficiency is identified, and captured in detail in a list of requirements. The systems engineering lifecycle is utilized to ensure that all of these requirements are met in the finished product, and therefore the prior need is fulfilled. Accordingly, a great deal of time is invested up front in the development and validation of these requirements, and then in planning how to best meet them. The implementation or development of the system is more efficient and then completed in a shorter period of time because as many problems and risks as possible were well-understood from the start, and they have been addressed and planned for in advance. In addition, this process ensures that a team of engineers can work together on a project. Information about the system as a whole is captured and documented so that all team members can possess a clear picture of the system. Requirements and design components are modularized so that responsibility for their completion may be split between team members without fear that the completed product will have incompatible parts. The high-level phases of the systems engineering lifecycle are shown in Figure 2-1.

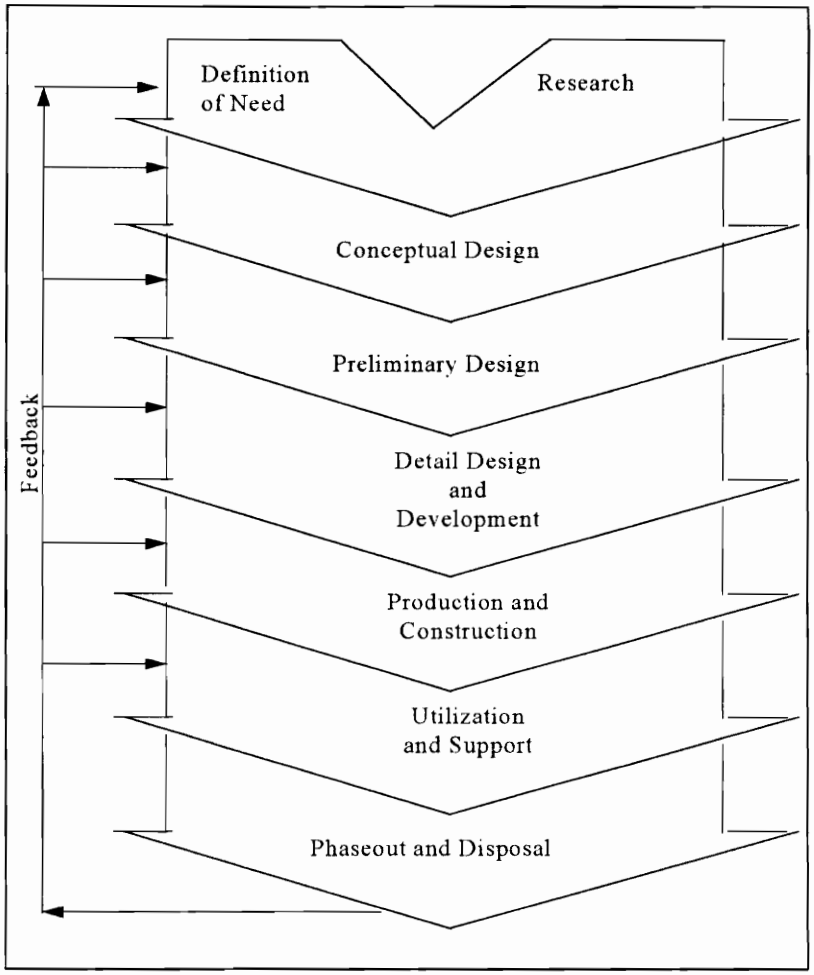


Figure 2-1: The Systems Engineering Lifecycle.

2.3 Conceptual Design Phase

This first phase of the process is critical to success of a systems engineering project. If the need for a system is misunderstood or not fully captured, then it is impossible for the finished product to meet all of its expectations, and sometimes even to be of any use. Other elements of this initial phase include performing feasibility studies of the proposed technologies, and clearly documenting the operational and maintenance requirements for the system.

Before any systems engineering project may be designed, the project management must be sure that the need for the project is fully understood. The need is generated by the end-users of a system who desire some change or improvement in the current

deficiencies of the existing system. This deficiency may be real (for example when a bridge has be worn by time and use and is no longer structurally sound) or perceived (as when a new and flashy technology is introduced which achieves the same goals as an existing technology, but in a more visually attractive manner). Since there will be many decisions to be made during the design process and often several alternate designs will be proposed and considered, it is important that all aspects of the users' need be well understood so that each alternative may be critiqued by its success in fulfilling the need.

To ensure the need is well understood, several items must be considered. The current problem or deficiency must be well understood and documented. A deadline for the replacement capacity must be established. The resources available for implementing the new system must be determined and obtained. And finally, the priority of the new system must be established so that its place with respect to all other ongoing projects is clear. None of these items may be determined by the engineers alone; close communications must continually take place with either the customer of the project, or the end-users of the system.

Even at this early stage of the process, it is sometimes advisable to perform feasibility studies of various technologies which may be used in the implementation of the system. This step is far from designing solutions to the problem, but it begins addressing potential problems and alternatives and results in a proposal of the technology which would be most appropriate as the foundation for the project.

The next step of defining and documenting the system requirements is also critical. The engineers must develop a full understanding of the conditions under which the system will be operated, such as the location and physical environment, the amount and patterns of expected use, any restrictions on size or weight of the finished product, and the full details of the mission that the system is expected to fulfill. The product of this information gathering is a concept of how the finished system will be operated, usually expressed in a list of the requirements of the system, which should be written in clear language, so that they can not be interpreted in multiple ways.

A second product of understanding the operational requirements is and understanding of the maintenance requirements necessary to support the system

operations. The most cleverly designed system loses all utility if it is awaiting repair more often that it is actually be used. To avoid such a scenario, plans for the maintenance of a system occur early in the design process and are kept in consideration at all later phases and when deciding on design alternatives. The maintenance concept should address the levels of system maintenance; what activities can be performed by the users of the system, and which must be handled by specialists or even by the manufacturers of the system components. This information will provide a basis for supportability, reliability, and maintainability requirements of the system.

At the conclusion of this phase, all members of the design team should understand the system they are developing. At this point the system is not yet described in terms of individual components and interfaces, but by the functionalities that it will provide for the users. This understanding is demonstrated and proven by successful completion of a Conceptual Design Review. The tasks involved in the Conceptual Design phase are shown in Figure 2-2.

2.4 Preliminary Design Phase

When the concept of the system is well understood, the systems engineer is able to begin performing a functional analysis of the system. This process ensures that all discrete events which must take place to meet the objectives of the system are addressed and taken into account. It also ensures that all portions of the system development are remembered, all portions of the system are defined, and interfaces with interdependencies are identified. The functions of a system are best addressed with a series of functional flow diagrams. These graphics depict what is to be accomplished through the use of the system. The functional requirement will later drive the development or acquisition of components of the system best suited to meet these functional needs.

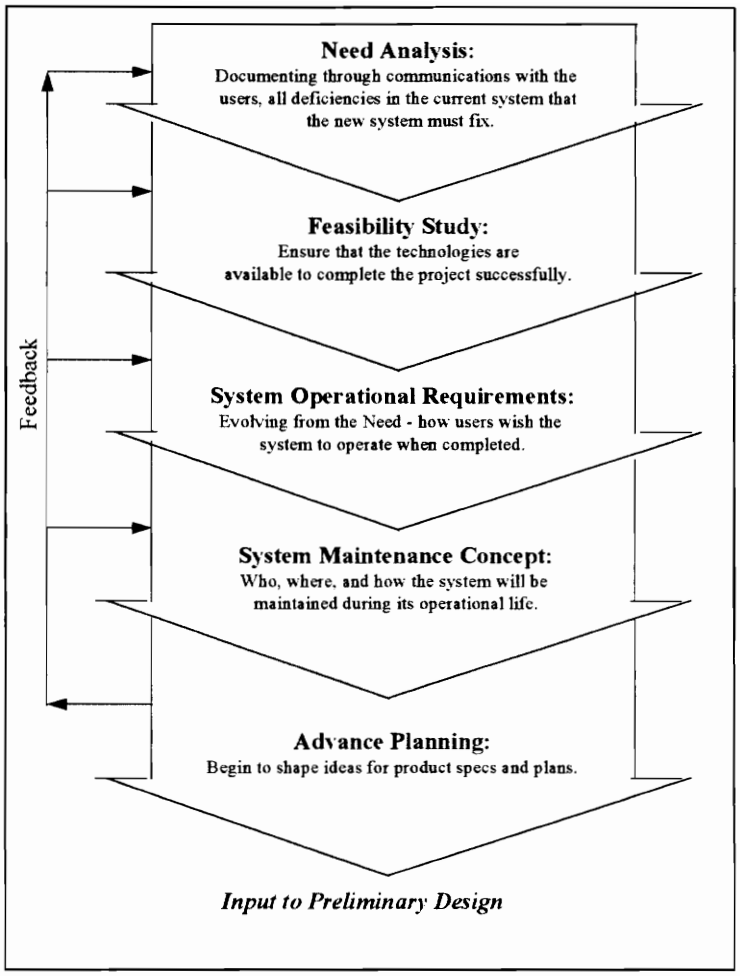


Figure 2-2: Conceptual Design Phase.

Functional flow diagrams may be broken down into two categories; those depicting operational functions, and those depicting maintenance functions. Operational functions evolve from the operational requirements developed in the prior phase. The diagrams start at a high level of detail, showing the entire life of the system, and then each function may be broken down into a more detailed diagram of its functional components. Sufficient detail has been achieved when the designer can begin to derive packaging concepts, and can begin to make recommendations on the components required to build the system. Maintenance flow diagrams, in turn derive from the operational flows, and from the maintenance concept previously defined. Various operations may either succeed or fail, and various maintenance functions are required in the case of failure. Maintenance

flows should address both scheduled, and unexpected maintenance, as well as support maintenance functions.

The next step in translating requirements into design criteria involves allocating these requirements to low-level portions of the system. The designer divides the system into appropriate subsystems, units, and possibly even to the assemblies of the units as determined to be appropriate. The engineer determines what requirements these elements must fulfill in order to meet the aggregate requirements previously defined for the system. This process eliminates any uncertainty of the role of a component in the whole system design. The expectations of each element are well-defined, therefore a different team of engineers could be assigned responsibility for design of each subsystem and there would be no danger of the finished products integrating improperly when combined into the complete system.

Now that an idea of the system components which will be required has been developed, two final steps of the preliminary design can be useful in validating correct choices for these components. Trade-off studies involve developing a set of evaluation criteria for a particular system element or component (usually derived from the requirements) and then measuring several alternatives against those criteria. This measurement may be accomplished through use of mathematical models or simulation. Or, in terms of selecting a commercially available product, research may be performed to identify available products and their specifications may be compared to determine which meets the largest set of system requirements at the most acceptable cost. Synthesis involves integrating the selected components into a coherent entity. Additional analysis is performed on the system components and the results feed as input to the detailed design phase. To ensure that the preliminary system design has been performed correctly, and that the results are meaningful, a System Design Review is held. Figure 2-3 illustrates a summary of the Preliminary Design Phase.

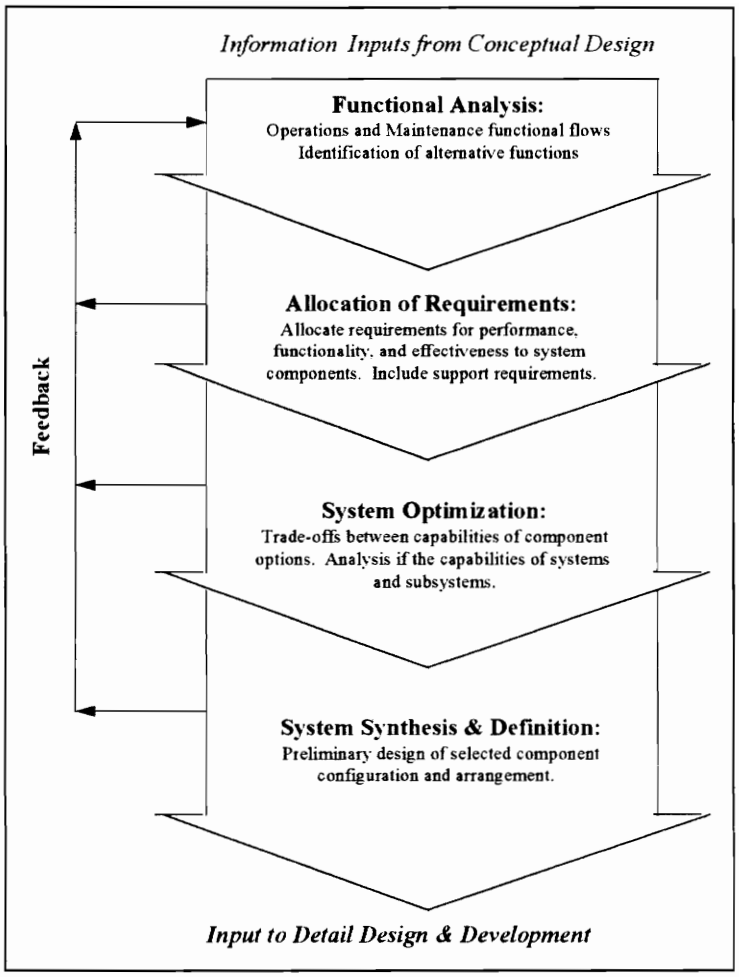


Figure 2-3: Preliminary Design Phase.

2.5 Detailed Design Phase

This final phase of system design, shown in Figure 2-4, uses the concepts and definitions produced in previous phases, and adds further detail until the entire configuration of hardware, software, and information can be implemented. The detail design requirements are listed, which must be consistent with the operational and maintenance requirements defined in the concept stage, and must support the allocated requirements determined in the preliminary design stage. Special effort must be made to ensure that these design constraints include provisions for all aspects of human use; support for reliability, maintainability, human factors, supportability, economic feasibility, and social acceptance can not be overlooked.

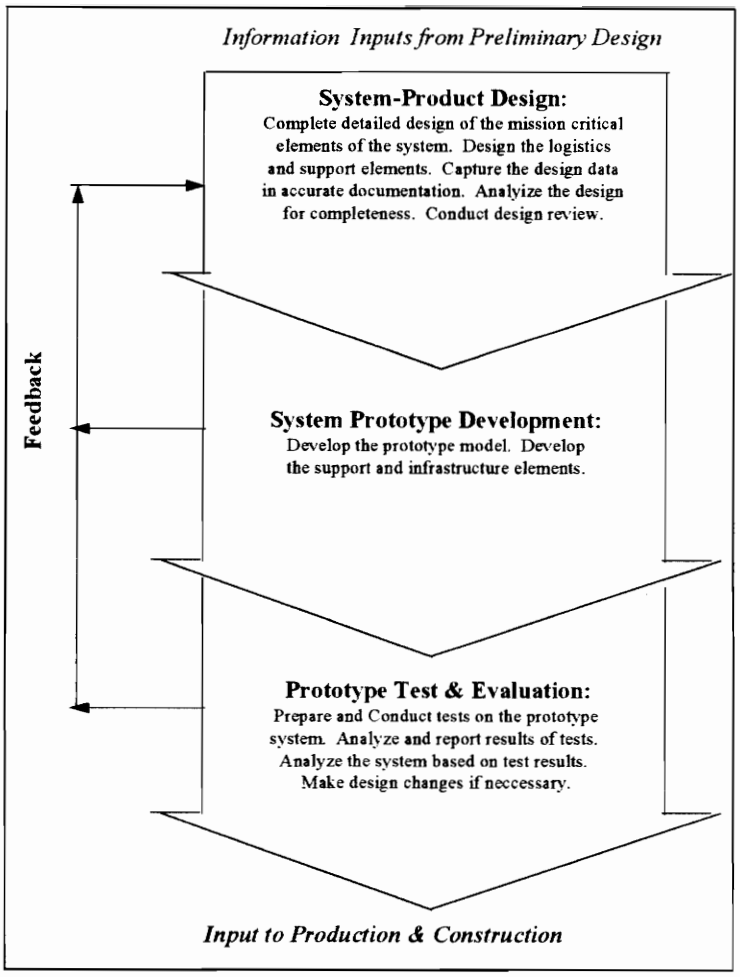


Figure 2-4: Detail Design and Development.

The actual activities of designing and implementing the system may now take place. First the design team must be established and responsibilities defined. To do this, a plan will be developed which describes the structure and organization of the engineering team and the procedures that will be put into place to manage its operations. A detailed schedule will be developed that demonstrates the time period in which each activity must be completed in order to meet the milestones established by the customers or end users.

The details of the system design are now driven out through an iterative process of selecting or creating system components that best meet the requirements, and then developing and defining their interfaces with other components. As this design process is taking place, all aspects are well documented through text and diagrams. Sometimes tools such as documentation databases and CASE (Computer-Aided Software

Engineering) tools are used to assist in the documentation process. At the completion of this process, there should be no further decisions to be made regarding system implementation, and the plans and documents could be passed off to a separate team of people (programmers, computer services technicians and installers, integrators of electric components, etc.) and these people should be able to perform the implementation of the system, even without an in depth knowledge of the design process which has preceded their involvement. At times, it is helpful to create a prototype of the system before actual construction takes place, so that difficult implementation features may be tested in a risk-free environment. If this is the case, it is important to provide a smooth migration path to the operational system.

There must be a means of testing the finished system design to ensure that all of the requirements were in fact met. Therefore, one of the critical design documents which must be completed and utilized is the system test plan. This document explains the philosophy for system testing, describes how testing will take place so that no vital issues are overlooked, and will provide a standard format for testing procedures and for documenting test results.

At the culmination of this phase, a formal design review is held to ensure that all stockholders in the project and all participants agree that the design is successful and correct and that it is ready for implementation.

3. Conceptual Design

3.1 Statement of Need

The employees of AmeriClean Corporation need to have electronic remote communications capability from their company headquarters, and for employees traveling at various locations in Northern America.

3.1.1 Regulatory Environment

Due to the popularity of graphical user interface tools and the World Wide Web, a great wealth of information is being made publicly available on the Internet for anyone who has access to the service. AmeriClean has several reasons to access this information which cannot be fulfilled in the current system configuration. Because they manufacture and sell products made of various chemicals, some of which are dangerous in certain combinations, there are many government regulations and laws that must be followed. These laws regulate safe ways in which to handle and dispose of potentially dangerous chemicals without harming either the users or the environment. In the past, government agencies such as the EPA (Environmental Protection Agency) and OSHA (Occupational Safety and Health Association) published the current regulations and guidelines once each fiscal year in hard copy format. As new bills were passed into law during the year, change pages would be printed and distributed. In order to receive these documents, companies would often subscribe to the mailing lists of various agencies, in which case they would receive the documents in the mail periodically. Unfortunately, no single agency compiles and maintains all of these directives in a single document, so many relationships needed to be maintained. Some of the agencies did not want the trouble of maintaining mailing lists, and therefore simply published yearly catalogs of the current regulations, and companies would have to request these catalogs and order the applicable documents.

Today, the government agencies are following a trend of efforts to cut costs and perform their missions with fewer employees. The agencies which enforce the regulations for chemical handling are refusing to publish hard copy documents, and often even refuse

to cover the costs of creating and mailing out computer disks. Instead, they are making these documents publicly available on Web pages and for download. Companies are being given deadlines by which they must develop Internet capabilities in order to receive the documents; after that time their ignorance of current regulations shall not exclude them from the penalties of law.

These penalties can be quite severe, especially for small companies which cannot afford to lose revenue. If a corporation is caught, in a government inspection or audit, handling or disposing of hazardous chemicals in an illegal manner, the fines for such crimes range from $100,000 to $100,000,000. In addition, a company's reputation is harmed because the government publicizes lists of offenders on a quarterly basis. There is also the possibility of a company being sued if a factory worker or an end-user of a product is injured due to improper labeling. In the past, such personal injury lawsuits have had to be settled out of court by AmeriClean's competitors for several million dollars. AmeriClean executives have assessed the risk of either receiving a fine or being the defendant in such a lawsuit to be more than the company could survive without going bankrupt due to revenue loss and loss of business. Therefore, they are making every effort to comply with the government and to receive these regulations in a timely manner and in the recommended format.

3.1.2 Additional Information Research

Environmental and safety agencies are not the only organizations which publish information of interest to AmeriClean on the Internet. In the past, only technical or computer-oriented organizations made information about their products and operations available on the Net. Today, companies selling everything from cars to beer have home pages where consumers can read about their products and prices, and can submit e-mail requesting additional information. Several of AmeriClean's largest competitors are huge conglomerate corporations which manufacture not only cleaning supplies, but paper products, snack foods, and even diapers. These companies are enough of a presence on the American business scene, that they have Web pages which provide a combination information source and advertisement. AmeriClean marketing personnel are anxious to

have access to this competitor information so that they can be aware of forthcoming new products before they hit the shelves, and can compare their own financial performance to trends demonstrated by other companies.

In a similar manner, some of AmeriClean's suppliers are placing information on the Internet. Those who sell raw chemicals are facing some of the same regulations and laws that manufactures of cleaning products do, and therefore are putting information about safe handling of their chemicals on the Net. In this way, they hope to attract new business by developing a reputation for responsibility and concern about their customers. AmeriClean can use this information to their advantage when selecting and ordering chemicals. In addition, some suppliers of plastics and packaging, as well as shipping organizations advertise their wares on the Internet, and AmeriClean can use the information to compare prices. Following this trend, the AmeriClean marketing would like to place their own home page on the Web so that current and potential customers could find out more information about their products and prices, and they can differentiate themselves from other small to medium sized businesses who still rely on print media and trade journals for advertising.

3.1.3 E-mail to external individuals

AmeriClean currently has an e-mail system in operation on their internal corporate LAN. In the year and a half that it has been in use, employees have begun to depend on the service for keeping in touch with members of other departments and those located in different parts of the headquarters building. It has been much easier to get needed information from people when they do not have to be caught at their desks by the telephone, and sometimes when they can read messages and requests in their own time, and reply with desired business information when they are ready. The old paper memo system which was replaced by e-mail was not nearly as efficient. A secretarial staff used to type up requested memos and circulate them to employees on written distribution lists. The entire process took significant amounts of time since employees did not create and distribute their own memos, and requests for information usually resulted in arrangements for face-to-face meetings rather than repeating the memo process in reverse.

Now that all members of the corporation are used to quickly composing and transmitting e-mail messages that provide information or request assistance, and recipients have access to these messages within a few minutes, the employees need to extend this capability to the outside world. In particular, employees who frequently communicate with customers or suppliers would like to take care of routine matters without always having to place a personal phone call, or sacrifice the time needed to send a letter. Sales people would like to confirm visits to a customer location a day or two beforehand with a brief e-mail message. Marketing would like to send changes in pricing policy or product lists to a distribution list of current customers which would result in reduced postage costs and in time savings. Those employees responsible for procurement of materials from suppliers would like to be able to arrange shipment details and receiving schedules via e-mail. In addition to time savings, each employee is then able to maintain an electronic file of communications records on their own PC. Less information is lost through inefficient paper filing, and an audit trail is maintained where each employee can easily access the information. Research has indicated that approximately 12 - 16% of the company's $13,000 per year total telephone tolls and postage expenses could be eliminated by changing some traditional communications to e-mail. Although such numbers will not make or break the company, these saving can be applied elsewhere to advertising efforts for example. Increased communications via e-mail will be distributed among more employees so that no single group is over-burdened.

3.1.4 Customer service

3.1.4.1 E-mail "hot line"

AmeriClean currently maintains a traditional 1-800 number hot line on which to receive feedback from consumers regarding both positive comments and negative complaints. Unfortunately, this system has been found to be very inefficient. The line needs to be staffed at all times by someone who is knowledgeable about all of the company products and is able to represent the company in a friendly and professional manner through all telephone conversation scenarios. Since the company's consumers live

in various time zones across the western hemisphere, the line must be staffed beyond normal business hours in the headquarters time zone in order to be accessible to everyone. The time frame of the incoming calls is not predictable or evenly distributed. Records of calls received over the past year demonstrate that out of a given day, the telephone operator spent approximately 2.5 hours of paid working time waiting for phone calls without performing any useful function. Since this operator is earning a $8.00 per hour salary, this translates an average of $4,900.00 lost per year. However, when he was handling a call, customers would often hang up without getting through due to frustration and the length of time they were being kept on hold. This lack of accessibility for customer service issues creates the perception that AmeriClean does not care about their customers, and can result in lost business. A small company cannot afford to lose established customers, and a survey performed in 1993 to 1995 of all canceled accounts indicated that 70% of those accounts were canceled because the level of service was unacceptable and could be better provided by a competitor.

In a specialized use of external e-mail connectivity, AmeriClean wishes to establish an e-mail address specifically for questions and comments. In this manner, no customer would ever find themselves unable to reach the company except in the unlikely event that servers were unavailable and connectivity was down. Each message could be replied to individually, and messages could be stored which answer frequently asked questions in order to make such responses efficient and consistent across all requests. No operator would need to be applied full time to this task, rather all received requests for information could be parceled out to several employees who are experts in specific areas such as product safety, instructions for use, dissatisfaction with performance, etc. Answering these requests could be interleaved with their existing responsibilities, and since customers are not requesting information in real time, this additional responsibility could be scheduled in between employees other time-critical tasks. In addition, archives of received e-mail messages could be stored as a concrete record of customer communications. There would no longer be reliance on the operator to capture the pertinent details of a customer request correctly; the message would be stored in the customer's own words. Research

could be performed on these messages in the future to ascertain trends in customer requests and therefore needs for product improvements or educational campaigns.

3.1.4.2 Electronic order placement and order tracking

Many of AmeriClean's current customers (including grocery and convenience stores and wholesalers) are beginning to practice just-in-time inventory management. They cannot afford to store excess amount of their wares, or waste quantities which do not sell or are stocked beyond the guaranteed date on the packaging. On the other hand, these organizations also cannot afford to lose sales because they do not anticipate the demand for particular products, and as a result, run out during a major promotion or due to unexpected demand. To keep up with such a complex inventory scheme which does not afford room for error, the customers need their orders to reach cleaning product suppliers quickly and accurately, and have the shipment of the order initiated immediately upon receipt. Many of these customers are operating their own computerized inventory management systems to track the availability and order quantities of hundreds of products at any given instant. If they were able to link their product ordering to such an existing system, then hitting a specified level of inventory in the database could automatically trigger an order. Therefore little human intervention would be required and errors could be reduced. Some customers have expressed a desire to be able to track a shipment in progress, similar to the service performed by Federal Express or UPS. By being able to call up information about a current order on-line, purchasing employees would be able to easily convince management that inventory issues are under control.

The customers would like to be able to utilize a form of electronic commerce or electronic data interchange (EC/EDI) to place their orders for AmeriClean products electronically in order to meet these needs. Order placement would be quick and could wait until the quantity of products needed was accurately calculated. In addition, those customers with AmeriClean accounts could transfer funds to pay for the order electronically between bank accounts. This would also streamline the process and eliminate problems with bill collecting and delinquent payments. Information on orders could be linked to a form on a Web page so that customers could enter an order number

and receive information on the status of their shipment. The driver for these changes is the fact that AmeriClean's single biggest customer, the Stupendous Mart chain of retail stores and wholesale clubs, has mandated that they will no longer purchase from suppliers who do not support EDI orders. Obviously, AmeriClean is not the only available source of cleaning supplies, so if they do not provide this capability, their competitors will easily absorb the market shares. Stupendous Mart sales make up 20% of AmeriClean's total yearly business, so they cannot afford to lose this client. In addition, if the desire for EDI orders and shipment tracking is ignored today, other customers will probably follow the lead of Stupendous Mart and their business will eventually be lost as well.

3.1.5 Remote Database Access

AmeriClean currently has in operation a very efficient corporate database in which they track data on inventory, orders, shipments, and current customers and suppliers. This system has greatly increased the accuracy of data which each employee has access to, and has streamlined the process of accepting and filling orders. However, the bulk of the orders received are not for a consistent product volume, placed at regular time periods. Rather, the orders fluctuate based on consumer demand and on the efforts of the sales force to generated new business and increase the orders of existing customers. While some sales are made over the phone or in correspondence, the bulk of this new business growth is generated by personal visits by the sales people to the customer locations. To make such trips more efficient, sales people generally visit anywhere from four to twelve customers per trip, depending on proximity and amount of time required to complete business transactions.

During these trips, sales people are recording order information, satisfaction levels, and gathering information about the store and competing products on paper forms. When they complete a trip and return to headquarters, the salespeople enter the information into the database. By that time, some of the information is up to a week old. It is even possible that orders may be accepted for a quantity which was available when the sales trip began, but which has since been promised or even shipped to other customers, making it impossible to honor the order until quantities are replenished. In addition, the time lapse

between information receipt and information entry often introduces errors into the data. Sales people either remember or record the information gathered on a trip incorrectly, and when errors are identified at the home office, too much time has passed and the appropriate customer is not always available to ask questions.

It also would improve accuracy and speed of placing new orders to be able to initiate orders directly into the corporate database from the road. Each sales person could be issued a laptop computer which contained all of the required forms to record trip data. They could fill out the information while meeting with customers or immediately afterwards. Once each day, they could remotely access the corporate database and download the day's information. In this way, new orders could begin to be processed while the remainder of the sales trip was still in progress.

All of these reasons have been identified as deficiencies in the current AmeriClean system of performing information processing only within the organization, and therefore are documented needs for external Internet connectivity with the rest of the outside world.

3.2 User Functional Requirements

In the preceding section, the business needs which prompted initiation of this project were discussed. In this section, those needs are summarized in functional terms, independent of the technologies which may be utilized to implement them.

- AmeriClean employees need to be able to transfer files of information from remote, computer systems to the company's private network. These files can range from 10 kilobytes to 5 Megabytes in length and may consist of both ASCII text and binary data.
- There is a need to gather information about competitors and suppliers from publicly available electronic sources. This information must be readable, transferable, and printable, with fast performance requirements of access within 30 seconds after information request, and transfer of information within two minutes of request.
- Employees require the capability to communicate with external organizations in written, electronic format. Based on the amount of mail, fax, and telephone correspondence which users have indicated could be replaced electronically, it is

anticipated that between 80 and 450 electronic communications would be created and transmitted each day. These messages also consist of ASCII text and binary data, and must be received by the recipient within two hours of being sent.

- AmeriClean salespeople need to be able to read and write to information stored in the computerized database at company headquarters in real time while traveling on business. This interaction must not only include access to status data, but the ability to initiate and track the status of product orders remotely.
- AmeriClean needs to make information about its products available to potential customers located across the country without individual interactions requesting the information. This information must be accessible to 50 individuals simultaneously, and allow these individuals to read information as well as transferring order information to AmeriClean headquarters.
- AmeriClean needs to protect company proprietary data and product formulas from any external individuals who utilize the communications capabilities just described.

3.3 Operational Requirements

The detailed analysis of the need which AmeriClean has for external electronic communications can now be captured in specific operational requirements for the system. By documenting what the users require of the finished system, it is possible for engineers to decompose these statements into qualitative and quantitative measures of what must be provided and designed to accomplish the implementation of an acceptable system.

3.3.1 Mission Definition

There are two primary missions that the enhanced networking communications system at AmeriClean shall support: it shall provide AmeriClean employees with a capability for remotely accessing information sources, and it shall allow external users (who are not AmeriClean employees) access to information about the company's products and services.

3.3.1.1 Employee Communications Requirements:

Electronic communications: AmeriClean employees have become accustomed to communicating with each other via electronic format. Driven by user familiarity with this capability and also by requests from business contacts for an e-mail address with which to correspond, the new system needs to extend this capability to provide e-mail over the Internet. The company currently uses Microsoft Mail as their e-mail application. This product does not use an Internet compatible format for mail messages, so the system will either have to include a different protocol, or provide a means of converting the Microsoft format to a format which can traverse the Internet. Employees do not wish to have separate accounts for Internet mail and local mail; they wish to be able to organize all received mail messages in a single directory on their user accounts, and to have the fact of whether a message was created internal to the company or external to the company be transparent in how they must handle the message. All of the company's 50 employees need access to this capability.

Information Gathering: Some employees need to be able to read information stored on the Internet via the World Wide Web. The need requires access to a Web browser which properly display graphics and text. Capability to display video or sound is not required. Access to the Web shall be available at the user's workstation / desk, and shall be provided during all hours that he is at the office. Response time for accessing and viewing pages must be high. No user should be required to wait more than 30 seconds for the site supporting a given page to be contacted. Depending on the amount and complexity of graphics on the desired page, the wait to view the page in its entirety shall not exceed two minutes. Since access to the Web includes access to an infinite number of sites which are not business-related and at which an employee could waste time, requests for Web access will be evaluated by the System Administrator before being met. It is estimated that 75% of employees will be provided with this access, but the system shall be designed for the possible situation where all employees wish to utilize the service at the same time.

Information Publishing: Some information about the company must be made available for the external community to read. This is done by hosting the data on an

information server which accepts connections from the external world. The World Wide Web home pages shall be utilized to support incoming requests for this information. The System Administrator shall be the only employee allowed to write information to the public information server. In this way, it may be ensured that no company proprietary information is being made available. Any department which wishes to place corporate information on the Web shall submit the data to the System Administrator, who shall confer with management or with other departments at his discretion to ensure that the information revealed is harmless.

File Transfer: Again only a portion of the AmeriClean employees need to be able to download large collections of information from remote sources. For example, as described in the Need Statement, there is a growing need to download electronic formats of government regulatory documents and guidance. The finance department will also need to download tax guidance and input forms from local, state, and federal government. The System Administrator will need to download new versions of software or bug patches from the vendors. These types of documents will be too large to be efficiently transmitted as an attachment to an e-mail message. Therefore, those employees who can demonstrate a need to download large documents will be provided with the client to use a file transfer protocol.

Remote Access: The traveling sales force needs to access the corporate database for information on current product inventory levels and prices while away from corporate headquarters. They also need to be able to input data collected from sales meetings into the database to place new orders while still in the middle of a trip. To meet these needs, each salesperson shall be assigned a laptop computer which shall be loaded with the same versions of software as used on the headquarters employee's computer workstations. Electronic forms shall be stored on the laptops which make it simple for the salesperson to enter information about a customer account while in the middle of a sales meeting. Information about the meeting and about orders must be stored locally until such a time that the salesperson can access the corporate headquarters remotely via modem and download the collected information.

3.3.1.2 Non-employee Communications Requirements:

External Internet users shall be provided similar communications capabilities to those of AmeriClean employees. In particular, they shall be able to send e-mail messages to AmeriClean employee accounts, and can receive messages generated by AmeriClean employees. They shall be able to access information servers from the Internet in order to read information about the company which has been made publicly available.

3.3.2 Physical Parameters

The physical parameters of the network components are not a primary design constraint, because they will not be frequently transported and do not need to reside in a constricted location. Workstations currently reside on each employee's desk, so additional space will not be allocated for the user interface to the network. All servers and central network control machines shall be located within a central computer room which is 12' by 16' in size. Racks shall be employed to use the vertical space within the room. Connections between machines shall be clearly marked in order to ease future system maintenance efforts.

The building and especially the computer room shall be climate controlled in order to dissipate the heat generated by the computers. All machines shall operate correctly with a temperature range between 30deg and 100deg F. They must function in conditions of 70% humidity or less, and operate on US standard 120V power supplies. The components should be sturdy, and able to withstand a force of 20 foot-pounds.

3.3.3 Use Profiles

The employees located at AmeriClean headquarters in Northern Virginia work a standard eight-hour business day. They have some flexibility to stagger their starting time and ending time to accommodate family responsibilities. Employees may arrive for the day between 6:30 am and 9:00 am and therefore leave between 3:00 pm and 5:30 pm. Allowing for the occasional need to work overtime, all portions of the system that headquarters employees use (workstations, file server, mail server, Internet access) must be available between 6:30 am and 7:00 pm. Within this time frame, the level of usage is

not constant. The bulk of the employees are present between 8:00 am and 3:00 pm with usage peaks between 9:00 and 11:00 in the morning and between 1:00 and 3:00 in the afternoon. Services on the headquarters network drop significantly over the weekends, with an average of 3 - 6 employees wishing to use the system on any given Saturday or Sunday. These patterns are depicted in Figure 3-1.

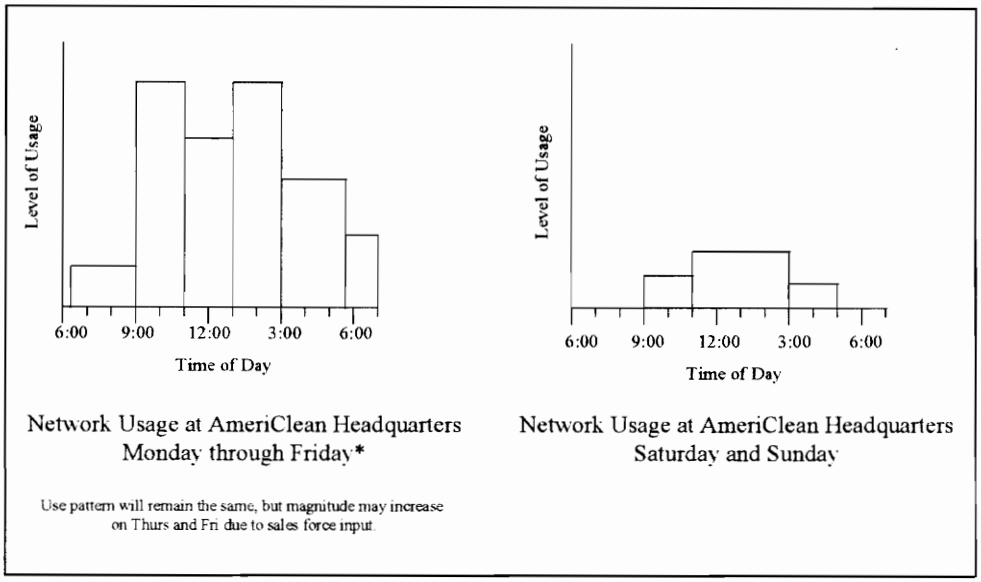


Figure 3-1: System Usage Profiles.

The traveling sales force will utilize the system in slightly different patterns. Much of the business day while on a trip is spent either traveling or meeting with customers. A low level of usage occurs during the day, mostly to type data into a laptop computer, or to remotely query the corporate database for current product and pricing data. System usage increases significantly during the early evening hours from 5:00 to 8:00 pm when the salespeople download the day's orders and collected customer information from their laptops to the corporate database at headquarters. In addition, most salespeople travel during the beginning of the week and return to headquarters to analyze and distribute collected information, train on new products, and create trip reports on Thursdays and Fridays. Therefore, usage of the system from company headquarters increases on those days, while remote access from sales trips decreases.

Finally, the usage patterns of external individuals accessing information about AmeriClean are very unpredictable. Customers and suppliers will send most of their

electronic communications during business hours, but those hours will vary depending on the time zone of the sender. Others will utilize home computer systems to complete work activities after normal business hours. Finally, end-users of AmeriClean's products and others who are merely curious will access the company's Web page at any hour of the day or night. Graphical representations of the usage patterns are shown in Figure 3-2.

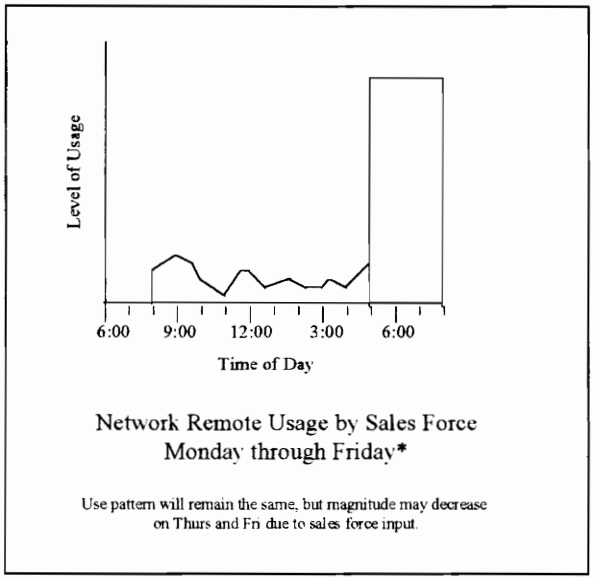


Figure 3-2: Usage Patterns for Sales Force.

In summary the system, especially the information servers, shall be maintained in an operational state 24 hours a day, seven days a week when possible. But the bulk of the administrative support for the system shall be applied during the high-usage periods described above and depicted in Figures 3-1 and 3-2, so that the system is ensured to be operating as expected during those times.

3.3.4 Operational Life

The lifetime of a personal computer today is considered to be two to five years before its capabilities are unacceptably obsolete in relation to the rest of the marketplace. This network architecture system is expected to remain in use without significant modifications for five years. During that time, software upgrades will be performed as new versions of supported applications are developed which fix current bugs or add additional capabilities. Additional workstations and user accounts may be added to the

system as the company grows. But no significant hardware investments shall be required such as replacement of servers, firewall, etc. At the end of the five year period, an analysis of the system shall be performed to address performance issues, user satisfaction, and new derived requirements for communications, and any new technologies which have developed which can improve the quality or efficiency of the communications system. At that time, management shall decide whether an additional design and development effort is needed to upgrade or replace the system and will create a plan accordingly.

3.3.5 Security Concerns

Providing connectivity to the Internet can be both a blessing and a curse. While it provides AmeriClean with access to information vital to successful business operations, it also provides a path for untrusted users to access sensitive corporate information or to cause harm to the network and its contents. For these reasons, security is a high concern when implementing the external connectivity. The system must ensure that only recognized AmeriClean employees are granted interactive access to data and files on the network. Information which is meant for external users will therefore be placed on physically separate machines which can be safely sacrificed without danger to the network as a whole. Users who have accounts on the system must provide their user ID and password to prove their identity before being granted access to network resources.

The system shall provide the capability to audit suspicious activities. This audit serves two purposes; to identify and stop an attack on the network while it is in progress, and to provide a trail for review if the system has been compromised to attempt to determine who performed the attack and how to avoid it in the future.

The system shall restrict the protocols and services which it allows incoming from the Internet. The fewer services supported, the fewer which must be maintained and policed for unexpected and unauthorized actions. In addition, some protocols are inherently risky, either because there are known security holes in their programs or because they allow the external user too much power (X Windows, and incoming telnet connections are examples). Therefore, only services which are absolutely required by the

AmeriClean users and which are well-understood by the System Administrator shall be supported on the network.

3.3.6 System Operational Requirements List

3.3.6.1 Electronic Mail:

- The system shall expand each employee's e-mail capabilities to include the ability to send e-mail to and receive e-mail from the Internet.
- The system shall include an e-mail client application with an intuitive graphical user interface.
- The selected e-mail application shall be compatible with the existing software and operating system.
- The system shall be able to communicate e-mail to and from the Internet, using compatible formats and protocols.
- The system shall allow each employee one Megabyte of system memory in which to store sent and received e-mail messages.
- The system shall store the addresses of all local users in an "address book" for ease of reference.
- The system shall provide the capability for users to create their own distribution lists of e-mail recipients both within and outside of the company.
- The mail server shall be operational 24 hours a day, in order to receive messages for employees. These messages will be made available to the appropriate user when he first logson to his workstation the next business day.
- The system shall reject incoming messages from the Internet which do not contain the user ID and Fully Qualified Domain name of the message originator.
- The system shall allow attachment files to be transmitted with e-mail messages created on the AmeriClean network.
- The system shall be capable of transmitting and forwarding encrypted messages.

3.3.6.2 File Transfer:

- The system shall allow ten users within the company the ability to simultaneously download files from external servers.
- These users shall demonstrate their need for the capability to the System Administrator before being provided access.
- The system shall download a 1 Mb file within 15 minutes.
- The system shall include an information server which shall make files of information available for external Internet users to download.
- This information server shall be distinct from all other network components, so that an external user can not access any information other than that which is made specifically available for distribution.
- Only the system administrator shall be granted write access to the information server.
- The information server shall support up to 50 simultaneous connections from the Internet.
- If more than 50 connections are attempted, the system shall reject additional connections without disconnecting existing sessions.
- The information server shall be in operation 24 hours per day.

3.3.6.3 Protection from the Internet:

- A network component or system of components shall be utilized to create a "firewall" of protection between information stored on the AmeriClean network and untrusted users on the Internet.
- This firewall shall control communications between the AmeriClean network and the Internet in both directions.
- The firewall shall utilize an access control list or rule set to allow only users in trusted domains or from trusted Internet hosts or addresses to communicate with the AmeriClean network.
- The firewall shall deny transmission of all communications and protocols not explicitly allowed.

- The firewall shall prohibit source routing on all incoming data packets from the Internet.
- The firewall shall prohibit IP address spoofing on all incoming communications from the Internet.
- The firewall shall hide the details of the AmeriClean network architecture, including ranges of IP addresses, from users on the Internet.
- The firewall shall reject attempts for direct FTP or telnet connections.
- The firewall shall provide the capability to audit and log attempts to communicate with the AmeriClean network from the Internet. This log shall be protected form deletion or modification.
- The firewall shall "fail safe." If any event shall cause the firewall to cease operating, it shall prohibit all incoming communications until fixed.

3.3.6.4 Physical Security:

- All components of the AmeriClean communications network shall be housed within the corporate headquarters.
- Laptop computers used to remotely access the communications network shall not store any sensitive or company proprietary information, and shall be physically protected by the sales employee assigned custody of the device.
- Physical access to components of the network shall be restricted to AmeriClean employees and temporarily provided to trusted contractors, consultants, or guests.
- The system shall provide the ability to scan floppy and hard disks for viruses. Hard disks shall be scanned once a week unless a manual scan is performed more frequently. Floppy disks shall be scanned whenever they are placed in a network workstation.

3.3.6.5 World Wide Web:

- The system shall allow each AmeriClean employee access to a World Wide Web browser which will provide read access to external information stored on the Internet on Web pages.

- The system shall ensure that 100% of the AmeriClean employees are able to browse the Web at the same time.
- The system shall be able to connect to any operational Web server within 30 seconds of connection request.
- The system shall be able to download the requested home page within two minutes of connection to the Web server.
- Web browsing capabilities shall be available during AmeriClean's extended business hours; from 6:30 am to 7:00 pm.
- An information server shall host a World Wide Web home page for the AmeriClean Company.
- All information placed on the home page shall be reviewed by the system administrator or his delegate to ensure that the information should be made publicly available.
- The system shall allow only the system administrator write access to the information server.
- The information server shall impose no access restrictions on who may read the posted information.
- The system shall support up to 25 simultaneous connections by external users to the information server without any loss of performance.
- The Web page on the information server shall be available 24 hours per day.

3.3.6.6 Access Control:

- The system shall store and maintain an access control list of those individuals possessing accounts on the LAN and therefore allowed access to services, data, and resources stored on the AmeriClean network.
- The system shall prohibit all users except for the system administrator from modifying information stored in the access control lists.
- The system shall prohibit remote access to files and applications on the LAN by Internet users (non-AmeriClean employees).

- If a user fails three attempts in a row to login to the network with the correct user ID and password, the system shall prohibit that user from logging onto the system for a period of one hour or until the system administrator resets the account.
- If a user logged on to the network does not create any activity at his workstation for ten minutes, the system will activate a password-protected screen saver which can only be removed by that user or by the system administrator.

3.3.6.7 Identification and Authentication

- The system shall require each user to enter his assigned user ID and password before being granted access to the AmeriClean network.
- Each user ID and password must be unique.
- The system shall not echo entered password information onto the screen as it is typed.
- The system shall require that each user's password be changed at least twice a year.

3.3.6.8 Audit:

- The network domain controller, firewall and information server shall provide the capability to audit significant events which take place on the network.
- The system administrator is responsible for defining which events are to be audited and for configuring the system accordingly.
- The system shall protect the audit log from unauthorized destruction of modification.
- The system shall secure the audit log in case of a breach of security.
- The system shall provide tools which aid in the review of the audit log and in the identification of suspicious activity.
- The audit log shall store the following information regarding auditable events: the user ID of the event originator, the type of event, success or failure of the event, and the date and time of the event.
- The system shall store audit information for one year after the event takes place.
- The system shall make audit information available for review within five minutes of the event taking place.

3.3.6.9 Physical Parameters:

- All central components of the network (not including individual workstations, printers, and cabling) shall be located within the computer room and therefore must fit within a 12' by 16' space.
- The system shall operate correctly between 30°F and 100°F.
- The system shall function in conditions of up to 70% humidity.
- The system shall be able to operate and withstand an applied force of 20 foot pounds.
- The system shall operate on US standard 120V AC circuits.

3.3.6.10 System Effectiveness:

- The system shall sustain no more than four hours of scheduled or unscheduled downtime per month during general business hours (on a weekday).
- The system shall sustain no more than twelve hours of scheduled downtime per month on the weekends.
- Scheduled weekend downtime shall be announced at least one week in advance by group distribution of e-mail.
- The Mean Time Between Failure (MTBF) of the network system as a whole shall be 45 days.
- The Mean Time Between Maintenance (MTBM) of the network system shall be 14 days. This figure includes scheduled maintenance such as software upgrades.
- The Mean Corrective Maintenance time (Mct) shall be two hours.
- The skill level required by personnel performing user level maintenance shall be low.
- The skill level required by personnel performing system administrator level maintenance shall be high.
- The skill level required by personnel performing vendor level maintenance shall be high.

3.4 Feasibility Analysis

The preceding statement of need developed through interviews with members of each of AmeriClean's business departments as well as through written surveys,

demonstrates acute awareness of current technological capabilities. No single employee has until this time been aware of the all of the multitude of ways in which the corporation could benefit from external network connectivity. But many employees have observed the ways in which other corporations are maximizing the impact of technology on even the least technological industries and have felt the urge to do the same. Now that a formal need analysis has been performed, the corporation as a whole is strongly supporting the project.

Since most of the needs have been observed by watching the actions of other companies, it is evident that none of the technologies required to meet their needs are too futuristic or out of reach. However, no one at AmeriClean has the knowledge and computer background required to shepherd the project through design and implementation. The only truly technical employee is the system administrator, but he is much too busy with daily tasks to perform the research necessary to learn new networking skills, and to analyze various products and design alternatives available. Therefore, the assistance of a telecommunications contractor team is required to ensure that design proceeds smoothly and that all of AmeriClean's needs are met with a minimum of disruption to business operations.

The CEO of AmeriClean is a staunch supporter of the project and has pledged a budget of $125,000.00 for the purchase of new equipment to enhance the existing LAN. However, the consultant in charge of the project must inform him early of any additional costs, such as monthly charges for Internet connectivity and use, training in particular products, and the consultant's own time. If sufficient funds are available, the probability of success for the project is significantly increased.

Finally, the fact that 80% of the company use workstations daily to perform their jobs makes it possible to execute a smooth transition to the new system. Employees are used to interacting with computer screens and graphical user interfaces, and have gradually grown to trust the corporate database to store information accurately and provide correct and timely summaries and reports. There is only a slight risk that employees will resist the change and unintentionally undermine its success. If the consultant is careful to maintain as much of the existing system as possible when designing

the enhancements, and uses well-tested technologies which prevent the company from feeling they are being treated as a test bed or experiment, the project has a high probability of successfully meeting all of the documented needs.

3.5 Maintenance Concept

In order to support AmeriClean's network communications system, there are three levels of maintenance that will be required: user / workstation level of maintenance, System Administrator / architecture level of maintenance, and the vendor / product level of maintenance. These levels are described in the following sections, and are summarized in Figure 3-3.

3.5.1 User Level

The users of this system are not highly skilled in technical areas. They excel in the areas of management, marketing and sales, manufacturing, and chemical engineering, but have no need to be conversant in computer or telecommunications technologies. Therefore, the users are expected to perform only minimal maintenance activities on their workstations. If the user has trouble getting the system to operate correctly when first using it, he or she is expected to check that the power to the system is on, (at the power strip, CPU, and monitor if each has a connection) and that all cable connections between components are securely fastened. If the user is having difficulty logging in to the workstation once power is supplied, he must check that his user ID is displayed correctly, that the domain or machine he is attempting to log in to is correct, that he is using the correct password, and that the Caps Lock key is not on. He may attempt to reboot the machine (power it off and then back on) to see if the problem is resolved. Finally, if the user has achieved access to the computer's applications, but is having trouble using them correctly (for example he is unable to determine how to create a table on the word processor, or automatically calculate the sum of twelve numbers on a spreadsheet) he is expected to use the Help option on the software menu to access any supporting documentation which the vendor has included to assist users in such areas. In addition, it is the user's responsibility to keep his workstation clean and free from food and beverage

spills and safe from physical dangers such as being dropped. If these limited maintenance actions do not solve a user's problem, he is then expected to call the system administrator and refer the problem to more expert hands.

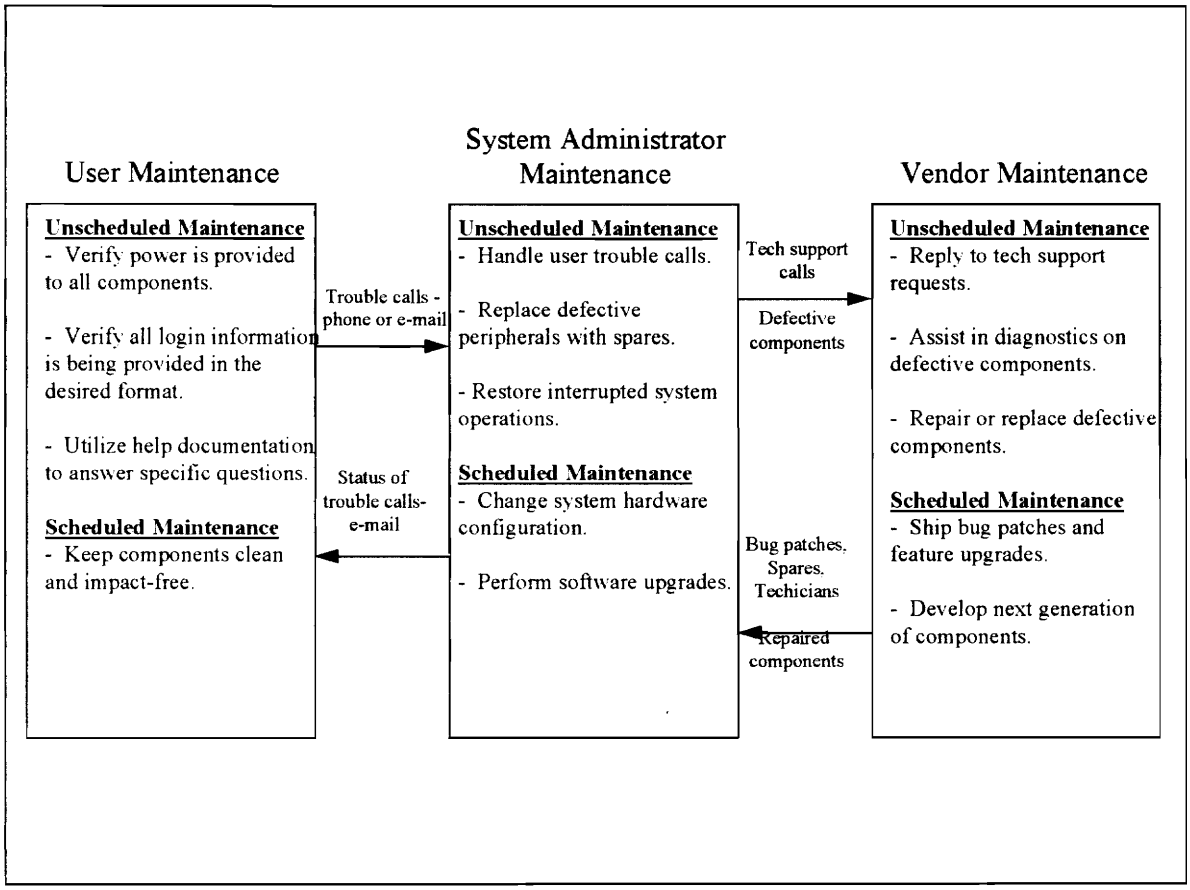


Figure 3-3: Network Maintenance Concept.

3.5.2 System Administrator Level

The system administrator is responsible for how all of the components of the network are integrated and configured at the AmeriClean headquarters. He will assist the consultant throughout design and implementation of the network enhancements to be sure that he knows what is being installed and why. Any portions of the system which he can not observe during installation, he must obtain training from another source. Therefore, when the consultant completes development of the system and declares it to be

operational, the system administrator will be qualified to take over the system maintenance.

The system administrator will provide informal training for new users who are hired by the company. This training will probably consist of a quick demonstration of software capabilities and of showing where both on-line and hard copy documentation are located. The system administrator will handle trouble calls lodged by the users of the system. If they were unable to get the system to perform properly at the user level of maintenance, the problem is referred to the system administrator, either via a telephone call or an e-mail message. The system administrator will troubleshoot the system to attempt to determine the source of the problem. Often, user problems are caused by errors in the system configuration. For example, the server may not be aware of the proper location of a workstation, or a software application may be installed incorrectly. If the system administrator can determine the source of a problem, and it is caused by the way in which the system is configured, then the system administrator will repair the problem if possible, and will notify the user when the problem is resolved. If the problem is beyond the capabilities of the system administrator, he will notify the vendor of the system component demonstrating the problem.

The system administrator is also responsible for performing some elements of scheduled and unscheduled maintenance on the components of the system. Peripheral devices, such as power supplies, disk drives, and monitors, do not have as long of an expected life span as the CPU of a computer, and sometimes fail unexpectedly. These devices are relatively inexpensive to replace in comparison to the rest of the computer workstation, and the tasks involved to replace them are straightforward. Therefore, the system administrator will keep a supply of one spare of each device for every 15 workstations on hand at AmeriClean headquarters, and will perform the replacement when such a device fails. The system administrator will then communicate with the vendor of the component to determine whether the offending unit may be repaired at the vendor facility, or whether it should be disposed of and a new spare ordered. The scheduled maintenance performed by the system administrator consists of system operational tests, cleaning machines, and performing scheduled software upgrades.

3.5.3 Vendor Level

The components of the AmeriClean network architecture will be procured from a variety of different vendors. Most vendors include technical support as a part of their service fee, and therefore the vendors will be able to assist the system administrator with his level of maintenance responsibilities. If the system administrator encounters a problem outside of his area of technical expertise, he is able to call or send an e-mail to the product vendor, often sending along information on the error generated. The vendor will usually be able to determine whether the problem is caused by an error in the way in which the item was configured, in which case the system administrator will be responsible for performing the maintenance required with advice from the vendor. On the other hand, some problems identified will be caused by the system component operating incorrectly. This type of problem must be repaired by the product vendor and can be handled in one of two ways. The vendor may send a technician to visit the AmeriClean headquarters and to perform the repair on site. This scenario is preferred if the vendor has a local division because it eliminates the risk of further damage to the product in shipping and handling, the turnaround time for the repair is quite low, and the technician can gather first hand information about the way in which the product is configured and is being used which may prove invaluable in diagnosing and fixing the problem.

If the problem cannot be fixed on site using portable repair tools, then the product must be shipped back to the vendor for repairs. Electronic and computer components are fragile and must therefore be packaged carefully and handled well during the trip. The customer must allow for a week of transportation time in each direction. This method of maintenance is reserved for the most serious errors in component operation, for example if an unexpected power surge melted some of the electrical circuitry of the hardware. Similar maintenance needs could be caused by a fire or water leak in the building. To ensure that the vendor maintenance actions are handled correctly, technical representatives will communicate in detail with the System Administrator before determining whether vendor repairs are truly necessary, and whether those repairs can be performed on-site. In addition, the vendor may supply the system administrator with diagnostic software programs which, when run, generate information about component

operations. This data can be e-mailed or downloaded by the vendor to aid in deciding the required maintenance levels.

3.6 Conceptual Design Review

Now that the need for the system is well understood, and the operational requirements and maintenance concept have been developed and documented, the consultant and his design team are able to move on to the preliminary design of the system and performance of a functional analysis of its operations and maintenance actions. Before this takes place, it is important to ensure that the data collected in the conceptual design phase is accurate and is accepted by all stakeholders. Therefore, a Conceptual Design Review is held, attended by management and by user representatives of each department and task. When all parties agree that the system requirements are complete and interpreted correctly, the project design may progress to the next phase.

4. Preliminary Design

4.1 Functional Analysis

The following series of diagrams (Figures 4-1 to 4-12) depicts the functions which must be implemented in the AmeriClean network system. The operational flows address how the system will operate from the user's point of view. They address only the functions supporting Internet connectivity; other operations the user will perform on the Local Area Network such as word processing, and use of the corporate database already are in use at the company and are not being modified or enhanced as part of this design effort. They should already be well-documented in existing operating procedures or manuals maintained by AmeriClean.

These flows demonstrate both how a headquarters user will operate the system and how a traveling salesperson will access the network remotely. The only real difference in these scenarios is the manner in which a user would log into the system. A headquarters user would be located at a workstation permanently attached to the network and would simply have to turn the system on and enter a user ID and password when prompted. He would then have access to her own directories and to any additional files or applications to which she has been granted permission. A remote user would have to execute an additional step whereby she utilizes a modem to setup a temporary connection to the network. Because any incoming traffic is suspect, she may have to prove her identity with more than a simple ID and password, by possessing a token or smart card as well. Once the connection has been established and the identity confirmed, the remote user has access to all the same files as if she were physically located at AmeriClean, including access to Internet applications. Therefore the functions and operations required from that point are the same for both categories of users.

There are no flows for functions required to access information on the other side of the Internet firewall. As much as possible, this device should operate without hampering the mission-related operations of the AmeriClean users. They should not

notice a drastic decrease in performance or increase in difficulty in using this safeguard. Therefore, there are no unique operations to depict regarding this system.

To this point, the types of services required by AmeriClean users are known, but no details have been developed of the products which should be procured or the means in which the services shall be implemented. Therefore, the flows are described in terminology that is not product specific. Operations may be implemented through hardware or software, and by a variety of commercially available products.

The second set of functional flows (Figures 4-13 to 4-15) demonstrates the required maintenance actions needed to support the system. These maintenance flows generally branch off from the functional flows at a point where things can potentially go wrong. If all components work perfectly, the path of the functional flow will be followed. On the other hand, if operations do not proceed as expected several situations can occur. These are called the "No Go" states where some action is required to diagnose the source of the problem and either take corrective action, or refer the problem to the next higher level of the Maintenance Concept. The maintenance flows for the user level of maintenance are fully depicted because they are independent of the products selected, and follow an easily captured set of rules. Administrator and vendor maintenance cannot be so easily depicted. These actions will depend on the details of the components selected, and should be captured in the product documentation. The process of determining which maintenance actions are needed is also not a programmed decision. This process consists of trial and error to determine the source of the problem, and will probably be executed in conjunction with the AmeriClean System Administrator and a technical support representative of the component vendor.

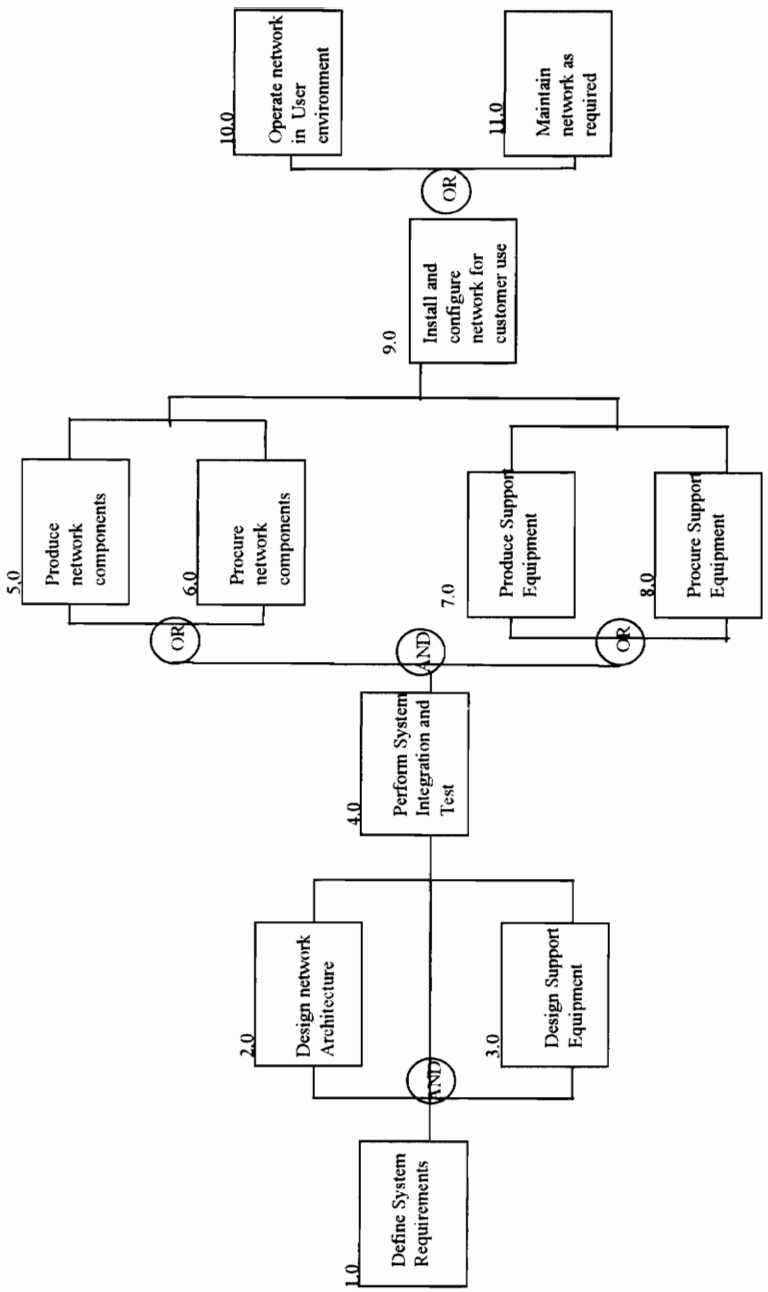


Figure 4-1: Operational Flow First Level.

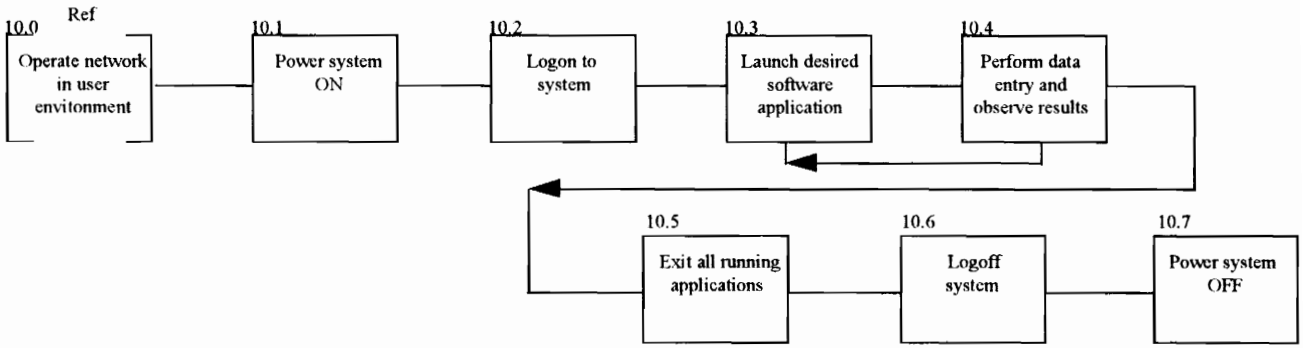


Figure 4-2: Operational Flow - Second Level.

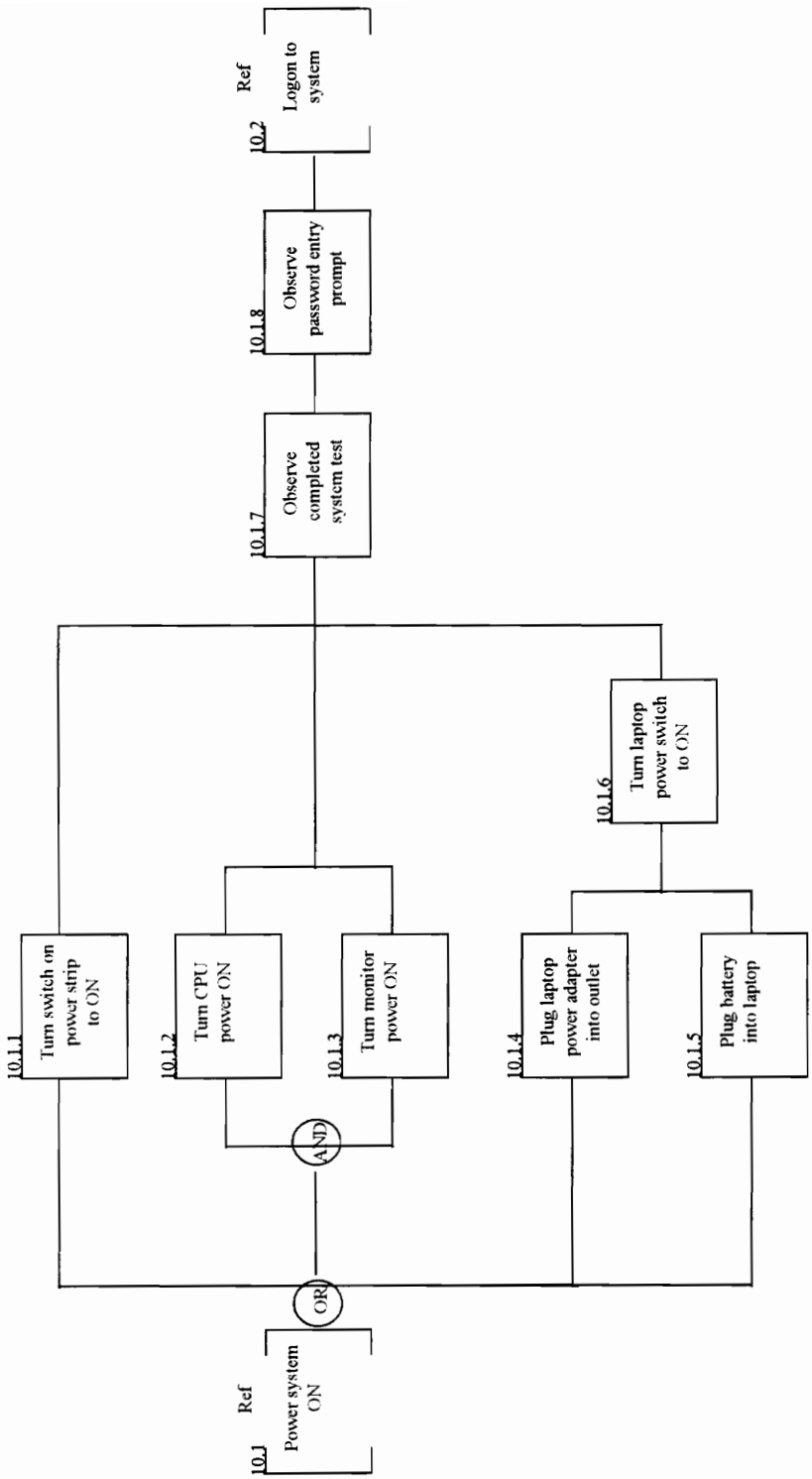


Figure 4-3: Operational Flow - Level 3a.

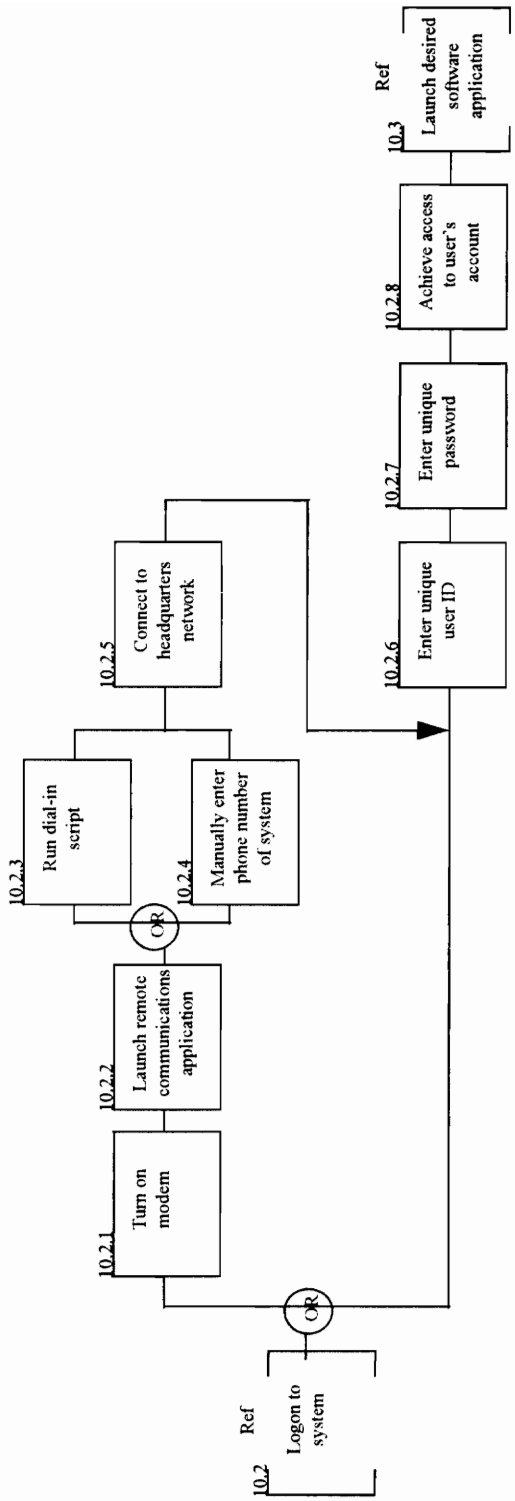


Figure 4-4: Operational Flow - Level 3b.

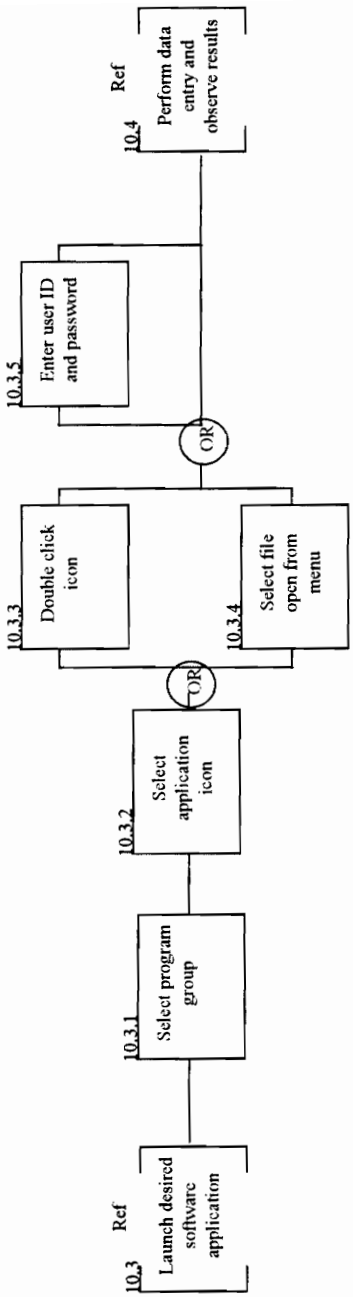


Figure 4-5: Operational Flow - Level 3c.

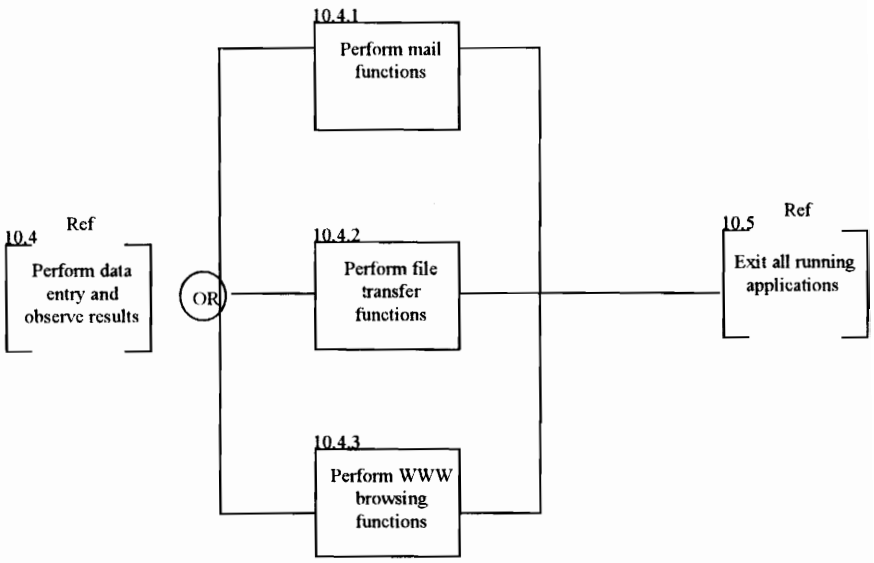


Figure 4-6: Operational Flow - Level 3d.

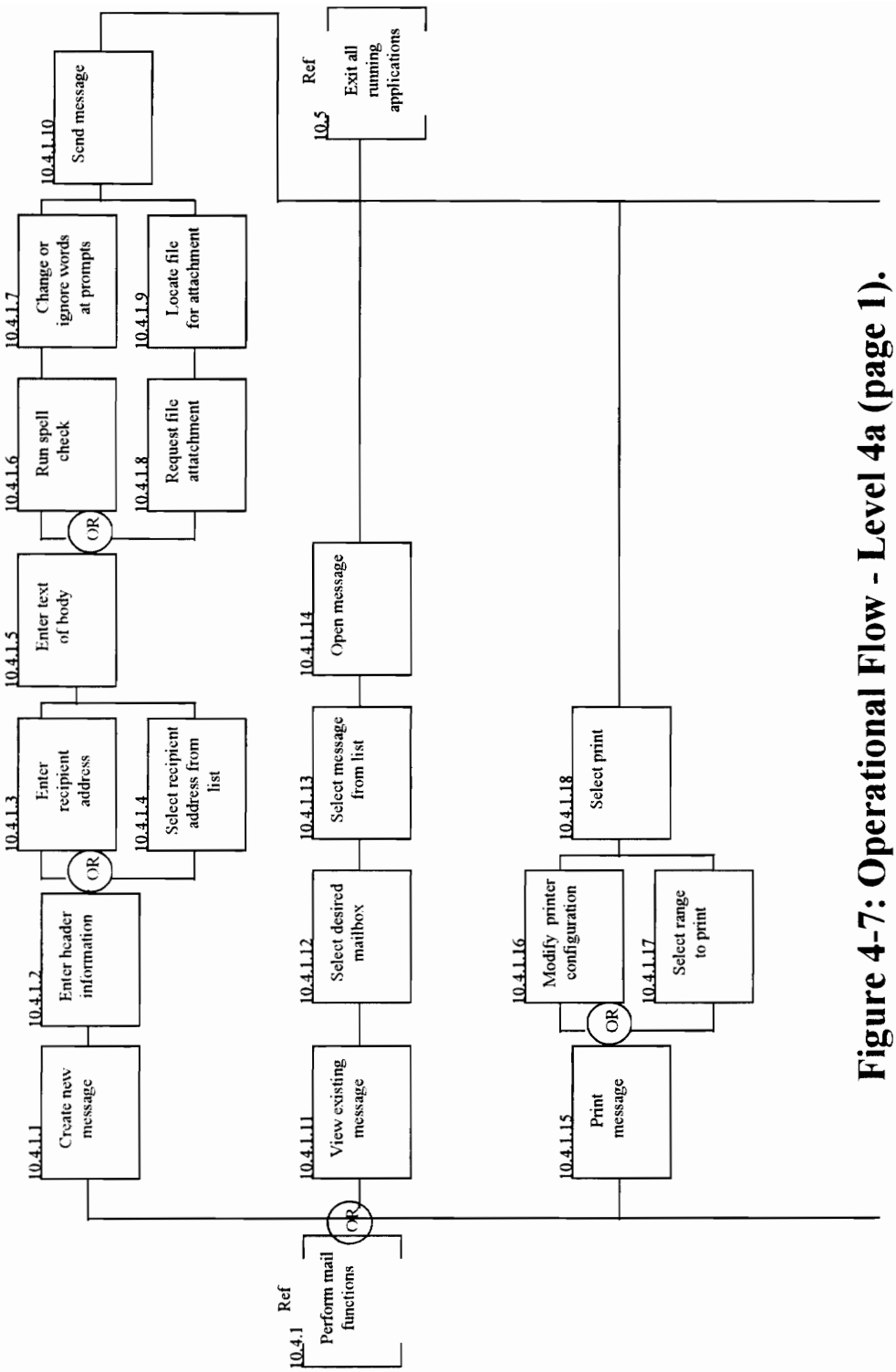


Figure 4-7: Operational Flow - Level 4a (page 1).

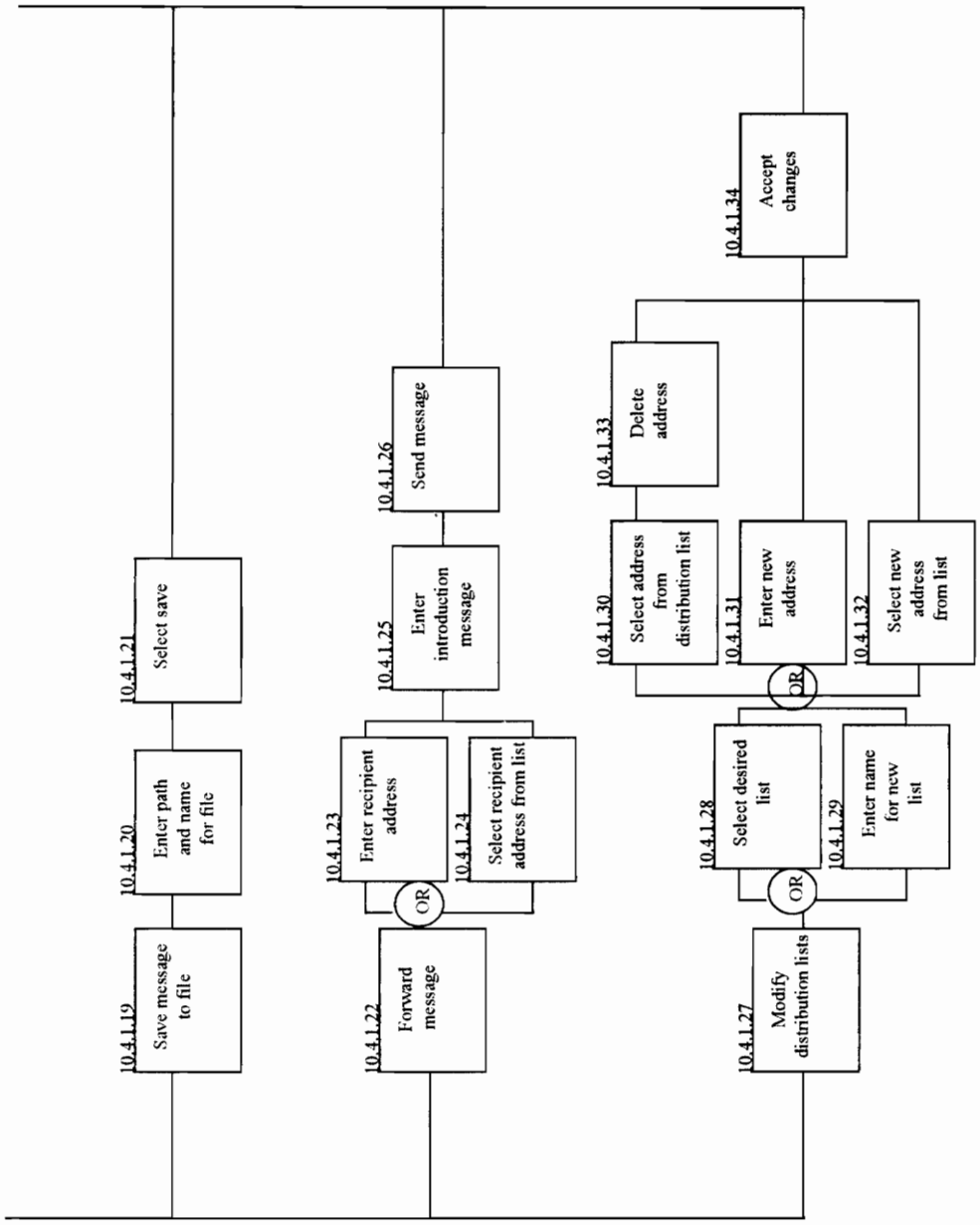


Figure 4-8: Operational Flow - Level 4a (page 2).

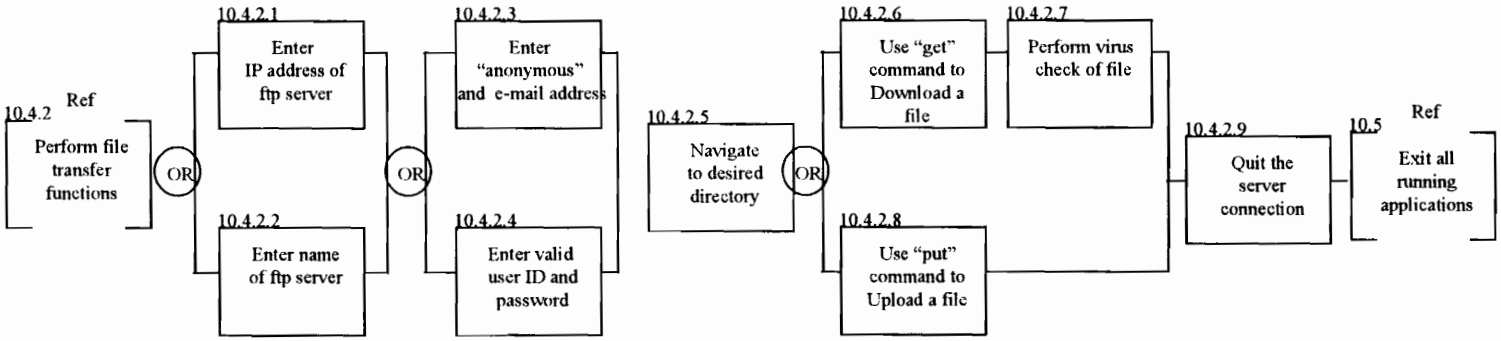


Figure 4-9: Operational Flow - Level 4b.

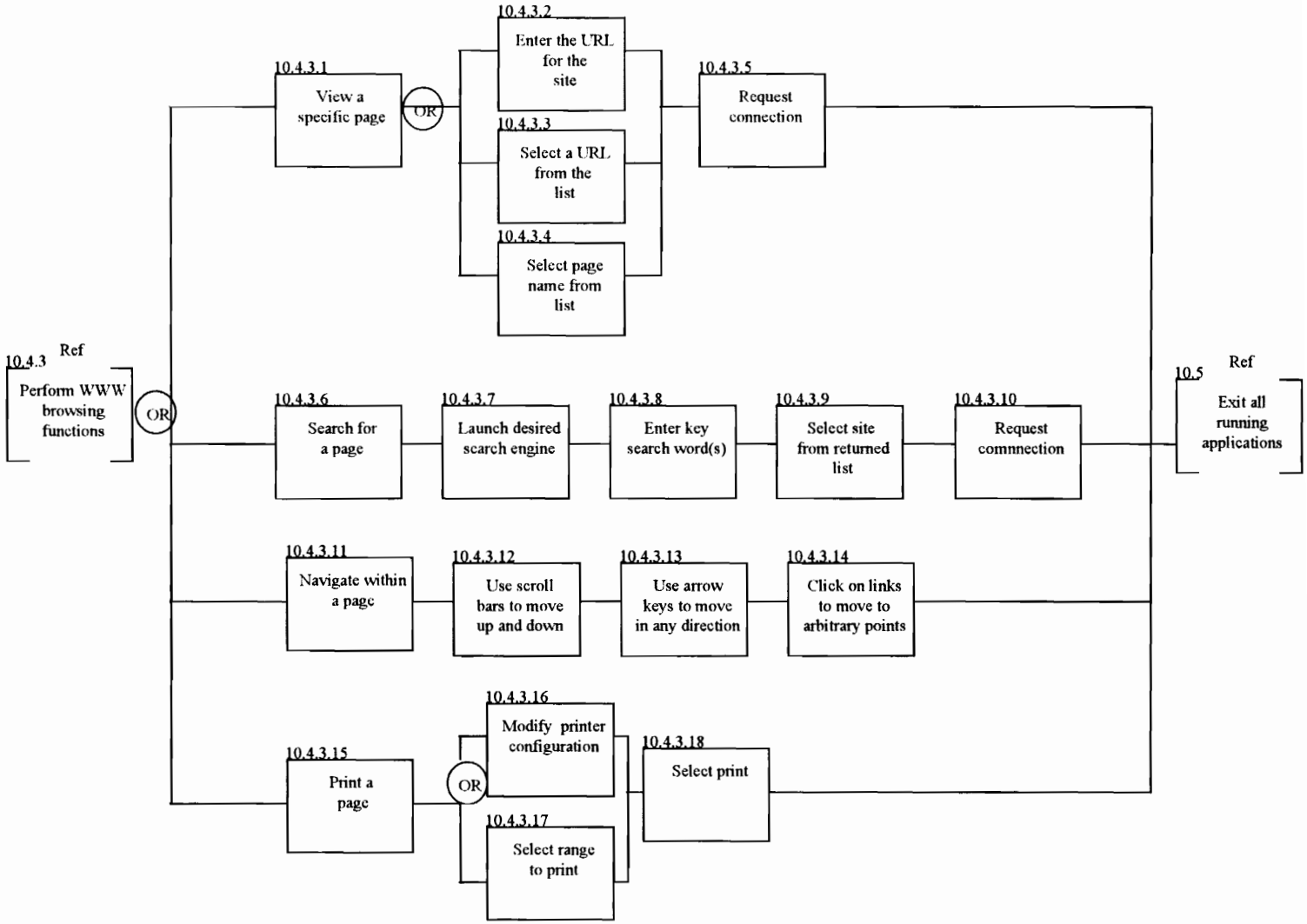


Figure 4-10: Operational Flow - Level 4c.

Figure 4-11: Operational Flow - Level 3e.

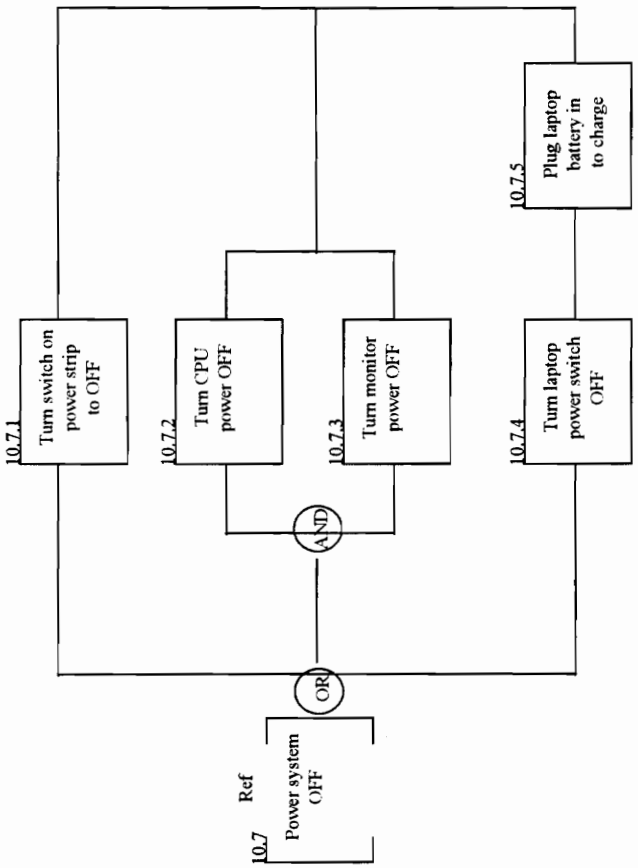


Figure 4-12: Operational Flow - Level 3f.

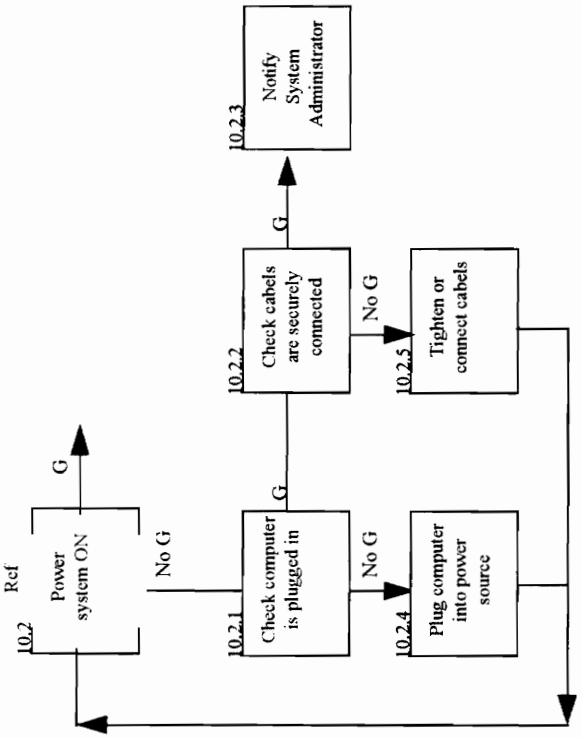


Figure 4-13: Maintenance Flow 1.

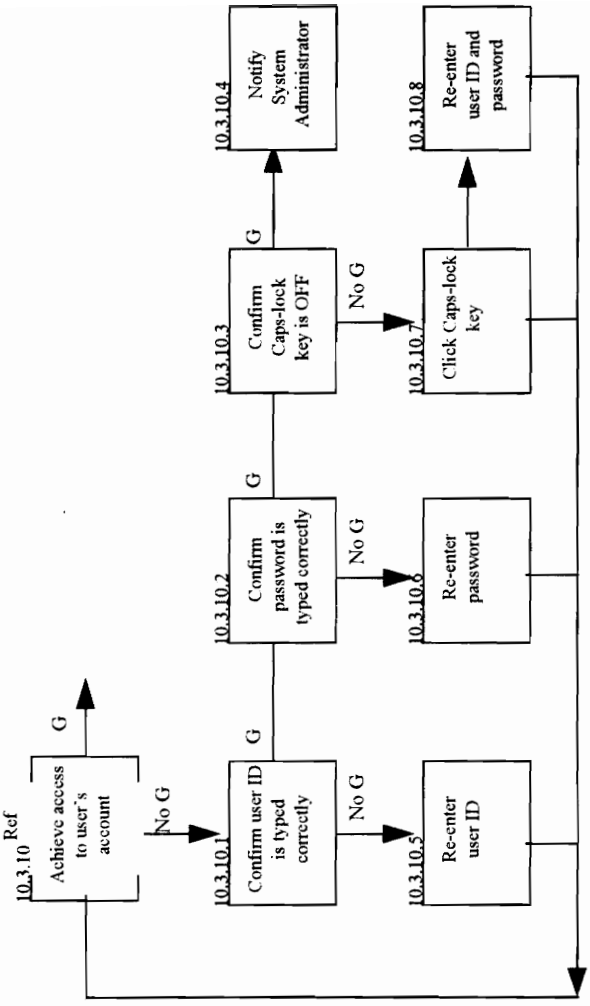


Figure 4-14: Maintenance Flow 2.

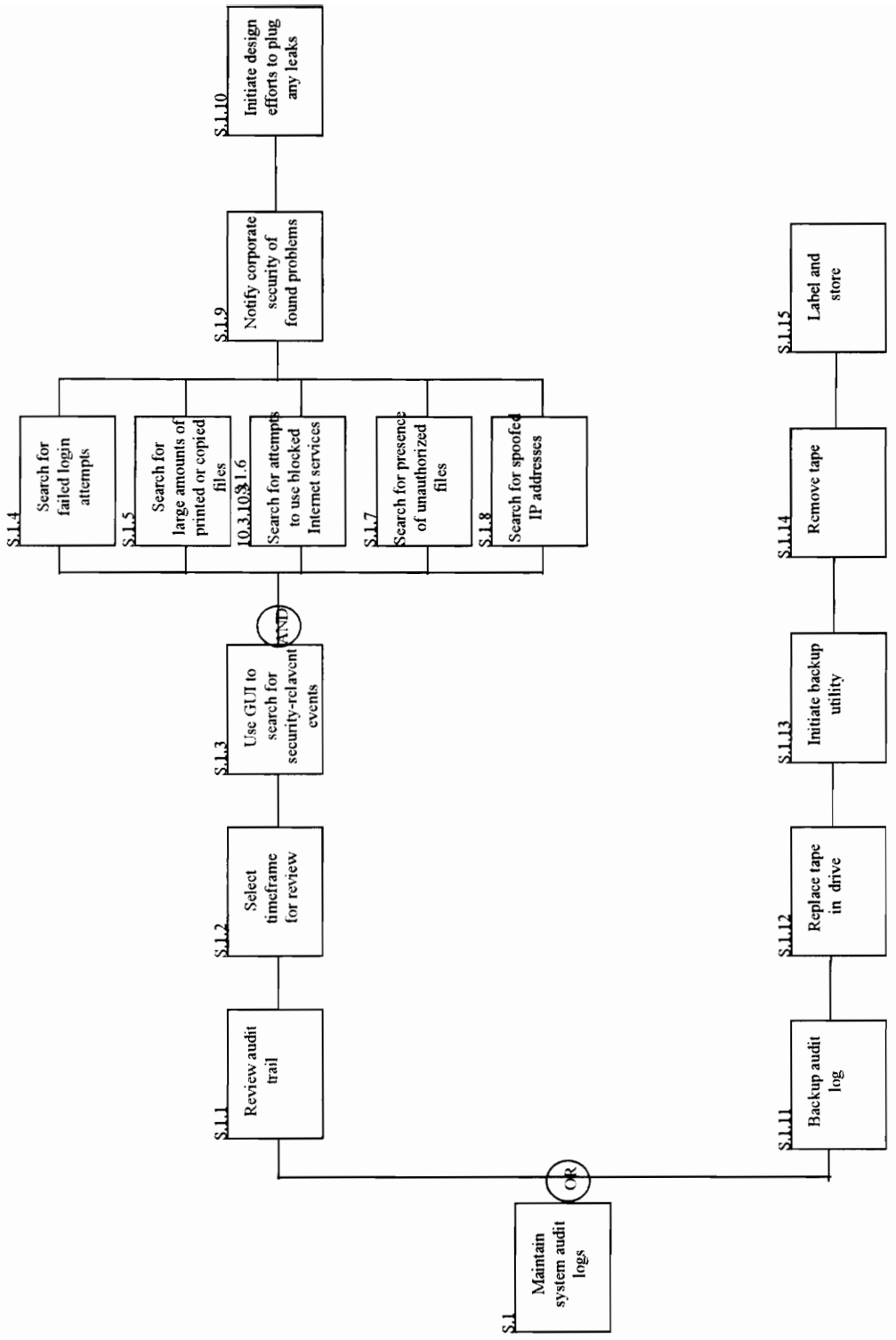


Figure 4-15: Support Function Flow.

4.2 Definition of System Components

Before the operational and functional requirements gathered up to this point can be utilized to formulate a design for the system, it is necessary to determine at a high level what types of subsystems and components are needed to make up the system as a whole. The validated requirements for what the system is intended to accomplish are combined with technical engineering information regarding the workings of communications networks to derive this component list. Then the performance requirements of the system will be allocated to this list of components, to ensure that if each component is designed or selected correctly, the integrated system will operate as expected.

A communications network of the type needed by AmeriClean can be divided into several subsystems. The infrastructure of the network is the set of components that make it possible for information to travel between network users. This infrastructure can be supported by several different technologies, of various levels of maturity, complexity, and expense. Regardless of the particulars of the technology, however, all networks need certain components of their infrastructure to include: a means of linking network nodes together (for example: cabling, fiber optics, radio or satellite links), and a means of directing information along an appropriate path to ensure that it is transferred correctly from the data originator to the data recipient. This function is performed by a network router which stores information about nodes that it is able to communicate with, and utilizes various algorithms to determine which data path is the most efficient at a given point in time.

The second network subsystem consists of communications servers. These components, as indicated by their name, provide a service that the rest of the network can utilize. The benefit of a server architecture is that a single machine needs to know how to carry out an operation or support a particular kind of data. The individual workstations or terminals on the network do not have to store their own copies of data or applications, but can rather access the single source. A good example of this concept is the database server. Fifteen to twenty years ago, individual machines were not frequently networked but operated independently. If employees of a corporation wanted to store data about the

company electronically, they could either contract for the development of a rudimentary data storage application, or create one themselves. If multiple employees utilized similar types of information, they would store copies of it on their individual machines. However, this data was not easy to keep synchronized, and often values would differ from machine to machine and the data entry needs were quite redundant. Keeping such information on a database server today ensures that all information meeting a particular need is stored in one place. It only needs to be entered into the system once, and is ensured to be the most current information available. Anyone in the company who requires the use of this information accesses it across the network from their individual computers. Many employees can read and utilize the information at one time without worrying about discrepancies, because the software takes care of resolving write access conflicts.

The AmeriClean network will require the use of several types of servers. File servers (called domain servers in Windows NT) which store the user's directory structures and data files already exist as part of the Local Area Network. Although they are a critical component of a network, they do not directly effect the enhancement project to provide Internet connectivity and will not be investigated in great depth unless a deficiency in the current architecture can be identified. In the same way, print servers exist to allow multiple users to send hard copy output to shared printer resources, and a mail server stores incoming and outgoing messages and determines how to direct them to their recipients.

Several new servers will need to be added to the system to support the specific needs of external Internet connectivity. Machines which are nodes on the Internet are identified by unique numbers called IP addresses. These numbers are long and difficult for people to remember, so most machines also have a name which people can use to refer to the machine. However, the translation from host name to IP address is not automatic, but is performed by a DNS (Domain Name System) server which knows how to research the address of any machine on the Internet when given its name by communicating with other such servers. The AmeriClean network will need such a DNS server which knows the names and addresses of all machines on the internal network, and can find out the addresses of other machines on the Internet. An information server will also be needed to

host both large files that are to be made available for external users to download, and the AmeriClean WWW home page for all users of the Internet to view. This server will probably require a combination of hardware and software, and should allow both AmeriClean headquarters users and external Internet users to view the presented information. Additional mail server capabilities will be required to allow users to communicate over the Internet rather than just over the local network. Specifically, a mail gateway will be required which can convert between the mail format used on the LAN to the format understood by Internet machines, called SMTP (Simple Mail Transfer Protocol).

An Internet firewall will be treated as a subsystem of its own. This device provides most of the security between the internal network which contains sensitive and company proprietary information and the unprotected external Internet. It is used to prevent those who wish to snoop on the data stored on the network or to erase or otherwise harm the data. Although a firewall serves one particular need of security for the system, it may consist of multiple components including one or more computers, routers, and peripherals. The components needed depend on the detailed design of the firewall, and often on how particular vendors choose to implement the security requirements.

4.3 Requirements Allocation

In order to be sure that the completed network system meets all of the requirements developed in the conceptual design, those requirements should be allocated to the subsystems and components just described. The requirements for each component will then be used to either develop the component to those specifications, or to select a commercially available component which best meets those requirements at the best price. The allocation of the performance requirements derived in the conceptual design to subsystems and components is depicted in Figure 4-16.

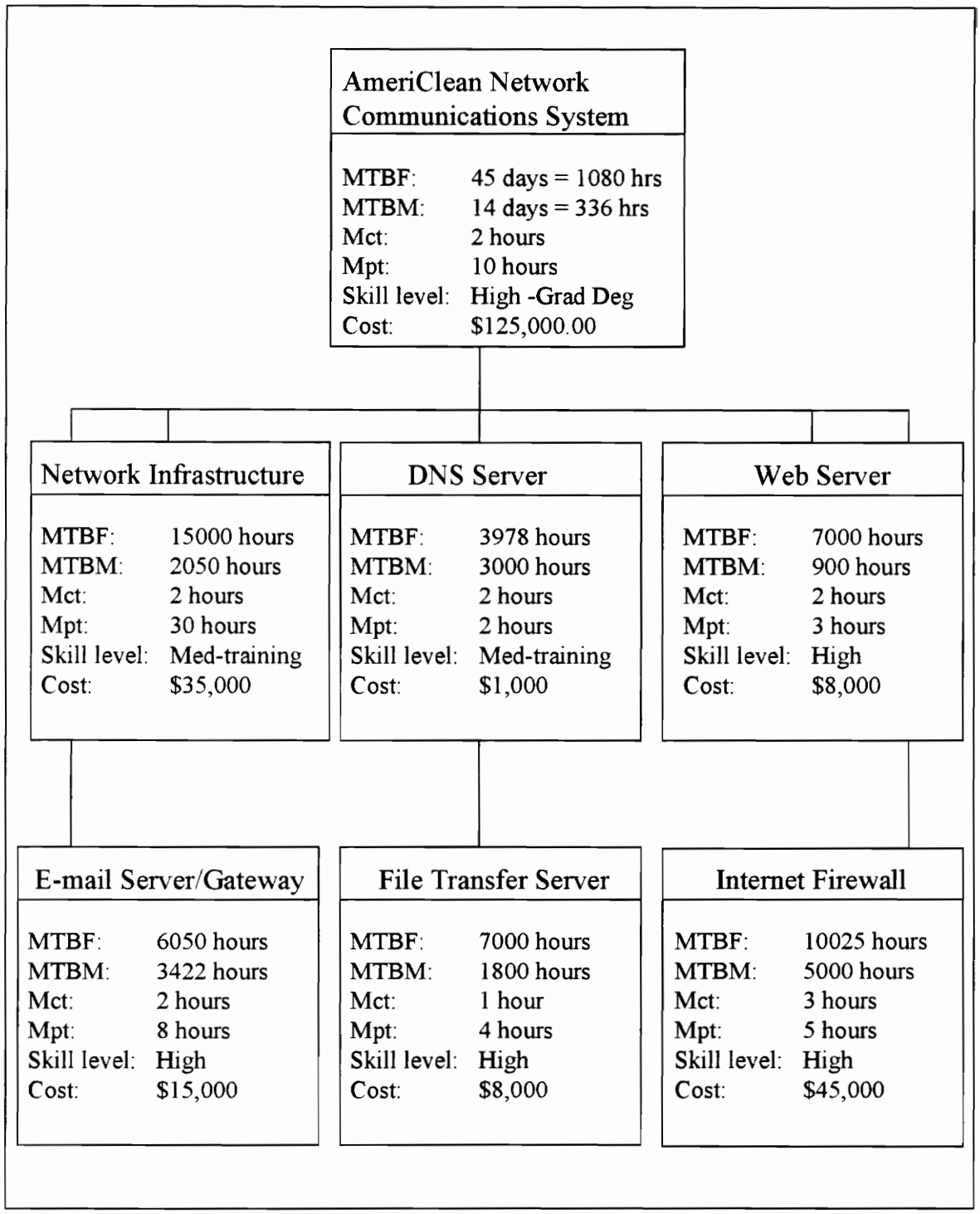


Figure 4-16: Allocation of Requirements.

4.4 Trade-offs

When designing the configuration of components which will implement the network communications system for AmeriClean, two primary design philosophies are utilized. Since this project involves modifying and enhancing an existing system rather than building a completely new one from scratch, the first philosophy is that as much of the existing system as possible will be reused. This is not to allow the consultant and his design team to be lazy in their use of the systems engineering process. Rather, it acknowledges the fact that there is no single best design to solve a given problem, but that there are always several design alternatives for each required decision, and the selection of the best alternative depends on the criteria most important to the end-users of the system. When a system has been in use for as long a period of time as the Local Area Network has at AmeriClean headquarters, the users have had time to become accustomed to the system and the role it plays in their daily tasks. It is difficult to introduce changes to such a pervasive system without creating animosity in the user audience, which may make system modifications unacceptable. It is easiest to keep the portions of a system that the users must interact with consistent unless the current system has real deficiencies or is extremely antiquated. Then additional capabilities and functionalities that have been requested can be added into an accepting environment. In addition, the reuse of existing components will frequently save significant amounts of money toward the overall project cost. For example, utilizing existing 486 computers may not provide the maximum performance possible as opposed to purchasing new Pentiums for each user, but the thousands of dollars saved can be applied to the purchase of high speed and high bandwidth connections to the Internet or extremely robust security devices.

The second design philosophy in place is that anything which can be easily purchased shall not be developed. Each component identified as required by the system poses a fundamental question of the design team; should this component be designed and developed in house as a customized product, or should the most appropriate commercially available component be researched and procured from a vendor? The benefit of designing and implementing a custom solution is that the finished product

should exactly meet the requirements of the particular product, with no extra unneeded capabilities, and also with no shortfalls which must be worked around. In addition, the members of the project team responsible for the design should be completely comfortable with every aspect of the product and how it is designed and operates. They are therefore fully qualified to integrate the product into the system, and to maintain and document its use. There are significant disadvantages to custom development, however. The most critical disadvantages are cost and time. It is extremely expensive and time consuming to build a system from the ground up, requiring research and development time, a staff with extensive expertise and creativity, and probably a great deal of time to test and debug the product. While there are situations in which this time and expense are justified, especially when a new technology is being developed for the first time, it is a waste when similar effort has already been devoted to solving a similar or identical problem. None of the requirements set forth by AmeriClean users and management are exceptionally revolutionary. In fact, many companies have arisen over the past few years to provide just such services and system components for companies who wish to extend their communications connectivity. Using such commercial products in the system should save money because another company has made the initial investment in time and effort to develop a product, and has the capability of selling thousands of products to consumers. Therefore, the cost of development is spread over thousands of products rather than sunk in a single item. Most vendors provide some level of technical support for their products, either included in the purchase price, or at a small additional cost. This service will remove a significant burden of the System Administrator who cannot hope to be an expert in every network component and technology available on the market. In addition, the commercial products have generally been well-tested, usually by the participation of a group of beta users. Results of these tests are generally available and allow the purchasing organization to avoid having to do extensive testing on their own.

Therefore, specific vendors and products will need to be selected for each of the components and subsystems described in the previous sections. The most efficient way of making such a selection and justifying it to the customers and the project management is through the performance of a trade study. Obviously, the selected product must meet the

requirements set forth by the users of the system and captured in the requirements allocation. If any of these requirements cannot be met in the finished system, this must be made clear to the management and the reasons why explained. But other factors besides the minimal requirements come into play when selecting components to purchase. Such factors, or product selection criteria, are weighted based on their importance to the system users, with the higher weight indicating a criterion carries greater importance. Next, three to five of the available products on the market are selected as appearing to best meet the requirements and selection criteria for a given system component. The capabilities and limitations of these products are researched using material produced by the vendor, as well as information provided by independent testers, such as computer and communications periodicals. Each product is measured against how well its capabilities meet the selection criteria, with an additional numeric indicator assigned to each, indicating that the product fully meets, partially meets, or does not meet that particular criterion. Each product will have a numeric total of performance against the selection criteria, and the product with the highest total is generally the best alternative for the system. An example trade study matrix is shown in Table 4-1.

Table 4-1: Example Trade Study Matrix.

Selection Criteria:	Weights:	Product A	Product B	Product C
Criterion 1	10	F	P	F
Criterion 2	7	F	F	
Criterion 3	5	F	P	
Criterion 4	3		P	F
Criterion 5	3	P	P	F
Total:		141	105	96

* - Weights indicate the importance of a particular criteria on a scale of 1 to 10

- Products are ranked as fully meeting criteria (F=6), partially meeting criteria (P=3), or a blank space which indicates it does not meet the criteria is given 0 points.

Some of the selection criteria which should be addressed for the AmeriClean communications network are the following:

- ***Ease of Use*** - The daily users of the system are not highly computer literate. They are considered experts in their respective fields, whether they are sales people, managers, chemists, or administrators, but cannot be relied upon to possess a high degree of computer skills. Therefore, they are more likely to accept a new system and to utilize it frequently and without making mistakes if the system is intuitive, and operates without their intervention whenever possible.
- ***Ease of Administration*** - Currently, AmeriClean hires a single full-time System Administrator. This person is already busy dealing with the problems and the daily maintenance needs of a system of approximately 50 users. Whether or not additional administrative staff is hired, it is a good idea to purchase products designed to be easy to maintain. Some products provide administrative tools in a graphical user interface which allow administrators to monitor component performance and make changes when necessary. Others allow remote administration from other machines on the network.
- ***Cost*** - Since AmeriClean is not a large company, they can not afford to simply invest in any intriguing technology. Rather, they need to be sure that the components purchased provide the most functionality for the lowest price.
- ***Security*** - There have already been numerous references to the need for protection from the external Internet environment. One entire subsystem - the Internet firewall - has been identified as needed to provide this security. However, other components of the network can provide security features such as audit and access control which can complement the capabilities of the selected firewall.
- ***Interoperability*** - Because the components of this system will be procured from a variety of vendors and may integrate several different technologies, it is important to determine that the selected components will integrate well with what already exists. This may be evidenced by the fact that several different operating systems or computer

platforms are supported. Or by the fact that support for system integration is provided by the vendor.

- ***Room for Growth*** - Simply because AmeriClean is still a small company is not reason to believe that it will stay that size for the life time of the communications network. Components should be selected that provide the capability to easily add more users to the system, to increase communication bandwidth, and to add features and functionality.

When all of these factors are taken into account, in parallel with the requirements for the given components, a recommendation can be made for the best product to purchase. In the following detail design section, the plans for implementing each subsystem and component of the AmeriClean system will be addressed, and a trade study will be performed to select the best available product which meets the detailed design criteria and should therefore be procured.

5. Detail Design

There are many decisions which must be made regarding selection of hardware, software, applications, and protocols in order to design a working network architecture which fulfills the external communications requirements of the AmeriClean corporation. In this section, each decision will be analyzed in approximately the order it needs to be addressed in the design effort. The technical alternatives for each decision will be discussed, and the best alternative will be selected and justified. If the selection requires the purchase of hardware or software, a trade study will be performed to select the best vendor based on the criteria discussed earlier in the trade-offs section of the preliminary design. Within this report, a full trade study will be performed as an example only for the selection of an Internet firewall system. For each other component which requires a complex decision, the selection criteria and their relative weights will be presented, and the analysis of alternative products to meet the criteria will be performed by the contractors as part of the completion of the project.

5.1 Selection of an Internet Service Provider

The first step required to establish external communications connectivity is to acquire a connection to an Internet node. This involves the acquisition of an electronic "pipeline" between the internal network and a machine that is directly connected to computers on the Internet. These pipes may come in various sizes or bandwidths based on the amount of electronic packets of information which an organization expects to pass to or from the Internet. It also involves some administrative activities such as registering the name and location of the company's internal network with the Internet Network Information Center (NIC) so that other organizations are aware of the network's existence and are able to communicate with it. Many companies have developed which devote themselves to providing such access to commercial clients. These companies are called Internet Service Providers (ISPs) and they offer a variety of setup configurations, as well as technical support activities based on an organization's price range and communications needs.

AmeriClean requires a fairly robust level of Internet access. A dial-in connection to the ISP via modem will not be sufficient, because any number of the 50 employee may wish to utilize Internet services at the same time, and should not be required to wait for an available connection. In addition the bandwidth, or number of electronic packet which can travel between points per minute, is low for modem connections. The speed and performance requirements for activities such as Web browsing can not be met over a modem connection. Therefore, the company must use an alternative, leasing a dedicated communications line from the local telephone company, in that way having Internet access available at all times. Such a line is termed a T-1 line and supports data communications at speeds of approximately 1.54 Mbps. Multiple users can access services at a single time, because their communications packets are multiplexed onto this line utilizing the higher bandwidth. There is no competition involved in leasing such a line at this time, because the only provider is the local telephone company for a particular region. However, various ISPs may charge different monthly fees for providing the Internet access on this communications line based on the capabilities of their systems.

The first criterion for selecting a company is location; an ISP must have local service to the geographic center of a company's headquarters. There are several ISPs in the Washington DC / Northern Virginia area which make strong candidates for providing services for AmeriClean. The two largest such companies are PSINet and UUNet. They all have the ability to provide similar services, such as service for the rented T-1 line, allocation of an Internet address range, and registration of the connection with the NIC. However, the difference in cost between ISPs can be significant. These companies have to make a large initial capital investment in order to construct a network architecture powerful enough to provide reliable, fast Internet access to multiple customer companies. Depending on the length of time and ISP has been in business, the power and age of their equipment, and the number of customers they have providing profit and fees, the costs of similar services through that company can differ. Therefore, the highest weighted criterion for selecting an ISP is cost. Of course they must be able to provide the minimum connection requirements such as the ability to pass Internet protocols over a T-1 line. This criterion can only be met or failed, and serves as a means of screening out extremely

low-volume providers. The second most important criteria is level of customer service provided by the ISP. AmeriClean's system administrator is not experienced in the issues of Internet access and integration, and therefore the ISP must have knowledgeable staff who can be accessible at all hours to answer questions about network configuration and aid in trouble shooting problems. Finally, the company should provide room for growth and expansion of services if AmeriClean grows or desires to upgrade their Internet capabilities.

Several potential selection criteria do not apply to choosing an ISP. Ease of use is not really a concern, because the fundamental Internet connection will be invisible to the non-technical system users; they will only interface though higher level applications. Security is not the responsible of Internet organizers, but must be provided and ensured by individual companies. And since the communication line is the lowest level of technical communications, it does not pose problems of compatibility with existing machines or software. All applications and systems are built to adhere to the same low level standards of data transmission and will operate with the leased line. The criteria to be used to select AmeriClean's ISP are shown in Table 5-1.

Table 5-1: Criteria for Selecting an ISP.

Selection Criteria	Weight
Meets minimal connection requirements	Y/N
Location of ISP	5
Cost of required services	10
Level of customer service	8

5.2 Network Communications & Protocols

Before an organization can begin to communicate externally, and therefore worry about its communications methodologies being compatible with those recognized by Internet servers, it is first important to address the communications protocols in use on the local network itself and begin to address compatibility issues locally. This brief discussion

of the underlying network technology which is providing the infrastructure on the LAN is included as background information regarding the current architecture, and then will address some alternative communications protocols which are supported by that infrastructure to transmit information packets between users.

5.2.1 Network Infrastructure

The AmeriClean network is currently built on an Ethernet local area network. This is a very common configuration for Local Area Networks (LANs) which generally span an area the size of an office building. The specifications for the Ethernet technology may be found in IEEE standard documentation 802.3 (Stallings). An Ethernet LAN architecture consists of a bus topology of computers directly connected to each other in a chain by coaxial Ethernet cabling about a half inch in diameter, and up to 500 meters in length. A transceiver device connects each individual computer workstation to the cabling, connecting the communications medium to the computer's processor bus. The operating system of the computer treats the transceiver simply as an input/output device, and sends or receives signals, not really needing to know any other information about the size or configuration of the attached network. The original form of Ethernet was a bit difficult to use because the cables were highly shielded from electrical interference and therefore difficult to bend and install. Transceivers were expensive and also difficult to install and maintain because they had to be located with the cabling (usually located in the wall or ceiling) not with the workstation.

AmeriClean uses a modification of the original Ethernet which solves some of these problems. Twisted pair Ethernet, also known as 10 Base T, uses a set of twisted copper wires like those used to transport telephone signals to transfer communications data without the physical layers of shielding required on original Ethernet. Each computer is connected by this wiring to an Ethernet hub or concentrator which can be located up to 100 meters away. This eliminates the need to have a permanent cable connection pulled through a central path in the building, and is much easier to configure and change dynamically, as when new machines are added to the network or moved. Ethernet, as mentioned earlier, is a bus communication topology because all workstations on the

network share a single communications channel. It further utilizes a broadcast methodology because all workstations receive all communications, and then chose to act on the communication or ignore it based on the addressed recipient of the packet. The speed of an Ethernet connection is 10 Mbps, and uses a system called Carrier Sense Multiple Access with Collision Detect (CSMA/CD) to allow multiple machines to access the Ethernet at the same time and to avoid electronic packets colliding with each other and becoming unintelligible. Each computer connected to the Ethernet on a particular network is assigned a unique 48 bit address which is used to identify the intended recipient of a communication packet.

5.2.2 Communications Protocols

Once a physical connection between computers on the network is established and they are aware of how to reach one another to transfer information, a communications protocol must be selected which knows how to break a communications stream into discrete packets, address the packets to the proper recipients, receive packets addressed for the host machine, and reassemble them into the original steam of communications. Various companies and computer manufacturers have developed proprietary protocols for communicating between their machines when networked together. For example, one of the earliest standard network protocols was developed by IBM to provide a consistent interface to build applications to communicate between IBM machines. Called System Network Architecture (SNA) this system was developed in the 1970s and is still utilized by IBM mainframe configurations. Apple computer company has developed a network protocol named AppleTalk especially for LAN communications between its Macintosh computers, and DEC has developed a similar proprietary communications mechanism for its machines called DECnet. However, with the advent of internetworking technologies, required communications between different types of computers caused proprietary solutions to be useless. A standard was needed so that no matter what brand of computing machinery was being utilized internal to a network, any computer which formed an external link to the Internet would speak a standard "language" so that it could be understood by the rest of the internetwork. A suite of protocols called Transmission

Control Protocol / Internet Protocol (TCP/IP) was developed to fulfill this need, and is now the communications standard on the Internet.

TCP/IP is a four layered protocol consisting of the highest and most general Application Level, the Transport Level, the Internet Level, and the Network Interface Level. In this way, it differs from the seven layer ISO model which was developed by an international standards committee, but instead TCP/IP was developed through research and spread through popularity of use. The two Models are depicted in Figure 5-1 (Comer). In each model, dividing communications protocols into layers ensures that each layer is responsible for a unique portion of the communications effort. A message sent from an application on one machine would travel down through each protocol layer on the first machine, with additional information being added to the message at each layer, or with some action being performed on the message. When the message reaches the hardware layer, it can then be transferred across the network to the recipient machine where it travels up though the layers to that machine's application, and has information in the message read and acted upon by each layer on the way.

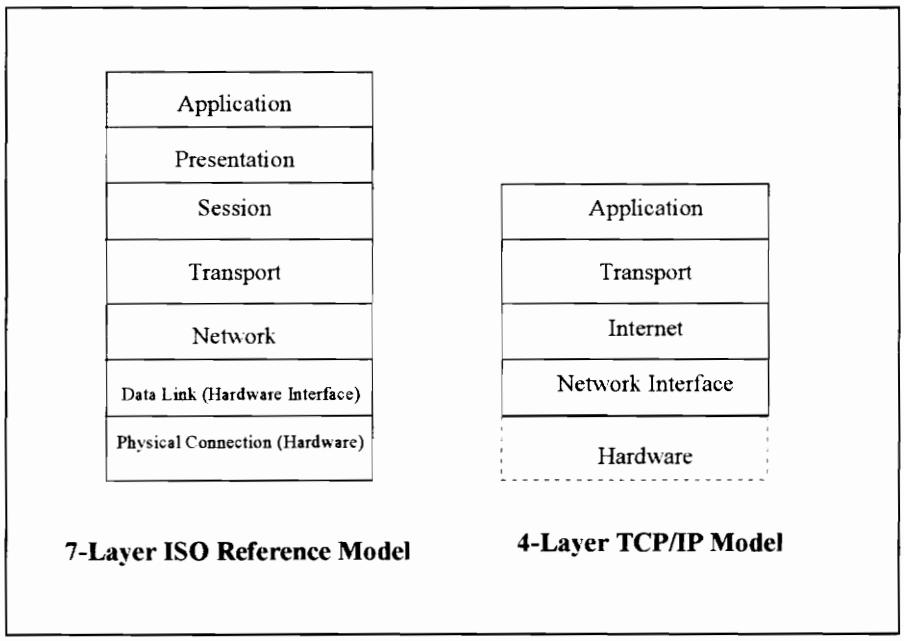


Figure 5-1: Comparison of ISO and TCP/IP Protocol Layers.

The TCP/IP suite contains two transport layer protocols which are responsible for providing a communication path from one application to the other. The first, TCP, is a connection-oriented protocol which establishes a virtual circuit connection between two machines before a stream of data is allowed to begin passing between the two. It is an extremely reliable protocol because by establishing a connection, and requiring the recipient machine to acknowledge successful receipt of each packet, TCP ensures that data will arrive successfully at its destination. The protocol will continue to send packets until this occurs. The second protocol called User Datagram Protocol (UDP) is connectionless. This is considered an unreliable device because delivery of all packets in a communication is not assured. A UPD data packet specifies the source and destination addresses, and then allows the network itself to determine the path for transferring each packet to its destination. No two packets in a stream have to take exactly the same path to the destination, and it is possible that some will be lost along the way. To prevent this from happening, the application which is designed to utilize UDP must perform some of the reliability functions instead of the protocol itself to ensure that the entire message gets through on some attempt. The IP protocol is used to route a packet through the network to its correct destination. IP algorithms are used to determine the most efficient path to send the packet on in order to get it to its destination. If the packet is destined for a machine on the same network as the source, IP can directly route it to that machine. If the packet is destined for another portion of the internetwork, IP must send the packet to a machine called a router which then determines a router on another network which would bring the packet closer to the destination machine. More about routing will be discussed in the next section.

The Windows NT operating system comes ready for internetworking connectivity with a TCP/IP stack included (Microsoft). It also has the capability to support other proprietary protocols discussed earlier, in case a particular LAN consists of machines other than PCs (such as Apple Macintoshes or IBM mainframes) and must support the communications protocol of that vendor. However, even if such a proprietary protocol is used, at some point before the communication packets leave the internal network and are transferred on the Internet, they must be translated into the TCP/IP protocol that the

Internet understands. This may require additional hardware and software called an Internet gateway which must also be purchased and maintained. Since the AmeriClean LAN consists entirely of PCs running Windows NT, there is no need to perform this additional step of translation. Rather, the network should run the TCP/IP protocol internally, as well as for communications with the Internet so that the system administrator must only be familiar with a single suite of protocols, and no performance or delay degradation should be caused by undergoing a translation process.

5.3 Router and Routing Protocols

Once packets of electronic data information can be transferred from one machine to another, both physically and logically, a means must be provided to allow the individual networks and machines to know the whereabouts of all other machines on the internetwork. As mentioned briefly in the previous section, this function is provided by routing. The Internet has quickly grown to a size where it is not possible for a single machine or central site to keep track of all machines on the Internet, allowing all other machines to query it for this information. This would cause an incredible bottleneck of information where no deliveries would ever be able to be completed. Rather, a set of machines called routers communicate amongst themselves to determine the identities and locations of other networks and machines. A router is a computer which is able to chose a path over which to send packets of information.

Each network must have at least one router which connects that network to at least one external network. Companies which have Internet connectivity usually have a router which is connected to a router at the ISP which in turn provides connections to all of the other machines on the vast Internet. The workstations themselves perform routing decisions using the IP protocol, and if the destination machine is on the same network as the sending machine, the sender can route it to its destination directly. However, if the intended recipient is not on the local network, the workstation does not have any information about its location, and must therefore route the packet in directly to the network router which makes all necessary decisions on where to send it external to the

LAN. The AmeriClean network will require one router computer which will provide the interface between the AmeriClean LAN and the service provider's gateway to the Internet.

5.3.1 IP Addressing Scheme

Once it has been determined that a router is required for internetwork connectivity, two additional decisions must be made; what protocols will be used to communicate between routers and the other computers on the network, and what address space will be used to differentiate the AmeriClean network from other networks on the Internet. Every machine which is connected to the Internet must have a unique identifier which distinguishes it from all other machines. A standard method has been developed of assigning these IP addresses so that the assignment is meaningful, and groups all machines on the same local network within the same address range (Stallings). An IP address is an integer 32 bits long, with all hosts on a particular local network sharing a common address prefix. Each address can be thought of as a pair of numbers where the first number signifies the network of the machine, and the second number represents a particular host machine on that network. The number of bits used in each part of the address depends on the class of the address. There are five classes of IP addresses, three of which are widely used today as shown in Figure 5-2.

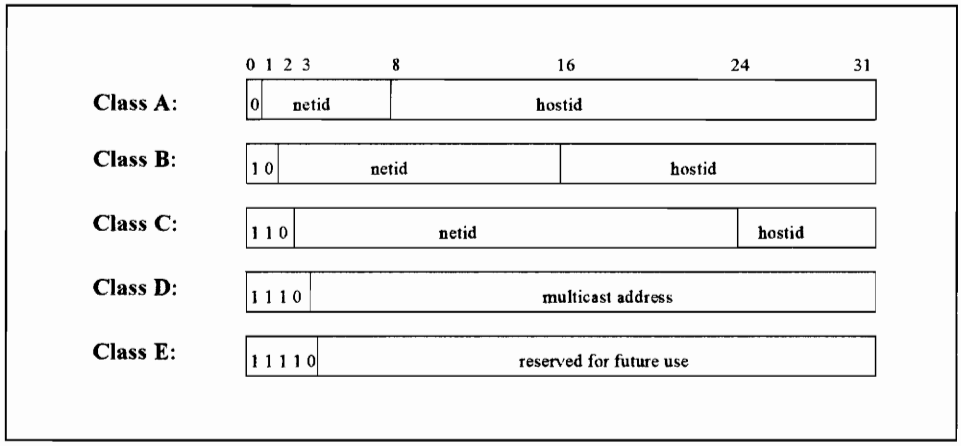


Figure 5-2: Classes of IP Addresses.

Class A, B, and C addresses are assigned to machines on the Internet today, and can be differentiated by the first three bits of the address. Class A addresses are used for the networks which have more than 65,536 (or 2^{16}) hosts; Class B addresses are used for between 256 and 2^{16} hosts; and Class C addresses which are most commonly assigned to a new organization joining the Internet today support up to 2^8 (or 255) host machines. To make the addresses easier to read, they are often written in dotted decimal notation, where each octet of the 32 bit number is written in decimal notation, separated by a period as shown in this example Class B address:

128.10.2.30

which is the same as the binary number

10000000 00001010 00000010 00011110.

Because of the size of the AmeriClean corporation and network, a Class C IP address will be perfectly adequate for its needs. It will also provide plenty of room for the organization of approximately 50 employees to grow over the next three to five years. A particular address cannot be selected but is assigned by the Internet Service Provider and registered with the NIC when an Internet connection is procured.

5.3.2 Routing Protocols

As mentioned in the previous section, routing computers are a necessary component of a network which plans to connect to the Internet. These machines connect two or more networks together and accept packets of information from one network and decide which connected network to route them to in order to send them on to the destination machine. Routers store tables of information regarding the networks directly attached to their interfaces, as well as other networks that have been identified through those interfaces. There are several different protocols that can be utilized to collect the information in these routing tables and to update that information when changes take place (such as a new network is added or an existing server fails). To some extent, the protocols may be selected by the network design engineer (Comer).

The original routers on the Internet used a protocol called Gateway-to-Gateway Protocol (GGP) to exchange information about connected networks and hosts. Each new

router added to the internetwork was assigned a neighbor with which it communicated. Routing information was passed from neighbor to neighbor in order to propagate across networks. Routers using GGP passed connection information in pairs consisting of the IP address of a host connected to the Internet and the distance in hops to that host. This hop count represented the cost of sending a packet on a path to that machine, assuming that a path of fewer hops is more efficient. This is not always the case, because GGP did not differentiate between hops on a LAN and hops requiring slower communications methods such as slow serial lines. This protocol is really not used today, because it took much too long for changes in the network to propagate between neighbors to the entire Internet, and because the required size of routing update messages grew in proportion to the size of the Internet. Several more scaleable options were developed to take its place.

The Exterior Gateway Protocol (EGP) was developed to communicate routing information between a group of networks controlled by the same administrator and the Internet backbone. The centrally controlled system is called and Autonomous System, and the router which connects that system to the Internet is called the exterior router. The EGP protocol which allows exterior routers to communicate has a feature which allows neighbor relationships to be set up dynamically, and lets the router periodically test that connection to its neighbors is still established. The routers periodically exchange updates on the networks and systems which are connected and responding. Essentially, the exterior router acts as an authority for its autonomous system, collecting all host machine information about all networks within that system and handling the maintenance of routing information for the rest of the world. It does so by receiving routing information from other routers regarding their autonomous systems, and by periodically polling the machines it learns about in this manner to ensure that connectivity still exists. There are some restrictions to this protocol, mainly the fact that EGP routers do not interpret distance to a specific host machine. Rather, they simply know whether a path to that machine is available, not how that path compares in relation to the speed and efficiency of any alternatives. Therefore, although it does provide useful information on existing network connectivity, it cannot be used by IP to determine the best path for routing data packets.

Interior Gateway Protocols (IGPs) are used to communicate within autonomous systems and pass the connectivity information learned from the exterior routers to all internal machines. These protocols also allow for decisions regarding preferred data path. One of the earliest IGPs was the HELLO protocol. It operates by synchronizing clocks on a set of machines, and measuring the delay that takes place when a packet is sent to each machine. This delay is used to compute the shortest path between networks, and therefore the preferred path for a communications session. Each router sends a list of routes and estimated delays to all of its neighbors to propagate routing information across the network. The HELLO protocol is not very stable if network information changes rapidly. Traffic tends to oscillate between two paths, as one path is advertised as shortest and many machines attempt to utilize it for their communications. That path quickly becomes overloaded making an alternate path more attractive and advertised as such. Routers begin to use one path and then the other, never resolving the over-utilization problem.

One of the most popular IGPs is Routing Information Protocol (RIP). Both routers and host computers can run RIP; routers in active mode broadcasting routing messages every 30 seconds, and hosts listening to update their information tables but without the authority to advertise themselves. Part of the RIP messages passed includes a hop count distance to the advertised machine, with the capability to set these counts higher or lower to compensate for differences in technologies and speeds over various lines. RIP includes some features that improve the time required for routing information to propagate across the networks. The protocol uses a low maximum hop count (16 hops) to ensure than incorrect routes or inactive ones are recognized within a relatively short period of time, and not assumed to be simply operating slowly. In addition, there is a variable called hold down which allows a router to ignore information it receives about a network being inaccessible for a specified period of time. Therefore, if that message is incorrect, or if the server is quickly restored, information about that connection has not yet been removed from the routing tables, and does not need to be transferred throughout the Internet to all interested routers from scratch.

One of the newest and most ambitious interior routing protocols is called Open Shortest Path First (OSPF) protocol. This protocol provides several advanced features

including the capability for system administrators to advertise different preferred routes based on the type of service (whether is requires high speed, high bandwidth, etc.). OSPF routers perform load balancing to keep traffic on several comparable routes at equal levels. It allows sites to be divided into areas so that routing information can spread more quickly through a site, and provides flexibility by letting administrators define virtual networks which may not physically be directly connected. While providing many such features may be a necessity for large networks, OSPF requires a great deal more effort to administer as much of the route selection information must be assigned by a system administrator rather than determined automatically by the router machines.

The routing problem is a rather simple one at an organization the size of AmeriClean. With only 50 users and host machines, the autonomous system of the organization can include a single Local Area Network as exists today. Within the network, such complex features as virtual networks and definition of different paths for different media and technology are not needed. Therefore, the routing information can be distributed among internal machines using the simpler RIP protocol. This will put little burden on the system administrator because all of the accumulation and update of routing information is performed automatically by the computers. The router which connects the AmeriClean network to that of the Internet Service Provider should communicate with its external neighbors via EGP. In this way, it serves as the authoritative source for all computers on the internal network, collects current information about existing paths on the external network, and can redistribute that information when acquired to the internal machines using the RIP protocol that they are configured to understand. Only that single router is required to interact with the outside world.

Only a few companies produce routers today, and these routers have roughly the same capabilities as far as supported protocols and the ability to integrate with a wide variety of host computers and network protocols. Cisco has become a veritable industry standard, offering routers in all sizes and price ranges to support small organizations such as AmeriClean up to large organizations hosting multiple interconnected networks of thousands of computers covering a range of platforms. For an organization with a single network of approximately 50 users, a router from the Cisco 2500 series will support the

routing protocols selected above with only minimal administration requirements, and will allow plenty of room for growth within the lifetime of the network. It also provides several tools to make router configuration and maintenance more simple, including the ability to configure the router remotely or from a laptop, and a scripting language for setting up network parameters and optimizing the routing paths. Such a simple routing machine costs approximately $2,000.

5.4 Domain Name System

When the previous components, Internet access and a means of communicating and routing data on the local network have been configured properly, the system possesses all of the basic components required to communicate across the Internet. However, such a level of capability would be very inconvenient for the ordinary user to cope with. The result would be a system which could only communicate with other data sources by knowledge of their IP addresses, and could only perform a limited set of functions which would require knowledge of many cryptic commands and codes. The next system components addressed will be utilized to bring a technically complete communication solution to a state where it can be utilized by the largest possible set of users with little or no specialized training.

The first and most indispensable tool for ease of network use is the Domain Name System, or DNS. Although each host machine which is part of the Internet must be assigned a unique 32-bit integer IP address, these addresses are almost impossible to remember and differentiate by human users. Therefore, a system has been developed which allows system administrators to assign meaningful names to the machines on their networks, and then relate these names to the IP addresses that the machines require to communicate between themselves. The assignment of such names is not arbitrary. As the original Internet grew to a size that could not be administered by a central site, machine naming conventions were created to structure all member machines into various hierarchies. The domains shown in Table 5-2 were created with the plan that each organization and its Internet accessible machines would fall into a single domain (Comer).

Table 5-2: The Set of Internet Domains.

Domain Name	Meaning
COM	Commercial organizations
EDU	Educational institutions
GOV	Government institutions
MIL	Military groups
NET	Major network support centers
ORG	Other organizations
ARPA	Temporary ARPANET domain (obsolete)
INT	International organizations

In addition, there exists a parallel geographic domain scheme in which each country has a country code domain. This means of representing organizations by their geographic location has not been very popular in the United States because the names are more difficult to remember and to decipher. The domain name is the most general portion of a host machine name. Any number of other identifiers, becoming more and more detailed, can be concatenated together to form the name, terminating in the most specific identifier or the name of the individual machine. Each identifier is separated by a period, with the most specific portion of the name on the left and the most general on the right. Computer names can be as long or short as the administrator chooses. The following is an example of a computer named "popeye" which is located in the sales department of the New York branch of a clothing company:

popeye.sales.newyork.express.com

The purpose of Domain Name System servers is to keep track of all of the names of computers located on the Internet so that users do not have to. No single machine or database can serve this function because the number of computers and their names are constantly changing. Forcing a single source to track all of these changes would take

considerable computing power and would cause an immense backup as every other machine would be forced to query it for name resolution. So instead, the DNS system consists of a network of machines which know all or part of the total machine names for one of the high-level domains. These servers provide redundancy so that if one or more fail to operate, the entire Internet does not grind to a halt. They also make name queries efficient because they are distributed over several different systems and generally only require name requests to be made of one or two machines before a server which knows the mapping is found.

To implement DNS in a network connected to the Internet, a machine on the network must operate as the name server for that network. This machine knows all of the name and IP address pairs for each host machine that makes up the network. In addition, it knows of at least one other DNS server in another domain. Any machine on the network forms a DNS query asking for the IP address which corresponds to the name of the machine it wishes to communicate with. If that machine lies on the same network, the local DNS server will know how to resolve the name to an address, and will return that address to the requester. If the name is not on the local network, the DNS server forwards the request to the higher level name server. This server repeats the action of returning the address if it is known, and forwarding the request to a higher level machine if it is not. To increase the efficiency of this process, DNS servers cache name and address pairs as they learn about them. In this way, they do not have to constantly query machines located in other parts of the Internet for sites that they access frequently. In addition, the core, or highest level, DNS servers share name information back and forth in a network of name servers. Therefore, there is never a single highest level server that is the only source of information about a particular machine.

AmeriClean requires its own DNS server. This will be the authority for all machines in the AmeriClean domain, and will refer all unresolvable queries to the DNS server of the Internet Service Provider. The ISP should also be registered with the NIC as AmeriClean's secondary DNS server in case the local machine were to fail, so that communications with sites on the Internet will not be interrupted. Unfortunately, Windows NT does not directly support the DNS system at this time (although that fact is

not clearly stated in the product documentation). Instead, the operating system supports a name resolution system called WINS (Windows Internet Name Service). As the name implies, this system can be used to resolve machine names to addresses over the Internet, but only when communicating with other machines which are running Windows. Although WINS does provide some useful capabilities, such as the ability to easily change name and address mappings dynamically, it is not a practical choice for Internet connections at this time, because many Internet servers are UNIX machines or even mainframes that will not understand the protocol. Therefore, in order to be compatible with the rest of the hosts on the Internet and to allow external machines to communicate with AmeriClean machines by name, AmeriClean must purchase a third-party software package that utilizes the networking configuration of the Windows NT server and enables it to function as a DNS server as well.

There are two main options at this time for supporting DNS on a Windows NT machine; portings of DNS to the NT platform offered for sale by the commercial companies FBLI and MetaInfo. The most important criteria to be used in selecting a DNS server application is ease of administration. Since AmeriClean currently employs only a single system administrator, it is critical that changes to the network architecture such as the addition and deletion of new machines be a simple matter to configure. Such changes take place frequently within a growing organization, and if name and address table had to be completely rebuilt each time, the effort would quickly overburden the staff. Also, since Windows NT is designed to network PCs right out of the box, some information regarding machine addressing is entered when the computer is first installed as part of the network. The DNS package should integrate with NT to read this stored data and should not require duplicate entry by the administrator. A second critical issue is system reliability. If a network's name service fails to operate at a given time, then that network is essentially cut off from the outside world. Even listing the ISP as secondary DNS server is not an infallible backup, because that service is beyond the control of the network's administrator and can not be easily ensured. Therefore, the selected software must have been well tested by the vendor under a variety of stress conditions to ensure that no bugs cause the system to fail unexpectedly.

Security of the application is also important. Information about the names and addresses of machines on a network could prove useful to an attacker trying to hide his identity by impersonating a trusted computer on the network. Or if an attacker is able to change the DNS tables, it is possible to make the network inaccessible. Therefore, the software should protect the stored data, and ensure that only a privileged user (administrator or root) can modify the tables. Finally, cost is an issue. Since the AmeriClean network configuration is a simple one, it may not be necessary to purchase the most expensive software capable of tracking multiple subnets and networks of thousands of machines of different models. However, since the server is software, the total cost will be relatively low compared to other network components. The criteria for selecting a DNS product are shown in Table 5-3.

Table 5-3: Criteria for Selecting a DNS Server.

Selection Criteria	Weight
Meets minimal connection requirements	Y/N
Ease of Administration	7
Application Reliability	9
System Security	6
Cost	5

5.5 Electronic Mail

One of the most frequently voiced user requirements for Internet connectivity at AmeriClean involved a need for external electronic mail (or e-mail) capability. Even those users who possessed only the vaguest of ideas about what the Internet means had received countless instructions from customers and suppliers to communicate questions, comments, and other forms of business via a message to an e-mail address. E-mail is popular because it provides a simple method for allowing users anywhere is the world to communicate text messages and even file attachments back and forth at no additional cost or effort than

simply knowing the recipient's e-mail address. E-mail differs from other forms of network communications, because the connection does not need to take place in real time; in fact, the recipient may be away from his or her computer for weeks at a time, and the application must be able to store message information at another point (a spool or queue) so that nothing is lost until the next time they login. Some mail systems use TCP/IP to form an end-to-end connection between the sending machine and the receiving machine, and can therefore track the status of a message at any point in the cycle. Others require the use of mail gateways as intermediate machines which receive e-mail messages and then determine how best to forward them on toward the appropriate destination. Such intermediate machines are required to integrate systems which use TCP/IP mail protocols recognized by Internet machines with other systems which run specialized or proprietary mail applications.

The mail protocol which is most widely used because it is understood by all UNIX machines and is included in the TCP/IP suite of protocols is called Simple Mail Transfer Protocol (SMTP). This protocol is responsible for passing message across a link from one machine to another. It is left up to the particular e-mail application to determine how mail is passed to and from the end user, and how the mail is stored at a central location on the network. Although the protocol is called "simple" the software which is required to implement it is generally quite complex, including ways to create, edit, send, and reply to messages, store lists of users who should get the same mail messages, and sometimes handle forwarding mail when a user changes locations or is away for a period of time. The UNIX application sendmail is actually a large and rather complex set of code which is notorious for containing bugs and security holes, especially because certain operations must be performed with the program running at the highest level of privilege possible in the UNIX operating system.

In order to include more complicated information in an e-mail message than simply ASCII text, features are provided which allow a user to encode data files of other types and attach that information to a message. UNIX systems and many other e-mail applications support a method called uuencoding of data files. Generally, the user needs to take a specific action to decode the attachment portion of a message in order to return

it to meaningful information. A more recent standard for encapsulating non-text information is using the Multipurpose Internet Mail Extensions (MIME). Any type of file including that of a word processor application, a spreadsheet, a graphic, or a movie or sound can be encoded using MIME and then attached to an ordinary message. MIME allows a message to be divided into multiple parts so that various differed attachment types can be included with a single message.

Another standard for electronic mail (also known as message handling) has been developed by the Consultative Committee on International Telegraphy and Telephony (CCITT). The X.400 standard forms a model for message handling where a User Agent (UA) sits on a local network or a user's desktop and allows the user to create and edit mail messages (Stallings). These messages are then sent to a Message Transfer Agent (MTA) which forms a network with other MTAs across the Internet. These devices can forward the message directly to the destination UA, or to a Message Store (MS) where it awaits delivery to the UA when the connection is available. One attractive feature of this protocol is that it does more than simply pass messages between machines at the Internet level; this protocol actually specifies the services that will be provided from the sender UA to the destination UA with various conditions handled in between. Even more attractive, the X.400 protocol is usually implemented in conjunction with the X.500 protocol which establishes a common directory structure for message system users. This signifies that a user will no longer be required to know a message recipient's full e-mail address (including all of the domains and subdomains of his or her host machine) but can look a particular user up in a directory somewhat like a phone book. Unfortunately, the Internet does not yet comply with the X.400 or X.500 standards. Currently, they are only used on large private WANs like the upcoming Defense Messaging System (DMS) in development to support the Department of Defense.

AmeriClean has never had a need to comply with a standard e-mail protocol, because all electronic communications in the past have remained on an isolated network. As a result, their current e-mail application was chosen for ease-of-use and ease of integration with the rest of the applications on the network. They therefore selected Microsoft Mail so as to keep the suite of software applications supported by the company

consistent. MS Mail has an intuitive graphical user interface, and requires little administration to maintain in conjunction with Windows NT. Since the users are very satisfied with their e-mail system and understand how to use it well, this system will be kept if at all possible. This assumption is in line with the design philosophy of reusing as much of the current architecture as possible, supporting the users' desires for a simple interface. This application can be used for Internet e-mail with the addition of a mail gateway as described above. Microsoft sells gateway software which translates its own mail format into messages that are compatible with any of a long list of other proprietary network protocols or with the Internet. The software package can be installed on the current mail server machine, and will function to translate MS Mail messages into SMTP format before forwarding them on to the router and then over the Internet pipe. This application can be purchased from Microsoft for about $1,800. This is fairly inexpensive solution because the only required additions to the network are software. And since non-ASCII file attachments are supported in MS Mail, there is really no reason to switch to another protocol. A PC version of the UNIX sendmail program would really offer no improvements, because it provides an awkward text-based interface which users often hide behind a menu driven application in any case. And implementing the X.400 standard at AmeriClean would requiring searching out one of the few User Agents which currently exist to support the protocol, while still requiring the use of a translating gateway. Since no benefits exist in changing e-mail applications, MS Mail will be maintained with the addition of a gateway.

A special mailbox should be set up within MS Mail to receive customer comments or complaints and to provide support. Rather than being assigned a user ID name, this account should be assigned a generic name such as custsupport@Americlean.com. An alias record can then be defined in the mail server software to map this generic name to the e-mail account of a user responsible for customer support. The benefit of an alias is that if the customer support contact changes jobs, leaves the company, or simply takes a long vacation, the mailbox itself does not need to be given a new name which would then need to be advertised to all customers and suppliers who send mail to that account. Rather, the

alias record could be temporarily or permanently changed to point to another user in a move which is transparent to all other users.

5.6 File Transfer

AmeriClean users have identified a requirement to pass large files of data over the Internet. They need this capability in order to download software upgrades and patches from the vendors, download regulations and material handling guidances from the government, and to distribute their own files of product and pricing information to customers. To a limited extend, files of information can be transferred through e-mail applications as attachments as described above. However, the resulting e-mail files are often quite large, and they tend to slow down the operations of the e-mail server. Some e-mail systems have limits on the lengths of the files they allow through so that service is not degraded. E-mail also puts all of the responsibility for transferring the information on the sender; the recipient is unable to effect the time of delivery or gain access to information unless the sender is available on his end.

There is a standard application supported by TCP/IP which is intended specifically for use in transferring such large files from one location to another. Called the File Transfer Protocol (FTP), it accommodates the transfer of both text and binary files, and includes the ability to control user access. The application sets up a TCP connection to a server machine that the user specifies, and then the user enters a user ID and password and information about the file he would like to transfer. He is able to chose whether to download a file from that location, or to upload a file from his local network to the remote server. There are two forms of FTP that differ in their means of allowing user access. Anonymous FTP only requires that the user ID "anonymous" be entered with a password of the user's e-mail address. Basically it is allowing anyone on the Internet to access the files made available, and is very commonly used as an information server supporting shareware software, lists of frequently asked questions, educational material, etc. Companies often use anonymous FTP as a public information server where customers or potential customers can access information about their products or even samples (such as evaluation copies of software). User FTP requires that only certain people may access the

information on the server. Those people have to be given an account on the server, as well as a user ID and password in advance. This method provides more security for the files on the server, but it is impossible to administer if the number of people with a valid need to access the information is large. It is also not a fool-proof method of security because users with a strong knowledge of security holes can sometimes break out of the directories set aside for FTP and can use their account on the machine to cause damage or access information not intended for the public.

There are a few other applications used for file transfer, but they are not as robust as FTP and were generally designed for specific purposes. Trivial File Transfer Protocol (TFTP) is a smaller and simpler transfer program which relies on sending UPD packets and waiting for a reply from the recipient, rather than establishing a TCP connection for the duration of the interchange. It is frequently used by diskless machines on a network which transfer a boot file from another network machine and boot from it when powered on. Such a protocol is not frequently used for a session established by users for file transfer; in addition it contains some severe security holes which make it dangerous to use in such a way.

Because AmeriClean requires the ability to post files of product information for customers to access whenever they desire, the network must not only contain an FTP client application to perform downloads, but needs an FTP server as well. This application may be hosted on a separate computer or a portion of another computer and should have a specific directory structure set aside for public files. This directory should contain an index and a readme file describing the contents of the directory so users can navigate to the file they need without assistance. There is really no need for AmeriClean's network to contain any writeable space for Internet users to upload files to local computers. This can be a dangerous practice, because it allows untrusted users access to local computers for their own storage and potentially execution of files. AmeriClean will therefore not allow files to be "put" to their machines in this manner. More details about the security of FTP can be found in the section on firewall architectures to follow.

One of the benefits of the Windows NT operating system is that it includes various tools for not only internal computer networking, but for support of external Internet

connections. One of these included tools is the software to support an FTP server. This is a full-service FTP server which can run in the background on any Windows NT server machine (Microsoft). It includes the capabilities to configure the system for anonymous FTP, user FTP, or both; the ability to set read and write permissions for each partition of the disk; To annotate file directories to provide contents information; and the ability to log connections to the FTP server for audit purposes. At any time, the system administrator is able to view the list of users who are connected to the server, and can disconnect any or all of these users if a security risk exists. Such an application may not be sufficient for a large FTP site, such as a software company which has constant requests for software downloads, or an educational institution which supports a server of Internet white papers and RFCs or frequently asked questions lists. Such sites would probably require a dedicated computer with significant disk space and processing power to continuously support hundreds of FTP connections at a time. However, for a corporation the size of AmeriClean, the Windows NT FTP server which supports 50 simultaneous FTP sessions will be more than sufficient. Additional benefits include the fact that it builds on the NT security features, does not require an extra machine or installation process, and uses the existing user accounts for setup of non-anonymous FTP sessions. This will be a simple to implement and cost effective solution to AmeriClean's file transfer requirements.

5.7 World Wide Web

The recent explosion of popularity for the Internet and its services has been most strongly driven by the introduction of the World Wide Web (WWW) and its supporting HyperText Transfer Protocol (HTTP). This distributed information service is simple to use and flashy, offering a mix of formatted text and graphics as well as hypertext links between information sources which allow a user to quickly move from one topic to another in a sort of stream of consciousness. The World Wide Web itself consists of a network of information servers which are located throughout the Internet. The information stored on these servers is presented in the form of pages which can be viewed using special client applications called Web browsers. Netscape is currently the most widely used browser, and many Web pages are specially formatted to utilize the

capabilities of the most recent versions of Netscape and appear most attractive when accessed with that tool.

Web pages are created using a scripting language called HyperText Markup Language. This language is designed to allow attractive page formatting, and to embed links which access pages stored on servers located anywhere on the Internet in a transparent fashion. Two major benefits of the World Wide Web are the ease with which a user can access information, and the ease of utilizing various Internet protocols. Special applications called search engines are used to search all Web servers for a particular topic based on one or more key words entered by the user. In addition, a user does not need to know how to operate some of the Internet protocols such as FTP. Instead, the Uniform Resource Locator (URL) used to indicate the address of the site to be viewed, specifies the protocol which is supported at that site. Examples of URLs for Web pages and FTP servers, respectively are:

http://www.microsoft.com

and

http://ftp.rtfm.mit.edu.

Accessing a site which supports FTP allows the user to perform file downloads through a graphical interface rather than from the command line. The browser software is responsible for actually performing the connection and the transfer.

AmeriClean needs to be able to both view information stored on other organizations' Web servers, and also to make information available to customers and suppliers of their own. Therefore, they not only require Web browser clients, but Web server software that can host the company's pages and accept connections from external systems and transfer the requested information across the Internet via HTTP. AmeriClean does not anticipate a high volume of access for this information. Because they are a small company and not really a household name, they expect to receive Web page accesses, or "hits" mainly from current customers and clients, with some potential customers accessing in order to research the company and its offerings. Therefore, AmeriClean does not need to invest in a top-of-the-line Web server package which is capable of supporting hundreds of external connections at a time without noticeable performance degradation. Rather,

they will be content with a package with supports 25 simultaneous access to AmeriClean's Web pages, with response time becoming slower if more connections are attempted. The server software must be easy to maintain, including tools which aid in administering the server and the information pages that it hosts. The package must include HTML authoring tools which assist users with little or no computer programming knowledge in creating Web pages.

A small class of Web servers, called commerce servers, offer the additional feature of encrypted communications between client and server applications. Currently, there is no standard encryption algorithm that is used by all such applications, but various companies have developed their own implementations and offered them up for public scrutiny, or have utilized publicly available encryption algorithms. These commerce servers are designed to allow information to be passed in a private manner from a WWW client application to a Web server located at any network on the Internet. The benefit of such a capability is most obvious in the field of Electronic Commerce/Electronic Data Interchange (EC/EDI). It allows business to be conducted over the Internet with orders being placed for product or services, and even allowing money to exchange hands via the transfer of credit card information. This capability could be especially useful to AmeriClean in streamlining the communications process between the headquarters organization and its customers. The standard order forms which are currently created and filled out in paper form should be reproduced as a HTML Web page form. These forms are special data objects on a page which allow the user to enter information rather than having read only access. Customers can then access the order forms from their own computer networks, and can fill out the orders electronically at their leisure. When the form is complete, simply clicking a button transfers the data back to the AmeriClean server where it can be loaded into the corporate database and used to initiate a sale. The encryption function of the commerce server will ensure that potentially proprietary information is not seen or understood by unauthorized Internet users.

The criteria to be used to select a World Wide Web server therefore include compatibility with Windows NT, since there is no benefit to purchasing a new UNIX machine or operating system for this purpose. The Web server should be hosted on the

same machine as the FTP server, since they are serving similar purposes of making non-sensitive information available to the public, and since the NT FTP server has been selected, the Web server should be compatible as well. This significantly reduces the number of available options. As mentioned above, the Web server must include HTML authoring tools, support up to 25 simultaneous connections, and include an encrypted HTTP protocol to provide secure electronic commerce. As always the cost of the package is a factor, because the company does not wish to pay for more functionality that they actually need, and the Web server should be as easy to administer as possible. The criteria to be used in selecting a Web server application are listed in Table 5-4.

Table 5-4: Criteria for Selecting a WWW Server.

Selection Criteria	Weight
Meets minimal requirements	Y/N
Compatible with Windows NT	10
Number of supported connections	5
HTML authoring tools included	7
Secure commerce capability	8
Cost	5
Ease of administration	7

5.8 Remote Network Access

In order to implement a remote communications connection between AmeriClean headquarters and traveling employees, a combination of hardware and software is required. A device must be able to accept incoming calls from remote users with modems, and must then connect the users to the internal network and to their files and directories. This device is called a communications server, and may be a dedicated machine such as a specialized Cisco router or a terminal server designed by Shiva. Alternately, a PC running server software may be used, supplemented with a multiport card with allows many connections to the same machine. Windows NT Server comes bundled with a Microsoft

product called Remote Access Server (RAS). This product is especially designed to run with the Windows NT operating system to turn an ordinary PC into a fully functional communication server. It sits upon all of the security features built into NT, and uses an NT protocol called Dynamic Host Configuration Protocol (DHCP) to automatically assign IP addresses from an allotted pool to machines as they connect to the network.

Since authentication is critical over a dial-in line where no physical security can be afforded, it is important that RAS can utilize a variety of standard authentication protocols. To perform authentication, RAS acts as a liaison between the user and an authentication server housed on the network - usually at the Internet firewall. RAS passes password, PIN, or challenge and response information between the two in encrypted format so that an outsider can not eavesdrop on the identity proving information and use it in a later attack (Microsoft).

For security reasons, the RAS software should be not be located on the protected Local Area Network. This could allow dangerous users to get access to company files, bypassing the authentication requirements. Similarly, the communications server should really not be directly connected to the Internet because there is danger of unauthorized users dialing into the server and using it as a starting point to attack other Internet sites. Therefore, the recommended location for this service is in combination with the Internet firewall and shall be described in the following section. Since all of the traveling salespeople will be using dial-in connections to AmeriClean periodically and perhaps at the same time, the four connection ports which are standard on a PC are not sufficient. A PC multiport board, such as those marketed by Digi International will be required to expand the connections. The RAS server will communicate with the firewall's authentication mechanism to assure the identity of the user. This authentication will be performed using a physical token such as Security Dynamics' SecurID smart cards. Each user who requires dial-in access (the entire sales force, at a minimum) will need one of these cards. Finally the remote sales force will each require a portable laptop computer from which to initiate the dial-in connections. In order to achieve a level of performance that will allow the sales force to perform their jobs, significant computer speed will be required. The computer should be a Pentium processor with at least 100 MHz processor speed. 16

Mbytes of memory will be required to handle the corporate database application and to cache Web pages and process Internet connections. It must include an internal 28.8k baud modem to make the remote connection and decrease download wait time to a minimum, and also posses a smart card reader to support the SecurID cards. Finally, the laptop should have a color active matrix monitor suitable for displaying presentations to customer representatives.

5.9 Internet Firewall

5.9.1 Architecture Analysis

5.9.1.1 Packet Filtering

A packet filtering firewall is the simplest and cheapest to implement, but accordingly provides the fewest security options (Carnahan & Wack). The firewall is actually implemented with a single router, or computer with two network cards which stores and enforces a set of rules regarding which attempted communications connections will be blocked. These communications, or streams of packets, may be blocked based on source or destination hosts, or on the ports which support various protocols and services. Therefore, the firewall can block communications from untrusted IP addresses or domains, or can block dangerous Internet services such as X Windows.

There are some serious disadvantages of packet filtering firewalls. One critical disadvantage is that they do not provide audit logging capabilities. Without this capability, attempted attacks on the network may not be recognized in time to halt the damage. If an attack does take place, it will be impossible to determine the source of the attack or the methods used to pose the attack. These firewalls also do not provide strong Authentication and Identification capabilities; required I&A programs must therefore be installed at each workstation. Attempting to control all Internet traffic using packet filtering can result in a huge list of rules which are difficult to test, and unwieldy to administer, as well as placing an enormous amount of responsibility on the router as the single element of protection for the entire network.

5.9.1.2 Proxy Server

Proxy server firewalls, also called application gateways, have been developed to relieve some of the problems of packet filtering systems. These firewalls use a computer called a Bastion Host (because it is most vulnerable to attack and therefore most highly protected) to host software programs which communicate with external Internet servers on behalf of the individual machines on the network. These software applications are called proxies, and one can exist for each service such as SMTP, HHTP, telnet, etc. Multiple bastion hosts may be utilized to share computing power more efficiently. Proxy servers are a software solution which may be used in conjunction with any of the following architectures as a portion of a complete firewall system.

The advantages of the proxy server firewall are that they can perform audits of security relevant events, can hide details of the internal network architecture, can perform strong I&A techniques, and use simple filtering rules. On the other hand, using a proxy requires either a modified client application or modified actions on the part of the user. It is difficult to make the use of a proxy transparent to the users.

5.9.1.3 Dual-Homed Host Architecture.

A dual-homed host consists of a bastion host with two network interfaces with routing capability between the two networks turned off. It completely blocks IP traffic between the network and the Internet, and only allows external systems or internal systems to communicate with the dual-homed host rather than with each other. Communication through a dual-homed host is accomplished either by the use of proxies or by allowing users to log directly into the host. Since providing accounts on the machine grants users too much freedom to change the security configuration, the use of proxies is recommended. In Windows NT, disabling IP traffic through a host is simply a matter of checking a box on the configuration setup, and is not very secure. In addition this firewall is not flexible enough for the needs of every site since only services with proxies are allowed.

5.9.1.4 Screened Host Architecture

The screened host is more flexible than the dual-homed host. A packet filtering router is used to block dangerous protocols from reaching the proxy server. The server is attached to the internal network and needs only a single network interface to pass services with proxies to the network. However, this architecture allows the router to pass some trusted services directly to the network by going around the proxy server. Here lies the flexibility, but also potential security leaks. In addition, the screening router provides a single point of failure for the internal network security, and if an attacker manages to compromise the host machine, there is nothing left between the dangerous user and all accounts and data stored on the internal network.

5.9.1.5 Screened Subnet Architecture

This firewall is a combination of the capabilities of a dual-homed host and a screened host firewall. It increases both traffic throughput and flexibility, but is more complicated to administer. The architecture consists of an exterior packet filtering router, an internal router, and a protected perimeter network. This network supports any machine which needs to host publicly available material. This can include the proxy server(s), FTP server, etc. The routers direct traffic to the appropriate server on the perimeter, as well as providing redundancy to ensure that a hacker would need to break into multiple systems to reach the internal network. The servers on the perimeter network would be the only machines seen from the Internet, which also protects internal machines from attack. Higher throughput rates are achieved than if a single router acts as a choke point between the Internet and the internal network. This is the best architecture for a site expecting a large amount of traffic or with high speed requirements. The System Administrator must ensure that no protocols are forwarded around the proxy servers, and that the packet filtering rules are correct and well-maintained

5.9.2 Recommended AmeriClean Firewall Design

Within the AmeriClean network architecture, a firewall takes on a position of extreme importance. The corporation is creating for the first time a link between its

private information and the outside world, and operating procedures for protecting such data is probably not yet in place. The management and staff may not believe that they are at risk from hackers or other malicious attacks, but hoping to remain secure by virtue of being obscure is foolish. The competition would love to get their hands on sensitive financial data, and some hackers enjoy the power of harming as many systems as possible, not just be attacking well-known or large ones. The firewall utilized should be as robust and fail-safe as possible, therefore a screened-subnet architecture combining a double layer of packet filtering with application level security implemented via proxy server software is recommended (Peterson).

The firewall architecture will consist of three main parts:

- ***Exterior Router***: Is needed to protect the perimeter network from the external, untrusted world.
- ***Perimeter network***: Contains the bastion host (Proxy server) and possibly separate machines for information services (such as an FTP server).
- ***Interior Router***: Is used to protect the internal network from the Internet and from a potentially compromised bastion host.

5.9.2.1 Security of supported Internet Services

5.9.2.1.1 FTP

Outgoing: FTP is too risky to implement with straight packet filtering. Normal mode FTP requires the internal client to contact an external FTP server requesting a session on the control channel. However, the remote server is then given authority to initiate a connection to the internal client on an arbitrary port above 1023 to be used for the data channel. Use of packet filtering would require that all ports above 1023 permit incoming connections, leaving countless holes and open accesses. There is an alternative called passive mode FTP which allows the client to open both connections (data and control) however it cannot be consistently used because not all servers support it. Proxying will be a better choice because it allows reliable communication with no incoming connections except to the bastion host.

Incoming: Since there is a requirement for AmeriClean to make large files available for external users to download, an FTP server needs to be setup as well. This may be set up in one of two ways; to allow anonymous FTP or to allow only identified user FTP. User FTP requires that a user have an account on the server and they can then access any files they could reach when logged in. This is difficult to secure, and again allows untrusted users many privileges by granting them accounts on a secure machine. Anonymous FTP allows anyone external to the company to access the files which are specifically made available for public use. The recommendation is for AmeriClean to support anonymous FTP on a separate FTP server machine, allowing download only of files which the System Administrator has reviewed and certified as not containing sensitive information. The separate machine ensures that if an external user manages to get beyond the directory allocated for FTP files, there is no information of importance that he can access or corrupt. It is recommended that AmeriClean not provide write-able space on the FTP server for external users to upload files. These spaces are usually found by hackers and used to store or transfer undesirable materials, resulting in denial of communications services. Other file transfer protocols are impossible to guarantee secure, and therefore will not be allowed through the firewall (such as TFTP - trivial file transfer protocol, and FSP - file service protocol) (Chapman & Zwicky).

5.9.2.1.2 E-mail

The AmeriClean network will need to utilize an e-mail gateway to convert between Microsoft Mail format and the UNIX SMTP (Simple Mail Transfer Protocol) understood by the Internet. In addition, a mail server on the internal network will need to accept incoming messages and to forward them to the appropriate user's mailbox and to accept message from AmeriClean users and determine whether they need to be routed to other users on the network or sent on to an external network.

Outgoing: The AmeriClean mail server should be configured to send all outgoing mail to the bastion host. When the mail server on the bastion host receives the message, the message shall be forwarded to the external network. Mail will be forwarded to the Internet with the name of the bastion host as part of the e-mail address, rather than with

the names of individual internal machines, preventing external users from knowing about internal AmeriClean machines.

Incoming: Packet filtering should be used to allow incoming SMTP connections only to the bastion host on the perimeter network. The internal router will allow SMTP connections only from the bastion host to the mail gateway and server on the internal network. Use DNS MX (mail exchange) records to direct all incoming mail to the bastion host. The mail server on the bastion host will then route all incoming mail messages to the internal network. The mail server will need to determine which user receives the message. Since the bastion host only sends incoming mail to a single mail server address, this reduces the number of internal systems that can be attacked using SMTP if the bastion host is compromised.

5.9.2.1.3 HTTP

Client: Since HTTP can be configured to use one of many non-standard ports, packet filtering will not be a useful way of handling this service. Use of a proxy will provide access to servers on any port. The most popular and widely available HTTP clients (such as Netscape and Mosaic) support HTTP proxying, so the usual concern about proxying requiring special clients does not apply.

Server: The Web server should be located on a separate machine. As long as no additional servers are running on the same machine, a potential attacker can create little damage if he were to break out of the expected directory of public information. Since AmeriClean is already supporting an FTP server for public information which is also secure and has no write-able directories, an exception may be made to house those two servers on one machine to save money. If possible, a server should be selected which supports page caching in order to make response time faster and to decrease the total user bandwidth. No portion of the Web server shall have write-able directory access for any user except the System Administrator. This prevents attackers from uploading malicious code that the client will execute without recognizing the danger.

5.9.2.1.4 DNS

Since the firewall will be utilized to authenticate external user identities, and potentially to pass that information along to other hosts on the AmeriClean network the firewall should validate the accuracy of the host names of the communications initiator by performing double-reverse lookups of the name. To do so, the system performs a reverse lookup to determine the host name of the IP address on an incoming data packet. It then performs a normal DNS lookup for the IP address of that host name. If the original received IP address and the looked up address are the same, then the communication is probably not being faked. This solution is more secure than simply believing the incoming information, but it is not infallible. The only way to make completely sure that a packet originated from the claimed IP address is if some form of cryptographic authentication is used.

DNS can also be used in a defensive manner to hide information about the internal network from the outside world. The less a potential attacker knows about the configuration of the network, the types of machines utilized, and their names, the more difficult it will be to launch an intelligent attack on the network. Therefore, the recommended firewall will use DNS to hide internal network information. The system needs two DNS servers; one on the internal network which knows all of the information about the names and addresses of internal machines, and one on the perimeter network which functions as though it knows all of the same information, but in reality provides the external world with a modified version.

Configuring "fake" DNS server: The "fake" DNS server on the bastion host is the machine pointed to by DNS servers in the parent domain (at the Internet provider). This server acts as though it knows all the information about the domain, but it really stores only host name and IP address information about the machines which a user on the Internet would need to contact directly, such as servers on the perimeter network. DNS MX (message exchange) records must be published for each internal host or domain name which is used in e-mail addresses; otherwise external users will not be able to correctly reply to the message.

Any internal machine whose IP address will be seen by the outside world needs to have DNS configured to map a fake host name to the real IP address and vice versa. Using proxies makes this step unnecessary since the external world will only see the IP address of the proxy server - a significant time saver in configuration and maintenance.

Configuring Real DNS Server: A second DNS server which knows the real host names and IP addresses of all internal machines is set up on the internal network. This allows internal machines to be able to communicate with each other, as well as with external machines, by name. This should not be accomplished by allowing the internal DNS server to query Internet DNS servers directly, because the packet filtering would need to pass UDP (User Datagram Protocol) packets to the internal network. DNS runs on this protocol, but so do several other dangerous and nearly impossible to secure services, which must be blocked. Instead, the internal DNS server is configured to forward queries it cannot answer to the bastion host DNS server. This machine then deals with the external network.

Configuring Internal Clients: All DNS clients on the internal network must be configured to send name resolution queries to the internal, real, DNS server. If the request is about an internal machine or a machine whose address is stored in the cache, the server sends the correct reply to the client. If it does not know the answer, it forwards the request to the bastion host DNS server which determines the answer from the appropriate Internet DNS servers. It will answer the internal server which then answers the internal client.

Configuring Bastion Clients: Any DNS clients on the bastion host (proxy applications, for example) should be configured to make their name requests to the DNS server. This allows the applications to know the real host names on internal machines in order to send them traffic, while still hiding this data from the outside world. This does impose an extra step on requests regarding external machines, because the request is made of the internal DNS server which forwards external machine requests back to the bastion host.

Summary: The firewall architecture should use packet filtering and proxies to implement DNS service. Two distinct servers will be utilized to ensure that AmeriClean's

machines have all the information they need to communicate with both internal and external; machines by name, while external machines are only aware of the existence of the proxy server and information server machines on the perimeter network. In addition, double-reverse lookups should be used to ensure that incoming IP addresses are not faked (Chapman & Zwicky).

5.9.2.1.5 Modem Access

Providing access to the network via modem creates a potential backdoor to security, and therefore must be very carefully designed and secured. The user will dial in to a terminal server and then remotely connect to a particular system. This server should be located on the perimeter network, with the exterior router preventing direct routing between the Internet and the modem pool. The interior router would in a similar manner prevent routing between the internal network systems and the modem pool. The system should require strong Identification and Authentication of the user's identity before allowing access, using a physical token and a memorized password or PIN. Users dialing into the pool would have to go through the proxy server before accessing either internal network systems or the Internet. AmeriClean must make sure that no users connect modems anywhere else on the network than through the modem pool in order to keep the firewall system as simple as possible, and not introduce security holes.

5.9.3 Firewall Selection Trade Study

As the popularity of the Internet has expanded and the number of organizations connected to it has increased, the threat of attack by a hacker has increased as well. Therefore, many companies have either started or expanded their computer products to include security devices and Internet firewalls (Cooper, et.al.). As discussed above, these firewalls come in many different configurations and provide different levels of security, from that suitable for a single user to those capable of securing government agencies whose networks store confidential information. To perform the selection of a firewall for AmeriClean, the potential firewall vendors were screened to select those which provide systems including hardware and software because AmeriClean does not already own the type of powerful UNIX computer usually required as a host for a firewall, and would

prefer to use a machine supported by the firewall vendor and tested for reliability. In addition, hardware and software systems are delivered with the minimum configurations completed, which will ease some of the burden on the contractors and the system administrator. It must fulfill all of the recommendations listed in the recommended architecture section including packet filtering, application proxies, hiding internal addresses and names, etc. The procedures used to test the system must be documented and readily available so that the purchases can review them. And it must provide for support of a large and complex network, to allow AmeriClean room to grow in the future without having to increase security concerns. The following firewalls passed this screening and were selected for evaluation:

- ***Gauntlet*** - by Trusted Information Systems
- ***Sidewinder*** - by Secure Computing Corporation
- ***Smartwall*** - by Virtual Open Network Environment (V-ONE)

The primary features of each product are as follows:

5.9.3.1 Gauntlet:

- *Secure application gateway architecture* - Gauntlet functions as a dual-homed Bastion host with proxy applications, and can create a screened subnet with the addition of a router.
- *Modified UNIX operating system* - The basic BSD operating system is enhanced to prohibit IP address forwarding, detect IP spoofing attacks, support encrypted IP communications, and to prohibit source routing of packets.
- *Many supported proxy applications* - These include proxy applications for terminal services, file transfer, e-mail, WWW, gopher, X windows, printer, and remote execution. The use of these proxies is transparent to the network users.
- *Includes DNS, WWW and FTP servers* - If a site desires, they can host these services directly on the firewall machine so external users do not have to be allowed through the firewall.

- *Administration tools* - Firewall administration and setup can be performed from any host on the network or from a laptop computer using a Web browser. This graphical interface eases the complexity of administration and the time required to perform it.
- *Strong I&A* - The firewall supports the following types of authentication devices for screening telnet and FTP connections as well as dial-in connections: Enigma Logics, S/Key software from Bellcore, SecurId from Security Dynamics, SecurNet Key from Digital Pathways. Support for the following devices is under development and will be available in upgrades: CryptoCard, and DigiPass.
- *Configurable audit* - Gauntlet can capture all services which take place through the firewall to an audit log, which can be written to a secure machine. E-mail messages can be used to alert the administrator of events which take place which are specified as critical.
- *Firewall to firewall encryption* - Two networks protected by Gauntlet firewalls can encrypt all data communications between the two using the Data Encryption Standard (DES).
- *Crystal box / Simple Code* - The source code for all Gauntlet applications is included with each purpose for review. Software is designed to be short and simple with the average application requiring 1500 lines of code.
- *Packaging* - Can be purchased as a combination of hardware and software, pre installed and minimally configured or as software or upgrade only.
- *Cost* - The hardware and software solution system costs approximately $15,000.

5.9.3.2 Sidewinder:

- *Secure application gateway architecture* - Sidewinder functions as a dual-homed Bastion host with proxy applications, and can create a screened subnet with the addition of a router.
- *Secure operating system* - SCC has enhanced the BSD/OS UNIX operating system with type enforcement and with separate domains which support the operation and administration of different a[applications. This technology provides each user and application with the lowest level of privilege needed to perform their tasks, and was

developed and proven as part of the Department of Defense Multilevel Information System Security Initiative (MISSI). Two separate network stacks are maintained for information connected to the Internet and information connected to the internal network.

- *Transparent proxy applications* - Sidewinder includes the following proxy applications which are transparent to the user and hide the addresses of internal machines: NNTP news, Gopher, WWW, FTP, telnet, AOL, SSL, POP, WAIS, and whois. Additional proxies can be created for TCP-based services which use a consistent port.
- *Includes WWW, DNS and FTP servers* - These services may be hosted on the firewall machine if the site wishes. There are separate DNS servers provided for the external and internal stack in order to advertise different name information to the internal network and the outside world.
- *GUI administration and audit support* - Sidewinder uses a point and click interface for configuring system options and modifying access control lists. The administrator can run pre-defined reports which depict system operational statistics.
- *Strong I&A* - The Sidewinder supports the following authentication methods for FTP and telnet connections as well as dial-in connections: SCC's LOCKout authentication server, Digital Pathway's Defender Security Server (SecurNet Key), Security Dynamic's SecurId, or DoD Fortezza cards. The firewall can also require password entry for outgoing connections in order to log and audit internal use of services.
- *Configurable audit with alarms* - The administrator can select which events are audited and can be notified by e-mail, pager, or printed message of such an event. Critical events can trigger the "Strikeback" feature which collects information about the source of an attack and then terminates the session and automatically notifies the source site of the detected actions.
- *Firewall to firewall encryption* - This capability will be provided as part of the Sidewinder firewall in June of 1996. It performs mutual authentication of the remote and local connection machines and encrypts all communications using DES.
- *Packaging* - A bundled turnkey solution of hardware and software may be purchased, or the software may be bought separately.

- *Cost* - The combined hardware and software solution with customer support for up to 100 users costs approximately $16,000.

5.9.3.3 Smartwall:

- *Application gateway and packet filtering* - Smartwall supports both software proxy applications and a limited ability to perform filtering on incoming packets
- *Transparent proxy support* - Supports proxies for telnet, FTP, e-mail, network news, remote login, oracle database, WWW, gopher, and X windows without inconvenience to the user.
- *User Friendly GUI* - Allows the system administrator to configure the system and set rules through a graphical user interface.
- *Strong I&A* - Smartwall supports mutual authentication of remote access and can authenticate using the following devices: SecurID, SNK, Fortezza cards, and S-key.
- *Real-time auditing and monitoring* - Constantly analyzes all interactions with the firewall to indicate suspicious activity as it happens. Logs all activity and generates periodic reports.
- *Firewall to firewall encryption* - Supports the DES and RSA encryption methods to create a secure connection between two locations using Smartwall firewalls.
- *Supports three network interfaces* - Most firewalls only support an external and an internal network. Smartwall can connect to three networks, supporting large organizations
- *Supports multiple firewalls in parallel* - An organization which anticipates a high load of Internet traffic can install multiple Smartwalls in parallel and can distribute the load between them.
- *Electronic Commerce Capable* - Uses secured versions of telnet and HTTP to protect a network commerce server and send credit cards transactions over the Internet.
- *Customer support* - V-ONE provides telephone technical support 24 hours a day, seven days a week. Installation and training is included in the cost of purchase.
- *Packaging* - This hardware and software solution includes various extras such as installation and training, and ear of free patches and upgrades.

- *Cost* - a single Smartwall system costs approximately $18,000.

The differentiators for each product are as follows:

All three firewall offer similar general capabilities are fall within the same range of security options per dollar. The Smartwall is a little more expensive, and appears to be more firewall than AmeriClean really needs. Some of its differentiators focus on the ability to support multiple network interfaces and exceptional high-load networks (at the cost of multiple systems) but those features are not required in a small company even allowing for annual growth over the lifetime of the network. Other features, such as commerce capability have already been allocated to other network components and should not be paid for twice. Very little mention is made of the operating system and its means of providing security; it is more difficult for the customer to prove assurance.

The Gauntlet firewall software is well-understood. It's applications have been reviewed for bugs and have been used by thousands of network through TIS's publicly available firewall toolkit. However, its operating system itself is fairly standard UNIX with several options disabled. It appears to meet the minimum security requirements but does not include any real differentiators. Sidewinder , on the other hand, is built on an operating system which has been proven secure by the National Security Agency. Its division of applications and users into domains based on their needed privileges and the separations of network stacks ensures that untrusted users are restrained to harmless operations. And the ability to determine information about an attacker and notify their site offers more of a chance that an attacker will be caught. Table 5-5 demonstrates the trade study matrix which lead to the selection of the Sidewinder firewall.

Table 5-5: Trade Matrix for Firewall Selection.

Selection Criteria:	Weights:	Gauntlet	Sidewinder	Smartwall
Meets minimal requirements	Y/N	Y	Y	Y
Security	10	30	60	30
Support recommended architecture	8	24	24	24
Audit and alarm capability	4	12	24	12
Strong I&A	6	36	36	36
Ease of use (transparent)	5	30	30	30
Ease of administration	8	48	48	48
Cost	3	18	9	9
Total:		198	***231***	189

5.10 Network Architecture Summary

Based on the design issues discussed in the system detail design, the components which are required in the AmeriClean communications network are shown in **Table 5-6.**

Table 5-6: Total Components Required.

Component	Quantity	Cost	Description
Internet Access - setup	1	$10,000	T-1 leased line and any required tech support for setup.
Internet Access-monthly	1	$1,200	Monthly service and lease fee.
RAS server software	1 (already on hand - comes with NT)	N/A	Software which will allow a PC server to function as a communication server for dial-in connections. Will be hosted on the new Windows NT server.
RAS client software	15 (already on hand - comes with NT)	N/A	Allows sales people to use their laptop computers with modems to connect to the headquarters network.
DigiBoard	1	$5,000	Allows the PC hosting RAS software to support up to 255 connections.
SecurId cards	15 (sales)	$100	Smartcard which allows for strong I&A of remote connections.
Firewall	1	$16,000	Screens connections between the Internet and AmeriClean for security.
Cisco 2500 Exterior Router	1	$2,000	Allows AmeriClean network traffic to reach the Internet. Implements packet filtering security rules.
Cisco 2500 Interior Router	1	$2,000	Completes the screened subnet between the firewall and the protected network.
User Workstations	40 (already on hand)	N/A	Computers directly connected to the AmeriClean LAN.
Portable Laptop Computers	15 (sales)	$2,900	Computers for the sales force to use on business trips.
FTP server	1 (comes with NT)	N/A	Used to make information publicly available for download.
FTP clients	55 (comes with NT)	N/A	Used to access other FTP sites (40 for AmeriClean LAN, 15 for laptops).
Web server	1	$2,700	Makes AmeriClean's Web page

			available for external view. Will be installed on new NT server machine.
Web clients	55	$125	Allows AmeriClean employees to view other organization's Web pages.
Mail Server	1 (already part of LAN)	N/A	Stores messages until the user requests them. Forwards messages to the proper recipients.
Mail clients	55 (already have)	N/A	Interface that allows users to create and read e-mail.
Mail gateway	1	$3,000	Converts MS Mail format to SMTP.
DNS server	2	$1,500	Translates machine names to IP addresses. One for internal LAN, one for firewall.
Windows NT Server	1	$5,000	New machine is needed to function as the information server and communications server.

The network architecture as it will appear when the enhancements are complete is depicted conceptually in Figure 5-3. The bottom network represents the current AmeriClean LAN. The top of the diagram includes the components needed to provide Internet and remote dial-in access and network security.

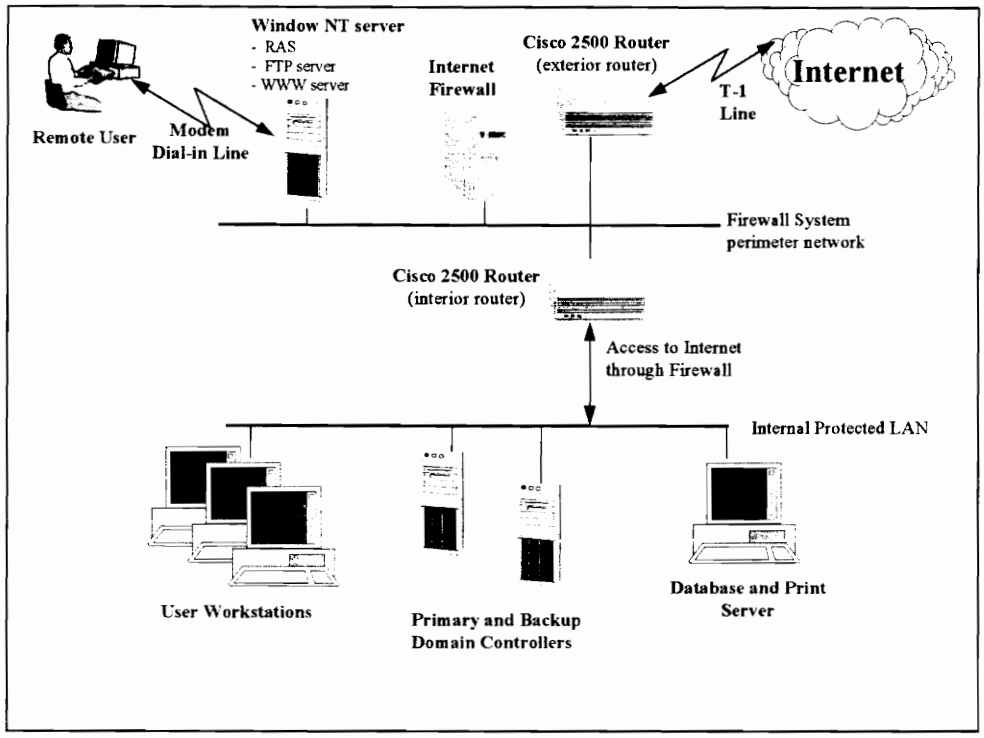


Figure 5-3: Recommended Network Architecture.

6. Life Cycle Cost Analysis

6.1 System Plan

Development of the AmeriClean external communications network will take place in three phases, Research and Development, Integration and Implementation, and Operation and Maintenance. No analysis is performed on the retirement and disposal of the system, because the system is designed to be continually updateable by replacing components of software or hardware as improved technologies become available, rather than being replaced by an entire new system. During the Research and Development phase, contractors will work to design a network architecture that meets the specified system requirements. The Integration and Implementation phase will entail procurement and installation of all components of the system, first in a separate test network, and after being tested as a portion of the AmeriClean operational LAN. Finally, the Operation and Maintenance deals with the continuing use of the network, repairing problems, and enhancing the system to support corporate growth and improved technologies.

6.2 Life Cycle Cost Evaluations

The main objective of the life cycle cost analysis is to determine the cost of the AmeriClean system. The life cycle cost will be based on all the costs associated with the development of the network, and will be determined for a five year period. The system should be operational in its completed form for this period of time, with a new evaluation of AmeriClean's requirements becoming necessary if the company continues to grow and modify its mission within the five year period.

6.3 Cost Breakdown Structure

The total system product cost can be determined from the costs of the three phases of the system life cycle. Each of the phases of the life cycle is composed of activities that must occur. A Cost Breakdown Structure(CBS) is used to portray the activities and their associated resources involved in the development of the system. It presents a logical

subdivision of cost by functional activity area. Figure 6-1 shows the Cost Breakdown Structure(CBS) for the AmeriClean network (adapted from Blanchard, p 513). The procurement cost of components described in Table 5-6 would be included in the engineering design activity (C_{RE}), under Research and Development (C_R)

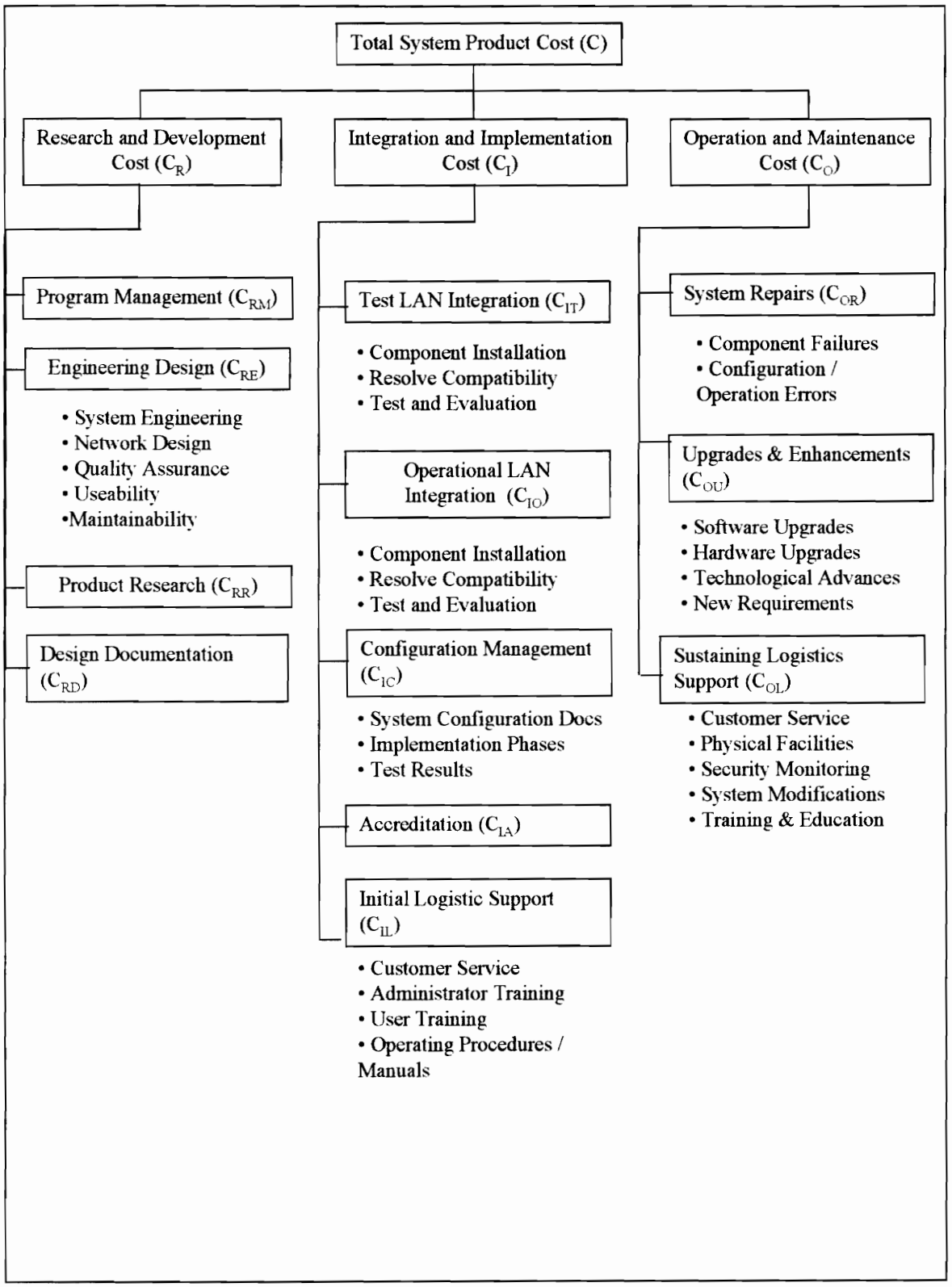


Figure 6-1: AmeriClean Network Lifecycle Cost.

6.4 Cost Activity Definitions

Research and Development Cost - The costs associated with all aspects of the Research and Development activities. Most of these costs are higher during the beginning of the project when the contractor design team is involved and technological alternatives are being evaluated. Ongoing R&D costs can include keeping current on technologies, and researching possible network enhancements. In year 5, some of these costs will start to rise again in anticipation of major modifications due to new company needs and requirements, and large component overhauls needed to replace obsolete equipment. The Research and Development Cost includes the following activities:

- **Program Management** - Costs associated with the management of the program. These costs (in present dollars) will be highest during system development, and while the contractors are directly involved.
- **Engineering Design** - Costs associated with System Engineering, Network Design, Quality Assurance Usability, and Maintainability. Includes contractor cost.
- **Product Research** - Costs involved in researching available commercial products which may fulfill system requirements. Includes research time and materials, telephone calls, and attendance at product demos,
- **Design Documentation** - Costs associated with creating the necessary documentation. Documentation includes the Concept of Operations, Maintenance Concept, Systems Requirements Document, System Design Document, Test Plan/RVTM, Test Results, User's Manual/Standard Operating Procedures, and System Administration Manual.

Integration and Implementation Costs - Costs used to install the selected COTS components and integrate them with existing components first in a test LAN and then in the operational LAN. Configuration and troubleshooting skills are utilized, in activities which include:

- **Test LAN Integration** - Cost of procuring commercial network components. Engineering labor costs associated with installation of those components,

configuring the system to meet AmeriClean requirements, and testing the architecture. Debugging and some design changes may be required.

- **Operational LAN Integration**- Costs associated with migrating the working test network capabilities to the operational LAN. New components must fit within the existing framework; users should be disrupted as little as possible; security must be preserved to protect company proprietary information.
- **Configuration Management** - Costs associated with keeping various configurations of components distinct. Documentation is completed and maintained in a file or tech library, test results are filed and accessible for queries, no changes are made to network configuration files without being captured and justified.
- **Accreditation** - Costs associated with creation and execution of a formal testing and presentation package which assures AmeriClean management that the system meets the requirements and is secure for use.
- **Initial Logistic Support** - Costs associated with logistic support planing and development of system support requirements. Included are the costs of customer service, administrator training, user training, creating of operating procedures and manuals.

Operation and Maintenance Cost - After the system design is complete and the network is operational, this is the longest running phase of expense and can become quite expensive if room for modifications and growth were not considered in the design process. O&M costs include:

- **System Repairs** - Costs associated with unscheduled maintenance required to keep the system operational over the course of its lifetime. May include failures of components either due to malfunctions or to extensive use; as well as errors in the way in which the system is installed and configured.
- **Upgrades and Enhancements** - Costs resulting from scheduled maintenance which will keep the system current and useful over its lifetime. Includes periodic upgrades of hardware and software, as well as purchase of

components with new capabilities or which are needed to fulfill new customer requirements.

- **Sustaining Logistics Support** - These costs include maintenance activities not directly related to the mission specific system components. These include supporting the facilities which house the system, ongoing training for new users or for system changes, ongoing administration and monitoring of security features and audit logs, miscellaneous system changes, and supporting user problems.

6.5 Cost Estimates

The cost estimates for the AmeriClean communications network would then be developed for the five year expected life time of the network. Elements of the CBS are summed up to achieve values for their parent items. When all item costs are estimated, a total cost for the system can be determined. The costs can be predicted using current 1996 dollars, with the total dollar amount adjusted for 5% inflation per year. At this time, a well-informed estimate can be made of the value of the project over its lifetime versus its total cost. The maximum areas of cost over the lifetime of the system would fall under system maintenance, specifically Sustaining Logistics Support and Cost of Upgrades and Enhancements. In future system analysis, estimates will have to be created for each of the activities described in Figure 6-1. Currently, only the cost of procuring network components has been identified. The additional costs of labor, engineering resources, system support, etc., must all be calculated before it can be determined whether the recommended system is really a viable alternative in regards to cost.

The cost estimates for the AmeriClean communications network would then be developed for the five year expected life time of the network. Elements of the CBS are summed up to achieve values for their parent items. When all item costs are estimated, a total cost for the system can be determined. The costs can be predicted using current 1996 dollars, with the total dollar amount adjusted for 5% inflation per year. At this time, a well-informed estimate can be made of the value of the project over its lifetime versus its total cost. The maximum areas of cost over the lifetime of the system would fall under system

maintenance, specifically Sustaining Logistics Support and Cost of Upgrades and Enhancements. In future system analysis, estimates will have to be created for each of the activities described in Figure 6-1. Currently, only the cost of procuring network components has been identified. The additional costs of labor, engineering resources, system support, etc., must all be calculated before it can be determined whether the recommended system is really a viable alternative in regards to cost.

7. Test and Evaluation Plan

7.1 Introduction

As the AmeriClean communications network is being designed and developed though the systems engineering lifecycle, a parallel testing process is involved at each phase. As part of the systems engineering of the network, a test plan will be developed which will be used to verify system operational performance against the operational requirements of the system. This is accomplished through an iterative testing approach that examines system performance throughout the system life cycle. The test process assures that requirements have been met, determines areas in the system which need to be improved to meet system specifications, and reduces design costs by indicating problem areas as early as possible in the life cycle. This allows designers the maximum amount of time to correct any problems and minimizes the re-work costs to bring these areas into conformance with system specifications.

The development of the network test plan is begun during the latter stages of the conceptual design and the testing is executed through the deployment phase of the lifecycle. A variety of testing techniques are used during these stages, including analytical analysis, component testing, integrated component testing, and user testing. Finally, it attempts to minimize its own costs and execution time through a well-planned, logical progression of testing which eliminates the need to re-visit previous testing. Additionally, wherever possible, tests are combined to measure multiple system requirements.

In this project, the testing process is somewhat streamlined because the focus of the project is on component integration. Just as the philosophy of utilizing COTS components when possible decreases the cost and effort involved in developing and implementing the network system, it also eases the testing required. Most commercially available hardware and software products have been subjected to a rigorous process of testing within the development house, and through actual use at beta test sites, before being released to the market. Some companies make records of these tests publicly available. Others have their products tested and reviewed by independent third parties or

for documentation in trade magazines or journals. The testing process executed on the AmeriClean network will not repeat such tests in a time-consuming waste of effort. Rather, it will concentrate on testing the interfaces between components to ensure that the system as a whole meets the operational requirements.

7.2 Test Plan Methodology

The iterative test plan consists of five distinct testing phases - Analytical, Type 1, Type 2, Type 3, and Type 4 testing. These steps are designed to guarantee that system requirements are being met during each phase of the system design. They also are vital in surfacing potential system design problems as early as possible in the life cycle.

The test plan's first phase, analytical testing, is performed during the latter stages of conceptual design and throughout the preliminary design phases of the project life cycle. This phase is used to evaluate and predict the anticipated characteristics of the network. It is also used to indicate design areas that initially do not meet operational requirements. Because this testing phase occurs early in the system's life cycle, changes are easy to incorporate into the evolving system design and usually have little cost associated with them. Most analytical tests involve modeling the system, or performing research into the known capabilities of technologies and components. Much of the analytical testing of potential components will have been performed during component development and can be researched. Examples of analytical testing include:

- Ensuring the possibility of achieving the throughput requirements of the network,
- Determining limits for the performance and speed of various applications,
- Modeling the expected load on the information servers over the use profiles of the system.

The next phase, Type 1 testing, is performed during the early phases of the project's detail design phase. Type 1 testing is used to determine if potential network components meet system design requirements. It also helps to determine if functional integration of components allows these components to meet system requirements.

Assuming proper functional separation has been maintained between system components, necessary design changes will require minimal cost and time to implement. Type 1 testing includes:

- Testing the compatibility of the NT operating system with network components,
- Testing the integration of MS Mail with the UNIX gateway,
- Testing the router configuration allows Internet access in both directions.

The third testing phase, Type 2 testing, is performed during the latter stages of the system's detail design phase. Type 2 testing is used to evaluate the integrated system prototype. In the AmeriClean project, it may be useful to test and develop Internet connectivity as a second network, physically and logically separate from the existing LAN. Type 2 testing could be well-utilized to test the operations and security of this prototype LAN before the operational system is migrated to such connectivity. Successful Type 2 testing verifies that system maintainability and reliability for individual components and across component interfaces meet or exceed requirements. Because most of the design is nearly completed prior to this testing, changes made during this testing phase require moderate to significant cost and time expenditures. A complete set of test procedures will be executed by the design team at this time to ensure that every functionality works as planned. Type 2 testing activities can include:

- Successful sending and receipt of e-mail,
- Browsing the Web pages of other sites, and accessing the AmeriClean page from the Internet,
- Performing intrusion testing or "hacking" on the Internet firewall.

The forth phase, Type 3 testing, is performed after system qualification but prior to full scale operational use. Type 3 testing is used to determine if the fully integrated system meets system requirements when utilized by consumers. To execute this phase of testing, a small subset of the computer users at AmeriClean will be trained in the use of Internet services, and will be granted access to the client software. The rest of the company will

not yet be given access. For a defined period of time, this test population will utilize the new capabilities in performing their daily tasks, and may surface additional system problems, as well as problems with the training and documentation. This process validates the compatibility of prime equipment with logistical support, and verifies the compatibility of the various levels of logistic support. Because of the advanced state of the project life cycle, changes made during this testing phase are the most costly and time-consuming for the company to absorb. Type 3 activities include:

- User execution of network scenarios,
- Spontaneous use of network capabilities in the completion of business tasks.

The final phase of testing, Type 4 testing, is performed during the operational lifetime of the network. Type 4 testing is essentially a process of monitoring system operations and is used to gain additional insight into a particular area of the network design. Type 4 testing also allows system designers to discover possible areas for improvement in future designs and indicates system requirements that were not surfaced during previous stages of design. Because of the unpredictability and exploratory nature of changes implemented during this phase, the cost and re-work time for changes made during this phase are extremely variable. They depend entirely on the type and scope of the change being implemented in the network. Possible Type 4 activities include:

- Testing system performance under more rigorous utilization patterns,
- Testing system performance under more extreme environments,
- Testing alternate user interface designs to improve consumer ease of use.

Figure 7-1 (Blanchard, p 104) shows a graphical representation of the system testing. It shows the effectiveness of system evaluation for each testing phase. Additionally, Figure 7-1 shows when each phase occurs during the system life cycle.

Figure 7-1: Test Phases in the Systems Engineering Lifecycle.

7.3 Test Plan Procedures and Implementation

To maximize the effectiveness of the test plan, all phases of system testing are governed by the following procedures. First, the test plan uses a Requirements Verification and Traceability Matrix (RVTM), linking each test performed to one or more system requirements. Using an RVTM assures that all requirements are inspected and validated during system testing. It also helps to reduce testing redundancy, saving the project time and money.

The network test plan further streamlines testing by using a combination of inspection, evaluation, and verification testing methods throughout the testing life cycle. By selecting the appropriate testing method based on the testing phase and information required for a particular test, the test plan ensures that the proper amount of data and analysis is performed at each phase of the system life cycle. It also uses normal operations testing and error scenario stress testing to ensure that the system meets required performance levels. In situations where the system does fail, stress testing ensures that it fails in a safe manner.

Finally, all testing results are documented using a standard test documentation format. This format begins by creating a unique report serial number for each testing report. This serial number, used in the requirements and usability traceability matrix, clearly identifies each testing report. By generating this number using specific prefixes for the testing phase, method, and type (i.e. operations or stress testing), critical testing information is encoded into the serial number for quick reference.

Test reports then provide the following information:

- Date(s) of testing
- Name of the individual preparing the report
- Component(s) tested
- Requirement(s) tested
- Test equipment and personnel used
- Test procedures utilized
- Data gathered during testing

- Analysis of testing data

This information is formatted as shown in Figure 7-2, and ensures that all information critical to testing has been captured for later use.

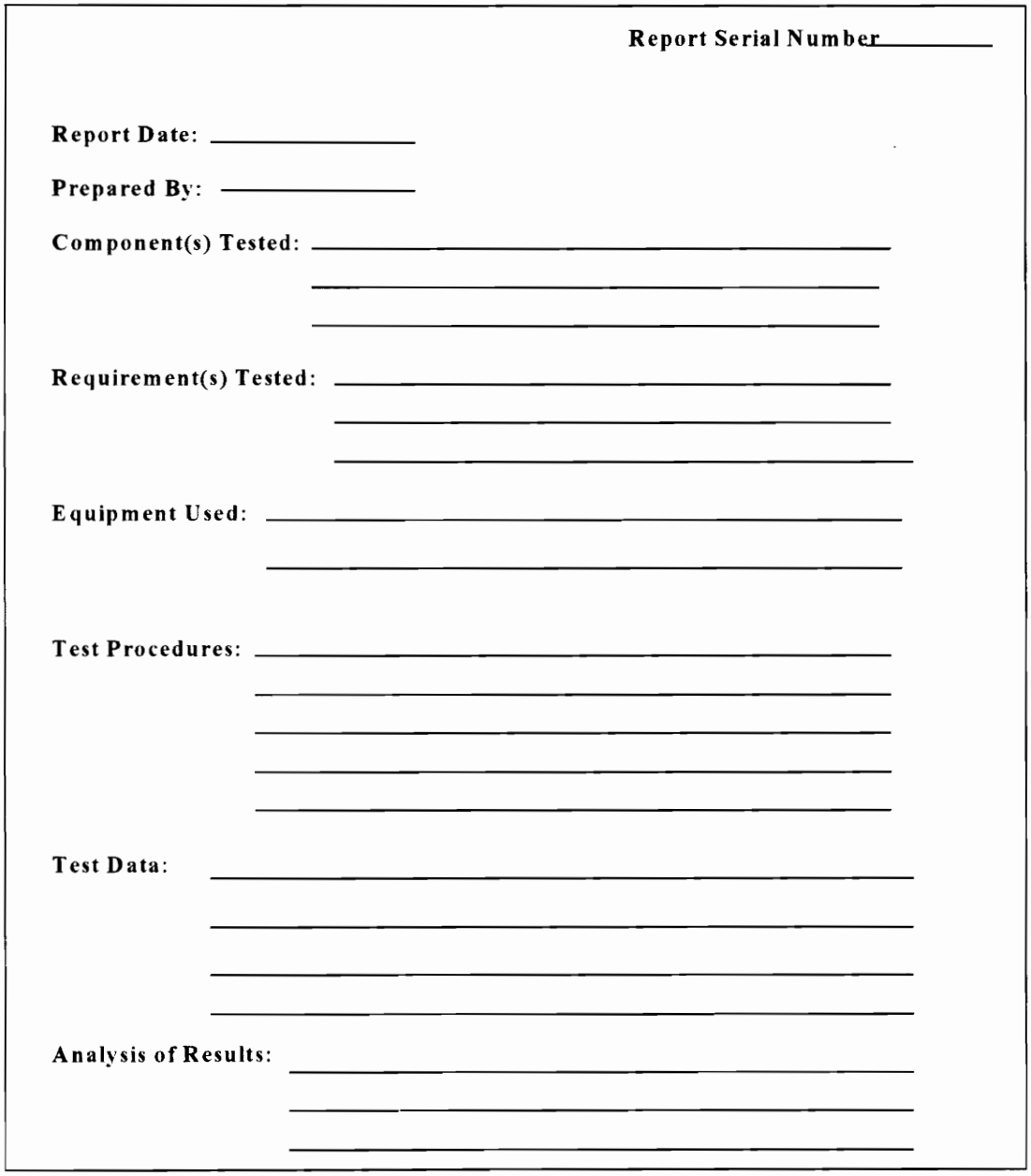


Figure 7-2: Sample Test Report Format.

8. Project Management Plan and Schedule

As mentioned throughout this report, AmeriClean will enlist the assistance of a telecommunications contractor to perform the systems engineering and integration for the network architecture project. This approach will enable to network architecture to be designed and implemented more quickly than if all work was performed in house, because the contractor's prior experience and knowledge can be leveraged in solving AmeriClean's communications needs. The AmeriClean systems administrator can take the opportunity to observe and assist the contractors in order to expand his knowledge and be better able to perform the on-going maintenance the system will require after the contractor's job is complete.

This section includes the plan for managing and executing the communications network enhancement project. Such a plan is important because is captures the expectations of the customer, AmeriClean, and the plans of the contractor. Through development of such a plan, both sides agree on the philosophy which will be used to manage the effort, and understand the context within which the technical tasks will be performed. Most importantly, a schedule is included which defines deadlines and milestones for all phases of the effort. Elements of this schedule may change over the life of the project, but the schedule provides a place for such changes to be captured, and for management to monitor the progress.

8.1 Management Approach

The network enhancements project team will focus on several key elements during the project life-cycle in order to ensure a quality project is completed within schedule and budget. These elements are:

- **Best qualified personnel -** The project will be staffed with engineers who are experienced in the field of high-technology telecommunications communications and computer networks. Additional areas of expertise include the systems engineering process, test and evaluation, and human factors and reliability engineering. All will meet minimum requirements for education and experience, and will demonstrate commitment to the success of the project.

- **Close tracking of project progress** - Project management will be responsible for tracking the progress of the system development at all stages of the life-cycle, without micro-managing the highly qualified technical staff. Procedures will be put in place to periodically review the design for accuracy and for compliance with requirements. In addition, cost and schedule of the project will be tracked using automated software systems, to ensure that all commitments to the AmeriClean customer are met while keeping the contractors' effort within budget.
- **Close contact with customers throughout the process** - A small team of volunteers from AmeriClean will meet regularly to serve as an advisory board on behalf of the system end users. Those selected should roughly meet the profile of the company as a whole, with a representative from each major department, possessing various levels of computer skills, and should be willing to review design and documentation periodically in order to provide a fresh perspective on the system as non-technical personnel.
- **Attention to details in design** - Throughout the product design process, close attention shall be paid to all details of the system design. Not only shall the technical aspects of integrating components manufactured by different vendors into a single system be addressed, but that system shall be designed to be easy to use and maintain, require infrequent maintenance, and grow with the company itself.
- **Thorough test and evaluation process** - A test plan shall be developed early which traces each operational and maintenance requirement to a procedure used to test that the requirement is met. The prototype system shall be thoroughly tested in each of these scenarios, and the results of the test documented. When the design is approved, AmeriClean management will observe the system operations, and accredit it as approved for operational use.

8.2 Design Team Organizational Structure

Since this is a short-term project, relying mainly on COTS integration rather than design and development of individual components, a small design team will be sufficient to meet the goals. Also, since the contractors will be selected for their experience in network design, a small group of about three engineers will be able to complete the project by each taking on multiple roles and responsibilities. The team shall consist of the following types of individuals in the following responsibilities:

- **Team Lead** - shall be the most senior and experienced member of the design team, possessing not only technical expertise, but the ability to analyze the system as a whole, and to communicate ideas to the other engineers and to the customer. He shall be responsible for the systems engineering lifecycle; performing the necessary analysis, trade studies, and recommending solutions for technical issues. She shall also track and manage the progress of the team, and shall be the liaison between the customer team and the contractors.
- **Network Engineer** - shall be responsible for the technical details of designing the communications network. This engineer shall have hands-on experience installing and configuring a variety of network components, in different configurations and manufactured by different vendors. She shall act as the technical expert in design reviews and presentations, She shall also be responsible for ensuring that elements of reliability, maintainability, and usability are designed into the system at all stages of the process. The network engineer will work closely with the team lead to ensure that all technical alternatives are assessed, and that the implementation fulfills the system requirements.
- **Accreditation Engineer** - shall be responsible for documenting the design and implementation of the system, and for writing and executing the system test plan. Since the contractors shall only be involved through the design and development phase without being present long into system operation and maintenance, it is critical that the system be well documented. All decisions should be captured and justified for later observers, and the configuration must

be explicit so that a different party is capable of making further system modifications and enhancements in the future. From the early stages of design, this engineer shall work closely with the project lead and network engineer to capture all user requirements, and to create the test procedures that will meet these requirements. By the time the implementation is complete, the AmeriClean management shall be able to review the system documentation and the results of the test, and can agree that their expectations have been fulfilled, and that the system is operational and secure.

- **General** - each team member shall be personally responsible for ensuring that the portions of the system within his or her control are designed to be easy for non-technical operators to use, and shall meet the maintenance and supportability goals of the project.

8.3 Technical Control

8.3.1 Project Reviews

Periodically, within the life-cycle of the AmeriClean network design, design reviews will be conducted by members of the design team, and presented to AmeriClean management, and to the user advisory board. Since the scope of the project is relatively small, these reviews shall focus on information flow between the customer and the contractor, and shall require as little preparation time as possible to not detract from the actual design and development efforts. The reviews shall consist of a presentation of briefing charts stating the objectives of the review, evidence that those objectives have been met, and a recommendation on whether the project should continue to progress toward the next milestone. The most important factor shall be that both parties are in agreement on technical issues. Several of the documentation deliverables due dates shall coincide with these formal reviews. The following reviews shall be performed within the project life-cycle:

- System Requirements Review (SRR)
- Preliminary Design Review (PDR)

- Critical Design Review (CDR)
- Operational Readiness Review (ORR)
- System Acceptance Review (SAR)

8.3.2 Documentation

All aspects of the product design shall be thoroughly documented in order that all people associated with the finished product shall be able to understand and use it to its maximum capability. This shall include the users, who must be able to operate the system in normal and unusual conditions, perform routine corrective maintenance, and understand the process for handling maintenance problems which are beyond the user level of expertise. System administration / maintenance personnel shall be provided with clear instructions for repairing or replacing components, and shall be extremely familiar with the process for handling multiple levels of maintenance. Any design team who shall be responsible for upgrading the network in the future or developing a follow-on system shall need access to the design documents and specifications. The following documents shall be created and maintained as a part of the AmeriClean product:

- Concept of Operations
- Maintenance Concept
- System Requirements Document
- System Design Document
- Test Plan / RVTM
- Test Results
- User's Manual / Standard Operating Procedures
- System Administrator Manual

The documentation shall be created and stored in both hard and soft copy. Hard copy documentation is easier to review and reference, but soft copy is easier to store, update or build on in the future. All documentation shall be reviewed for ease of understanding by the end user, and for accuracy and requirements traceability.

8.3.3 Companion Plans

Several additional documents shall be created to provide guidance on specific aspects of project management. Again, since this is a small project, these plans shall be tailored to provide critical information to AmeriClean management without an enormous amount of time on the part of the contractors. Content of these plans is significantly more important than format. These plans include:

- **CM Plan** - Document that details the procedures for maintaining and tracking various versions of project documentation and stages of design and test.
- **Risk Control Plan** - Continually updated document which lists all identified technical and management risks to successful project completion. Risks will be rated according to priority and potential impact to the project. Each risk shall have listed possible mitigation actions for means of lessening the impact of the risk if prevention is impossible.

8.4 Schedule Control

The AmeriClean network project's schedule shall be controlled by creating and storing a baseline project schedule in an automated project scheduling tool at project initiation. Maintenance of this schedule shall be the responsibility of the project lead, and shall be made relatively effortless by the automated software. Subsequent deviations in this schedule are captured in the automated scheduling tool as variations from the schedule baseline. The scheduling tool shall further track adherence to project schedule by performing critical path analysis, displaying schedule information in both Gantt chart and Pert chart formats, and resolving schedule and resource conflicts. The input dates for the baseline schedule are shown in Table 8-1.

Periodic status reports shall be created and provided to the AmeriClean management for review. These reports shall serve to keep management informed of schedule adherence and shall bring to attention any issues which appear to be turning into major project risks. These reports shall contain the most recent version of the project schedule, an updated risk assessment matrix, lists of open action items, lists of critical

issues and proposed solutions, as well as any other information that the design team feels would be relevant to management.

Table 8-1: Inputs to Project Schedule.

Activity	Start Date	End Date
Project Initiation	**1/1/96**	**1/1/96**
CM Plan	1/1/96	1/12/96
Risk Control Plan	1/1/96	1/12/96
Conceptual Design	1/1/96	3/1/96
Requirements Gathering	1/1/96	2/16/96
Concept of Operations	2/1/96	2/23/96
Maintenance Concept	2/1/96	2/23/96
SRR/Conceptual DR	**3/4/96**	**3/4/96**
System Requirements Document	2/16/96	3/4/96
Preliminary Design	3/5/96	3/27/96
Functional Analysis	3/5/96	3/18/96
Requirements Allocation	3/11/96	3/25/96
PDR	**4/1/96**	**4/1/96**
Test Plan / RVTM	2/1/96	6/28/96
Detail Design	4/2/96	5/31/96
Component Trade Studies	4/2/96	4/22/96
CDR	**5/31/96**	**5/31/96**
System Design Document	4/2/96	5/30/96
Installation & Integration	6/3/96	8/2/96
Procure Components	4/24/96	6/14/96
Configure Test Network	6/3/96	6/28/96
Testing	6/10/96	7/5/96
Integrate w/ Operational Network	7/8/96	7/19/96
Testing	7/15/96	7/26/96
ORR	**8/2/96**	**8/2/96**
Users' Manual	4/2/96	8/2/96
System Administrator's Manual	4/2/96	8/2/96

Test Results	8/2/96	8/2/96
Training	8/3/96	8/17/96
User Test Period	8/8/96	9/13/96
SAR	**9/20/96**	**9/20/96**
Operation & Maintenance	9/23/96	

9. Conclusions and Recommendations

The results of the detail design phase, along with the provided plans for project management and test and evaluation, place the AmeriClean Corporation well on the way to its goals of external communications connectivity. At this point it is possible to confirm that all of the user functional and operational requirements will be met by the completed system, and that the goals for reliability, maintainability, and cost will be met as well.

The network architecture design which will accomplish these goals is a combination of commercially available COTS products, integrated in a customized manner to meet the organization's requirements. Whenever possible, the components and functions of the existing isolated LAN are retained both for efficiency and cost savings, and for easing the users' transition to the new system. Two forces are balanced; the desire to provide access to services and to individuals across the Internet, and the desire to protect from unauthorized access the sensitive information stored on the network computers.

Several issues should be considered in the completion of the project and in the system's eventual operation and maintenance. AmeriClean should consider hiring additional technical support staff to perform administration of the system. The addition of the external connection has created greater requirement for scheduled and unscheduled maintenance, as well as the need for a significant amount of user training and technical support. Although the system design takes into account the size of the current technical staff, the point is soon reached where the additional capabilities become more than a single system administrator can comfortably manage.

AmeriClean should also make an effort to design a corporate strategy for combining its information system requirements with its business and growth goals. This project answers a short-term need for external communications connectivity, but does not go far enough in addressing the future of the company and the role it expects technology to play. When such goals are well-defined, AmeriClean and its consultants will be better able to balance such issues as cost versus capability in future system enhancements and support decisions.

Finally, AmeriClean management must show strong support for this project through all stages of implementation and use. A significant investment is being made in technological knowledge and equipment, and there is no guarantee that this investment will make the system successful. In order to truly succeed, the employees must be open to the changing environment and to learning the new skills and procedures required to achieve the most benefit of the system. This will take place most naturally, if the employees see the importance placed on the new system by their management, and if these leaders set a valuable example.

Finally, AmeriClean management must show strong support for this project through all stages of implementation and use. A significant investment is being made in technological knowledge and equipment, and there is no guarantee that this investment will make the system successful. In order to truly succeed, the employees must be open to the changing environment and to learning the new skills and procedures required to achieve the most benefit of the system. This will take place most naturally, if the employees see the importance placed on the new system by their management, and if these leaders set a valuable example.

10. Acronym List

CASE	Computer-Aided Software Engineering
CCITT	Consultative Committee on International Telegraphy and Telephony
CSMA/CD	Carrier Sense Multiple Access with Collision Detect
DMS	Defense Messaging System
DNS	Domain Name System
EC/EDI	Electronic Commerce/Electronic Data Interchange
e-mail	Electronic Mail
EGP	Exterior Gateway Protocol
EPA	Environmental Protection Agency
FSP	File Service Protocol
FTP	File Transfer Protocol
GGP	Gateway-to-Gateway Protocol
HTML	HyperText Markup Language
HTTP	HyperText Transfer Protocol
I&A	Identification and Authentication
IGP	Interior Gateway Protocol
ISP	Internet Service Provider
LAN	Local Area Network
Mb	Mega byte
Mct	Mean Corrective maintenance Time
MIME	Multipurpose Internet Mail Extensions
MS	Message Store
MTA	Mail Transfer Agent
MTBF	Mean Time Between Failure
MTBM	Mean Time Between Maintenance
MX	Mail eXchange
NIC	Network Information Center
OSHA	Occupational Safety and Health Association

OSPF	Open Shortest Path First
PC	Personal Computer
RIP	Routing Information Protocol
SMTP	Simple Mail Transfer Protocol
SNA	System Network Architecture
TCP/IP	Transmission Control Protocol / Internet Protocol
TFTP	Trivial File Transfer Protocol
UA	User Agent
UDP	User Datagram Protocol
URL	Uniform Resource Locator
WAN	Wide Area Network
WINS	Windows Internet Name Service
WWW	World Wide Web

11. References

Blanchard, Benjamin S., and Wolter J. Fabrycky. Systems Engineering and Analysis. Englewood Cliffs, NJ: Prentice Hall, 1990.

Carnahan, Lisa J, and John P. Wack. *Keeping Your Site Comfortably Secure: An Introduction to Internet Firewalls*. NIST Special Publication 800-10. US Department of Commerce, National Institute of Standards and Technology.

Chapman, D. Brent, and Elizabeth D. Zwicky. Building Internet Firewalls. Sebastopol, CA: O'Reilly & Associates, 1995.

Comer, Douglas E. Internetworking with TCP/IP Volume 1 - Principles, Porotocols, and Architecture. Englewood Cliffs, NJ: Prentice Hall, 1995.

Computer Shopper. April 1996: Vol 16 No 4 Issue 193.

Cooper, Fredric J.et al. Implementing Internet Security. Indianapolis, IN: New Riders Publishing, 1995.

Microsoft. Microsoft Windows NT Networking Guide. Redmond, WA: Microsoft Press, 1995.

Peterson, A. Padgett. *Firewall Security on the Internet*. Faulkner Information Services, 1995.

Stallings, William. Data and Computer Communications. New York: Macmillian Publishing Company, 1994.

The following corporate World Wide Web pages were used as reference:

- Cisco Corporation http://www.cisco.com
- PSINet http://www.psi.com
- Secure Computing Corporation http://www.sidewinder.com
- Trusted Information Systems http://www.tis.com
- UUNet http://www.uunet.com
- V-One Corporation http://www.v-one.com