

University of Virginia Network Failsafe and Disaster Recovery Plans

A Thesis
in TCC 402

Presented to

The Faculty of the
School of Engineering and Applied Science
University of Virginia

In Partial Fulfillment

of the Requirements for the Degree

Bachelor of Science in Computer Science

(Computer Networks)

by

Mike Newborn

March 23, 1998

On my honor as a University student, on this assignment I have neither given nor received unauthorized aid as defined by the Honor Guidelines for Papers in TCC Courses.

(Full signature)

Approved Mark Smith (Technical Advisor)
(Type Name) (Signature)

Approved Paul Sutter (TCC Advisor)
(Type Name) (Signature)

Preface

I would like to express my thanks to Mark Smith for all of his invaluable help on this project.

Table of Contents

PREFACE	I
TABLE OF CONTENTS	II
TABLE OF FIGURES	III
GLOSSARY OF TERMS.....	IV
EXECUTIVE SUMMARY OR ABSTRACT	V
CHAPTER 1: INTRODUCTION	1
CHAPTER 2: RESEARCH BACKGROUND INFORMATION.....	8
CHAPTER 3: THE DISASTER RECOVERY PLAN.....	18
CHAPTER 4: CONCLUSIONS.....	23
ANNOTATED BIBLIOGRAPHY	26
APPENDIX A: CONTACT NAMES, INFORMATION, AND ROLES	32
APPENDIX B: SERVICE PROFILES	35
APPENDIX C: MACHINE DETAILS	39
APPENDIX D: SELECTED RECOVERY COSTS AND INFORMATION	40
APPENDIX E: DISASTER RECOVERY RECOMMENDED INFORMATION SOURCES	41

Table of Figures

FIGURE 1: A STANDARD PHYSICAL NETWORK TOPOLOGY-----	1
FIGURE 2: AN FDDI LOGICAL RING TOPOLOGY-----	1
FIGURE 3: ESTIMATED REVENUE LOSS-----	19
FIGURE 4: NETWORK SYSTEMS ORGANIZATION CHART-----	21

Glossary of Terms

Asynchronous Transfer Mode (ATM) – A network protocol that can support transfer rates of up to 622 Mbps.

Backbone – The heart of a network. Most of the network converges to this point.

Coldsite – Computer-ready rooms, complete with wiring and raised floors (SunGuard Recovery Systems Inc.)

Disaster Recovery Plan – The ongoing process of creating, testing, and maintaining the policies and procedures an organization will follow should a disaster occur (SunGuard Recovery Systems Inc., 1995, p. 7).

Ethernet – A network protocol most commonly found at 10 Mbps and 100 Mbps.

Fiber Distributed Data Interface (FDDI) – A network protocol with a ring logical topology associated with it.

Hotsite – Pre-installed computers; raised flooring; air-conditioning; telecommunications equipment; networking equipment; technical support; and uninterruptible power supplies. (SunGuard Recovery Systems Inc.)

Mega Bits Per Second (Mbps) – A data transfer rate measurement of one thousand bits per second.

Mobile Recovery Units – Custom, preconfigured computer system; independent power source, office equipment,; technical support; and telecommunications equipment. (SunGuard Recovery Systems Inc.)

Network Logical Topology – The layout of a network from an internal perspective. (i.e. shows how the network components connect to each other)

Network Physical Topology – The layout of a network from an external perspective. (i.e. shows where cables are buried)

Network Interface Card (NIC) – A hardware device used for connecting a computer to a network.

Routing Protocol – The method a router uses to determine the path a data packet take in a computer network.

Router – A hardware device which moves packets from one subnet to another.

Protocol – A set of standards or a methodology.

Executive Summary or Abstract

The current, university-wide, disaster recovery plan does not incorporate the specifics of the Network Systems department. Due to the redesigning of the University of Virginia network, and the lack of detail pertaining to the Network Systems department in the current disaster recovery plan, there is a need for an updated disaster recovery plan. SunGard Recovery Services Inc. gives eleven comprehensive steps toward disaster recovery planning. In addition to logical topology, knowing the link characteristics of a network will help with disaster recovery plan development. When considering disaster recovery methodology at UVA, one should determine where to put network devices if a disaster occurs. The birth of disaster recovery and failsafe plans is a result of the dependence on computer networks. A disaster recovery plan can ensure network reliability. There is no set way to develop a disaster recovery plan. The manager acts as the central point for disaster recovery plan information. The critical applications and functions are the disaster recovery plan focus. It is important to append corrections to the original disaster recovery plan. Phase eleven, the final phase of developing a comprehensive disaster recovery plan, concerns maintenance. The disaster recovery manager is responsible for overseeing this phase. Disaster recovery can be minimized through disaster prevention. The financial justification for a disaster recovery plan is imperative. Many factors contribute to financial loss due to a network disaster. The disaster recovery plan that I developed is very preliminary.

Chapter 1: INTRODUCTION

I. Thesis Statement & Problem Definition

According to SunGuard Recovery Systems, a disaster recovery plan is “the ongoing process of creating, testing, and maintaining the policies and procedures an organization will follow should a disaster occur.” It is a contingency plan dealing with large disasters such as fires, floods, earthquakes, or power failures (SunGuard Recovery Systems Inc., 1995, p. 7). The primary goal of my thesis is to formulate a preliminary disaster recovery plan for a portion of the University of Virginia computer network.

The goal of a disaster recovery plan is to bring up the lost services as quickly as possible. A failsafe plan deals with smaller scale disasters and has a primary goal of not allowing an interruption in any provided network service. An example of a failsafe plan would be an online backup system in a computer network. The main difference between the two plans is that a disaster recovery plan would involve reconstructing an entire system, whereas a failsafe plan involves an alternative method that prevents service interruption. Since the two plans are so closely related, I will refer to both of them as disaster recovery plans.

I accomplished this project by working with the Network Systems division of Information Technology & Communication (ITC), specifically the Network Systems Manager, Mark Smith. The most difficult task in my project was detecting the limitations of the final disaster recovery and failsafe plans. Knowing that the plans are complete is the key to success. That is, knowing that my disaster recovery plan accounts for all vital services the university provides was essential.

An understanding of the physical topology and logical topology of the network is essential in formulating a good disaster recovery plan. Physical topology shows where cables are buried and components are located (ITCb, 1996). Figure 1 shows an example of a physical topology. This picture depicts a networking media known as fiber, a wire which uses light to transmit data, connecting routers that are located in Caruthers Hall. A router is a hardware device that moves data packets from one network to another.

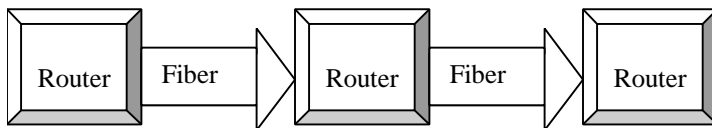


Figure 1. A standard physical network topology.

Logical topology shows how the network components connect to each other. In essence, logical topology shows what protocol or method of data transmission a network uses. For example, Figure 2 is a Fiber Distributed Data Interface (FDDI), a network protocol which has a ring topology associated with it.

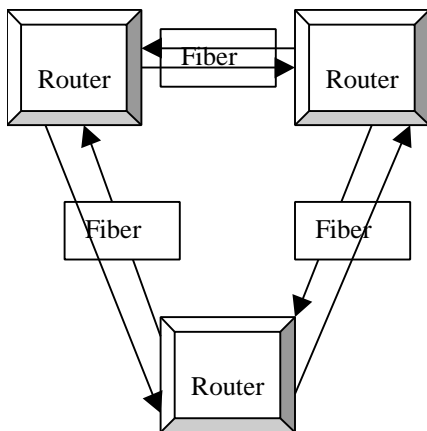


Figure 2. An FDDI logical ring topology.

A network's physical topology demonstrates the way a person would view the layout of a network, whereas logical topology shows the view from the network components standpoint.

From the physical topology perspective, I obtained an inventory of the services that the UVA network supports. This allowed me to single out vital network components and give them the highest level of redundancy. An inventory of both active and spare equipment was also necessary in formulating the plan. This information allowed me to determine what we had as a backup, in case a device failed.

From the logical topology perspective, I obtained information on the current and upcoming backbone of the network and the current routing protocols. One can view the backbone as the heart of a network. The current backbone is FDDI, but the new one will be Asynchronous Transfer Mode (ATM). The change in protocol will provide a maximum speed change from 100 Mega bits per second (Mbps) to 622 Mbps. These network changes require the redesigning of a large portion on the network.

The current university-wide disaster recovery plan does not incorporate the specifics of the Network Systems department. Due to the redesigning of the University of Virginia network, and the lack of detail pertaining to the Network Systems department in the current disaster recovery plan, there is a need for an updated disaster recovery plan.

Another problem the Network Systems department is facing concerns the choice of routing protocols. Routing protocols determine the path that a data packet takes in a network. For example, if there are five different paths to get to a mail server, how a network should send the data packet is a decision made by a routing protocol. An older inferior network is used as a backup in case of mainstream network failure. The routing protocol is responsible for bringing the backup system online if necessary. However, the current protocol choice, Routing Information Protocol, does this inefficiently. To address this problem I am investigating the following routing protocols: Routing Information

Protocol (RIP), Interior Gateway Routing Protocol (IGRP), and Enhanced Interior Gateway Routing Protocol (EIGRP).

II. Literature Review

Today when people think of disasters that could disrupt their lives, they think of natural disasters such as tornadoes, hurricanes, floods, and earthquakes. However, a disaster is not limited to natural types. In fact, a business disaster is “any unplanned, extended loss of critical business applications due to lack of computer processing capabilities for more than a 48-hour period” (SunGard Recovery Services Inc., 1995, p.5). The four most likely disasters are power outage, flooding, fire, and computer hacking (Patterson, 1997, Personal Interview). Disasters can be very costly. A quick evaluation of services can yield estimates of the potential damage a disaster may cause. Payroll, sales, billing, inventory, and production control are just a few of the potential services that may be lost during a disaster.

SunGard Recovery Services Inc. gives eleven comprehensive steps toward disaster recovery planning. They consist of the following: organize team, select disaster recovery manager, identify tasks, develop organization chart for disaster procedures, match personnel to team skills, identify critical applications, develop applications profiles, create procedures, develop resource documentation strategy, test, and maintain plan. I used these steps as a guideline in developing my preliminary disaster recovery plan.

When planning for disaster recovery it is important to become familiar with the logical topology of the specific network. The logical UVA topology is as follows. The primary backbone that UVA had is single-mode FDDI. In Carruthers Hall are the links to

the Internet and VERNet. The West Grounds consists of a multi-mode FDDI ring that connects to the main backbone in Gilmer Hall. In addition, the Medical Center multi-mode FDDI ring covers the non-academic portions of the Health Sciences Center.

Ethernet is the most commonly used media at UVA (ITCb, 1997, Map).

In addition to logical topology, knowing the link characteristics of a network will help facilitate disaster recovery plan development. The network at UVA has the following link characteristics: 6 Mbps backup line to Sprint Link for Internet access, a 155 Mbps link to Net.Work.Virginia. Off of the Net.Work.Virginia link there is a 45 Mbps link to the Internet, a 45 Mbps link to ESNNet (The Department of Energy Research), and lastly a 155 Mbps link to VBNS (Internet 2) (ITC Network, 1997, Map).

When considering disaster recovery methodology at UVA, one should determine where to put network devices if a disaster occurs. It is also important to find out if backup systems are necessary. If so, what are the functions of the backup systems, and which machines will they backup. Another approach is to define the purpose of each device in the list that encompasses the recovery plan. An excellent place to find security and disaster network related information is <http://www.sans.org> (Patterson, 1997, Personal Interview).

It will also be necessary to take into consideration other aspects of the network system at UVA. The designer must take into account the anticipated down times if a building's network services fail. How does one know if a disaster recovery plan is complete? Consider the following services in the design: dialin access, Pcmail, general mail service, mail gateway service, electronic news, user database (whois), primary Unix machine access, mainframe access, core NetWare servers, calendar service, help desk

network, computerized class rooms, and Internet access (Smith, 1997, Personal Interview).

III. Rationale and Scope

The world that we live in is undergoing technological change at a rapid pace. Historically, one of the facilitators of rapid growth in organizations involved some sort of a network. Whether it is a network of people, machines, or ideas, networks play an important part in the growth of any organization. Computer networks represent some of most recent technological achievements.

As the integration of computer networks occurs, the need to take care of and maintain them becomes more apparent. Society becomes more interconnected, and the thought of a network failing or crashing can be detrimental, or even fatal. The birth of disaster recovery and failsafe plans is a result of this dependence on computer networks.

IV. Brief Impact Summary

There are many social and cultural impacts that result from networks. Our society makes extensive use of networks in its everyday operation. The farther we advance in technology increases our dependency on networks. Consequently, the destruction of a network or vital network component becomes a major threat, making the need for network reliability a top priority. A disaster recovery plan can ensure this network reliability.

Some adverse impacts of networking and disaster recovery planning include: loss of human contact, the development of dependence, and a false sense of security. Some beneficial impacts of networking and disaster recovery planning include: increase in productivity, faster communications, and the ability to ensure reliability.

V. *Overview of Contents of Rest of Report*

In the rest of this report, my goal is to provide information on the following subject matters:

- The development of a general disaster recovery plan
- Understanding the routing protocols RIP, IGRP, EIGRP as they relate to the current problem with the Network Systems department.
- Determining which routing protocol(s) will work best for the Network Systems group at UVA.
- Developing a preliminary disaster recovery plan for the Network Systems group.

Chapter 2: RESEARCH BACKGROUND INFORMATION

I. Disaster Recovery Methodologies

There is no set way to develop a disaster recovery plan. Every situation requires a slightly different approach. In general there are certain guidelines or phases that should be followed and tailored to each specific situation. In the following section I will present a phase by phase breakdown of a general disaster recovery plan. The phase names are taken from SunGuard Recovery Systems Inc., however their definitions have been modified.

The first or initial phase is the justification of implementing a disaster recovery plan. This will vary from situation, but it usually involves some background research concerning the organization. The plan can be a costly task and organizations may not be willing to jump directly into the planning process. Finding out an organization's revenue and evaluating revenue dependence on the computer network will be essential. Showing a significant organizational dependence on a computer network will also help persuade managers. The objective of this phase is to show that loss of a computer network will incur more damage than the cost of having a disaster recovery plan.

Proving the financial gain of having a disaster recovery plan does not stop with the specifics of a particular organization. There are plenty of case histories out there to justify having a plan. For example, "a study estimated that within the first ten days of a disaster a company can lose two percent to three percent of its annual sales... Fifty percent of the companies that lose critical business systems for ten or more days never recover... Finally, ninety-three percent of companies without a disaster recovery plan in place were out of business five years later" (Louderback, p. 130). Another study of over

800 PC users showed only about one-third of the participants were connected to a network that was fully protected which left two-thirds of the corporate PCs exposed. This study was verified by Comdisco Disaster Recovery Services of Roesmont, IL by conducting similar studies yielding confirming results. Comdisco found that “although management is highly cognizant of the importance of disaster recovery for data centers, networks receive only about ten percent of disaster-recovery budgets” (Brown, p. 25). A discussion of recent disasters relating to similar companies may prove invaluable toward getting the plan’s finances approved. In the Chicago Flood of 1992, Hurricane Andrew, and the World Trade Center Explosion many companies lost their networks and suffered multimillion-dollar losses. However, “companies with disaster recovery plans such as Credit Agricole, John Alden Life, Northern Trust, and Transamerica Commercial Finance escaped these disasters relatively unscathed” (Brown, p. 25).

Obtaining specific numbers as to how costly a disaster could potentially be is a tricky process. An overwhelming number of factors affect the final numbers. The recommended approach is to list all relevant factors that contribute to revenue loss due to a disaster. On several occasions I have found organizations make claims that employees are at a certain level of capacity with the loss of their computer network. In a presentation one might compute out the total hourly revenue each employee brings in and make the claim that without a computer network the average employee is at fifty percent capacity. If this percentage is too specific, then listing several percentage levels may prove more useful. A hypothetical example of this method would be the following: Let’s say we have company XYZ that has 200 employees and brings in a revenue amount of one dollar a minute per employee. One day a disaster occurs and the network is down for

one workday, which is equivalent to eight work hours. If the employees are at a fifty-percent capacity, then they are losing four hours of work. Turning these numbers into a dollar amount we take sixty minutes multiplied by four hours multiplied by 200 employees multiplied by one dollar a minute and we come up with \$48,000. After a disaster that took down the network for one day, the net result is a loss of \$48,000. The numbers can be overwhelming and play a large role in winning over a higher budget.

After budget approval, one can move onto phase two of the planning process. Team organization is the goal of this phase. Taking individuals who are familiar with the normal operations of their departments is the recommend approach. The responsibility of these individuals will become more apparent as the disaster recovery planning process goes on, however each individual will be responsible for the recovery of their department. It is important to have at least one person from each department that the disaster recovery plan will cover on the team. The next step is the selection of a disaster recovery manager. This person will be responsible for organizing the entire plan. It is their job to keep the plan up-to-date and be familiar with the plan inside and out. The manager acts as the central point for disaster recovery plan information. If a disaster occurs, regardless of the departments involved, the manager receives notification. The disaster recovery manager assumes a large role and is committed to the success of the project.

The goal of phase three is to identify tasks. Any task that the organization provides should be acknowledged. This is sort of a brainstorming phase and the separation of critical tasks from non-critical ones will occur in a later phase. Having a diverse disaster recovery team will prove to be very helpful for this phase.

Phase four involves the development of an organizational chart for disaster procedures. The purpose of the chart is to show the designation of responsibility in the organization. The chart lists the tasks that should be undertaken in a disastrous situation. The organization chart should include contact numbers and other staff information (i.e. land-line, cellular, pagers, etc.). It can be used as a quick contact reference in an emergency situation.

The organization chart can help with phase five of the disaster planning process. The goal of phase five is to match personnel to team skills and functions. By the end of this phase, a detailed list of personnel with corresponding tasks will be constructed. It is the responsibility of each member of the disaster recovery team to organize the proper number of personnel to ensure that a function remains intact. It is a good idea to have backup personnel in case some personnel are not reachable.

In the sixth phase it is necessary to identify critical applications and functions. The critical applications and functions are the disaster recovery plan focus. For example, company XYZ may offer a service that does payroll and a service that allows an employee to print to a network printer. If each employee in XYZ has a local printer, then the ability to print to a network printer becomes a non-critical service. On the other hand, payroll is a critical service and our disaster recovery plan will act more cost effectively if we concentrate on the payroll service. Distinguishing between a critical and non-critical service is a result of the sixth phase. Of course just because a function or service is not a focus in the disaster recovery plan does not mean it cannot be included.

The seventh phase builds on the sixth phase. The goal is to develop application profiles and to develop function profiles. The applications and functions identified as

critical are documented. Any specific information that one would need to recreate the application or function should be listed. This may involve any of the following: backing up data, keeping a record of hardware and software setup, keeping a record of “facility and equipment layout, connection devices (routers and so forth), server attributes, and general information on network topologies and protocols” (Phillips, p. 18). The specific computer equipment information, such as CPU, memory, Network Interface Card (NIC) type, hard-disk size, and network operations system version for each server should be recorded. It will also be important to note the maximum acceptable down time of each application or function.

The creation of procedures is the goal of phase eight in the disaster recovery plan. The procedures should specify what order to bring up the critical applications and critical functions. The procedures will vary from situation to situation, but in any case they should give detailed instructions. Since there are a variety of types of disasters that might occur, the procedures need to be flexible. One might consider hotsites, a site with preinstalled computer equipment, mobile recovery units, a custom preconfigured computer system, or coldsites, computer-ready rooms without the equipment. If software or equipment needs to be replaced, the vendor contact information should be available. One should remember that no disaster recovery plan is bulletproof, but you can make it close to bulletproof with a comprehensive set of procedures.

The goal of phase nine of the plan is to develop a resource and documentation strategy. This is where the entire plan comes together. All the different phase information should be constructed in some easy to understand way. Spreadsheets and organizational charts may facilitate the fast lookup of information. Specialized

procedures should be categorized based on the applications and functions they describe.

Always make sure there is a copy of the disaster recovery documentation close by.

People on the disaster recovery team are responsible for their department or area.

Although every phase is important in a comprehensive disaster recovery plan, the last two are extremely important. The goal of phase ten is to test and train. Although testing can be time consuming, and is often neglected, it makes the difference between having a booklet of papers and an actual disaster recovery plan. The training of all individuals involved in the disaster recovery plan is key to its success. There are many ways to go about testing the plan, but the most important part is that you find out if the disaster plan actually works. Testing includes a structured walk through, checklist test, remote test, communications test, full system hotsite test, critical applications hotsite test, and a mock disaster test (SunGard Recovery Services Inc., 1995, p.45).

After testing your plan, you may find that it needs some fine-tuning. It is important to append corrections to the original disaster recovery plan. Testing is useless if the results are not utilized. After making plan changes, more testing may be necessary. The plan should now be comprehensive, however it will not stay that way unless it is maintained.

Phase eleven, the final phase of developing a comprehensive disaster recovery plan, is maintenance. Technology and organization are constantly changing and the plan needs to change with them. The disaster recovery manager is responsible for overseeing this phase. Periodic tests may be necessary to make sure the plan still works. When making changes to a plan, updating anyone involved in the recovery process is

imperative. Maintaining and testing will play an essential role in keeping an organization protected

Disaster recovery can be minimized through disaster prevention. There is no way to completely prevent a disaster from striking, however one can have best practices that minimize the effect of a strike. The following is a list of recommended best practices that an organization should follow to ensure full disaster protection:

- Keep disaster recovery plan up-to-date.
- Keep personnel up-to-date on the recovery plan.
- Periodic testing of the disaster recovery plan.
- Priority of recovery must be agreed upon before a disaster occurs. The situation will be dynamic enough already.
- Make sure employees and users of equipment are properly trained.
- It is important to have at least one geographically separate data center. Avoid keeping too many applications and functions in one area.
- It is advisable to have at least two physically separate feeds into a data center, with each one connected to a different side of a carrier's ring.
- Keep hardware components that commonly fail in abundant supply. (i.e. disk drives, power supplies, NIC, and memory).
- Keep current backups of client configurations.
- Keep systems as simple to use as possible, error checking to ensure data has been entered is a plus, and take regular backups.
- If databases are used replication of the database is key to success.
- Star network topologies improve chances of recoverable infrastructure.
- Keep vendor information, Internet provider information, and WAN connectivity provider information on hand.
- Keep backup tapes offsite.
- Periodically check all backup tapes to make sure the data is backed up properly.
- Keep a record of hardware and software setups in hardware, including tape drive model and version of backup software.
- Limit the number of ports in a network and access to them.
- Good password management is important.
- Here are a few potential vulnerable points in a network: a single conduit to central offices, single central offices, a single long-distance carrier, a single CPU, a single building entry point, a single power source, and a single internetworking device.
- Look out for contractor's backhoe which could potentially cut both links simultaneously, separate routes are required to guard against its threat.

- Diversify the carriers you use and the routes that your circuits will take. Make sure the circuits do not run over the same route or through the same conduit.

II. Depth Into Routing Protocols

A routing protocol is the methodology by which a routing device decides of how to send a data packet. I examined three types of routing protocols RIP, IGRP, and EIGRP. Here at the University of Virginia there is a problem involving network protocols. RIP is the current network routing protocol. There is a failsafe network that connects to routers in case the mainstream network fails. The failsafe network is there for the purpose of a backup networking system and is not to be used when the mainstream networking system is operational. In fact, the failsafe network is a slower and less reliable network. Unfortunately, when both networks are connected, routers often send data over the failsafe network despite the operational status of the mainstream network. The reason for this is the metric that RIP bases its routing decisions on tells the router to send data over this failsafe network. In order to prevent this inefficient routing of data, the failsafe network must be kept offline and must be manually put online in case of mainstream network failure. This allows for a window of downtime that UVA wants to avoid. Therefore, in the following section I will discuss the benefits and pitfalls of each protocol as it relates to the routing problem here at UVA.

RIP is useful for routing within small to moderate sized homogeneous internetworks. In this protocol, the factor by which a packet is routed is the number of hops. Every time a packet hits a router, the hop count increases by one. RIP permits a maximum hop count of fifteen. This means that any destination, which is larger than fifteen hops away, is unreachable. Due to this constraint, RIP is very restricted in large

internetworks. However, this prevents the counting to infinity problem. The counting to infinity problem results in a packet going in an infinite routing loop, and by limiting the number of allowed hops the loop ends after a packet goes sixteen hops.

IGRP uses a combination of metrics to make its routing decision. Bandwidth, load, internetwork delay, and reliability are all factors in the decision. This makes IGRP a very customizable protocol. Reliability and load can take on any value between 1 and 255. Bandwidth can take on speed values from 1200 bits per second bps to 10 gigabits per second. Finally internetwork delay can take on any value from 1 to 2 to the 24th power. IGRP also permits multipath routing. This allows two lines to run a single traffic stream in a round-robin fashion with an automatic switchover to the second line if one line goes down.

EIGRP has all the features of IGRP and more. It is Cisco's version of IGRP. As it relates to UVA, it adds routing support for AppleTalk, IP and Novell NetWare data packets. EIGRP also uses less bandwidth and therefore incurs less overhead than IGRP and RIP. The only disadvantage is that one must have a Cisco product to use all these features.

EIGRP would appear to be the best choice for a routing protocol here at UVA. Fortunately, most of the routers here are Cisco products making the implementation of EIGRP rather easy. EIGRP would solve the problem of having a failsafe network that must be kept offline. This is because EIGRP uses many factors to route data packets whereas RIP uses only the number of hops.

It is important to note that with the new ATM network backbone the older FDDI backbone can be used as a failsafe backup system. By selecting EIGRP as the new

network routing protocol, the older FDDI system can be automatically switched online in case of ATM failure. If failure of both ATM and FDDI occurs, a coaxial cable version of Ethernet can take on the role of a failsafe system.

Chapter 3: THE DISASTER RECOVERY PLAN

I. Data Collection

I used a number of different methods to collect data for this project. I conducted various interviews, both in person and over the telephone. I searched case studies, books, articles, the World Wide Web, software programs, and CD-ROMs. Most of the specifics of the Network Systems Department came from Mark Smith, the Manager.

II. Process of Developing a Preliminary Plan for the Network Systems Department

I decided to go with the multiphase approach to develop the disaster recovery plan. Since I am not part of the Network Systems Department, obtaining the specifics personally was a difficult task. When I needed this type of information I relayed it to Mr. Smith who, in turn, retrieved the information for me.

In developing the preliminary disaster recovery plan for the Network Systems department, the team for developing the disaster recovery plan consisted of Mr. Smith and me. Fortunately, Smith is very knowledgeable in his department and I was able to use this benefit in the development process. It was decided that Mark Smith would be the disaster recovery manager and Jim Jokl, the Director of Communications & Systems, would be the backup disaster recovery manager. In the case of a disaster, they would among the first contacts.

The financial justification for a disaster recovery plan is imperative. In order to justify the plan for the Network Systems department, we came up with a few rough estimates. Figure 3 reflects the calculations and their results. Many factors contribute to financial loss due to a network disaster. These are extremely difficult to quantify. Depending on the time of failure, the weight of any of the factors may change. For

example, during grade and registration deadlines loss of network may have more of an impact on students and faculty. Loss of network services during grant deadlines, which occur throughout the year, may be responsible for loss of a grant. Research results are usually due at the end of a month, and loss of network services may be responsible for loss of publication. Poor network stability could result in a damaged school reputation. There are also legal issues to consider. For example, a student who cannot send their thesis to a graduate school due to loss of printing services, may miss the deadline and bring legal action on the university. This list goes on and on, however, obtaining dollar amounts is very speculative. The calculations in Figure 3 were computed based on the annual university income and a speculative capacity of the network customers. The estimated capacities of individuals without the use of network services were computed at seventy-five, fifty, and twenty-five percent capacity. Last year the total university revenue was about \$1 billion dollars (University of Virginia, WWW).

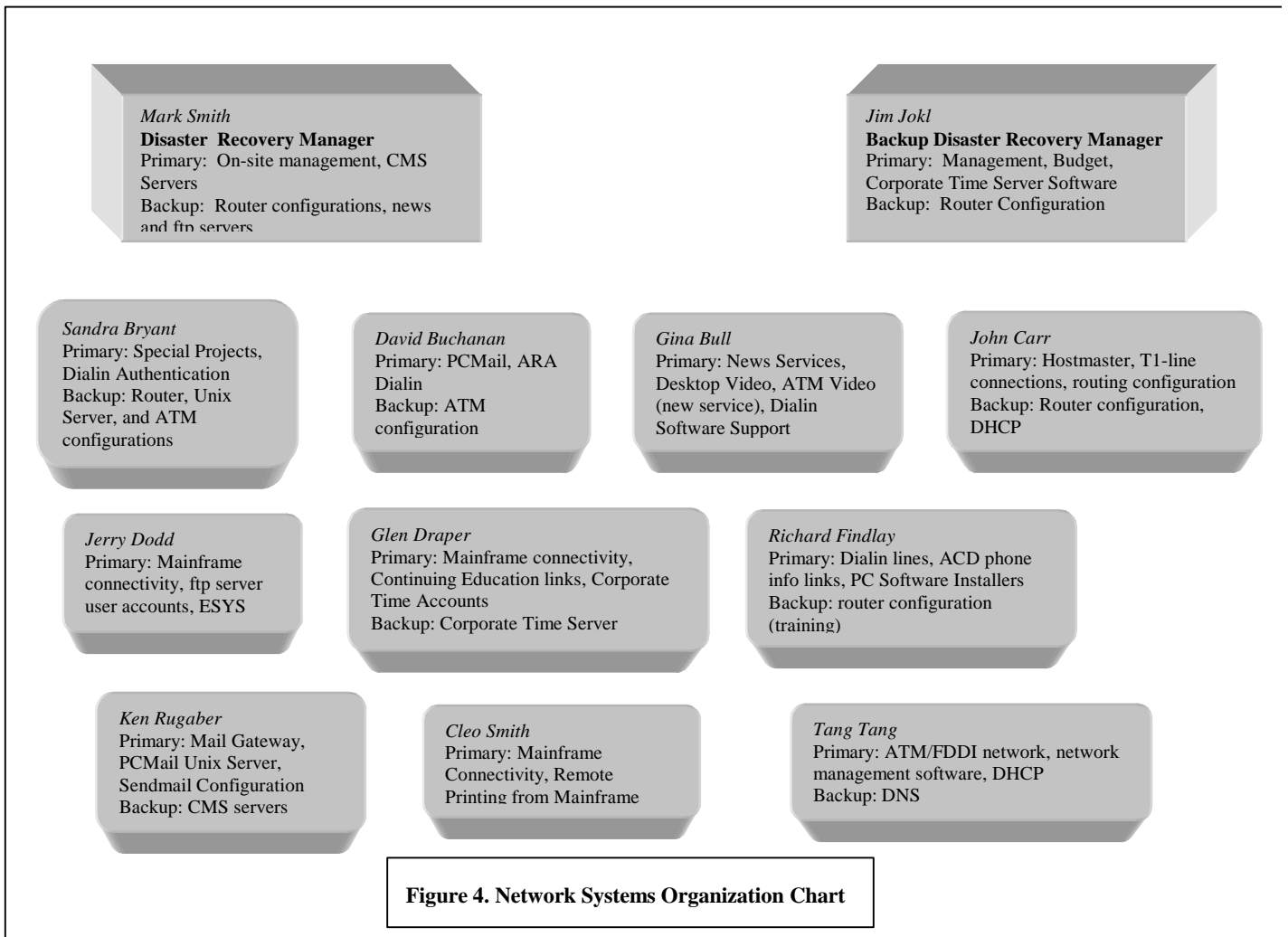
University Capacity without a network	Calculations for hourly loss of revenue [Yearly Total Revenue / 2080 work hours per year]	Revenue loss after 1 hour	Revenue loss after 1 day	Revenue loss after 1 week
75%	.25(\$1 billion/2080 hrs)	\$120,192	\$961,536	\$4,807,680
50%	.50(\$1 billion/2080 hrs)	\$240,384	\$1,923,072	\$9,615,360
25%	.75(\$1 billion/2080 hrs)	\$360,576	\$2,884,608	\$14,423,040

Figure 3: Estimated Revenue Loss

Mark and I brainstormed the different tasks that the Network Systems Department provides. This is what we came up with:

- Dialin Access 28.8 1-hr
- Dialin Access 28.8 30-min
- Dialin Access 28.8 15-min
- Dialin Access 28.8 department
- Dialin Access 14.4 1-hr
- Dialin Access 14.4 30-min
- Dialin Access ARA
- Dialin authentication
- PCMail
- Central Mail Service (IMAP/IMSP)
- Central Mail Service (IMAP ONLY)
- Mail Gateway Service (includes Majordomo)
- Electronic News
- User Database (Whois)
- Primary Unix Machine Access
- Mainframe Access
- Network path to Core Netware Servers, ACCPUBLIC, Labs + Classrooms, Dorms
- Calendar Service
- Help Desk Network
- Computerized Class Rooms Network Access
- Internet Access
- Routing Protocols
- DNS
- Mass Store Archive MAGGIE Access (SPECIAL CASE)
- Building Level Access
- DHCP

After we determined the tasks, we began to develop an organizational chart. Figure 4 shows this organizational chart.



This chart also demonstrates the match of personnel with their services (see Appendix A).

It was determined that all the services were critical and needed to be included in the disaster recovery plan. Next, a profile was developed for each of the services. We included fields that we felt were appropriate in developing each profile. These fields include: service, priority, primary machine name, primary machine location, backup machine name, operational state of service with backup, data or tape location, and additional comments (see Appendix B). In addition to these fields, we created a separate profile for each machine that played a role in providing the services (see Appendix C). The fields for a machine profile include: machine name, machine location, model, memory, disk space, serial number, vendor, additional information, and alternate supplier.

Due to time constraints, the procedures and documentation strategy were not completed. However, the procedures essentially consist of replacing the hardware and retrieving their configurations from backup. The Network Systems department currently backs up all configurations making this task painless. In the event that a backup configuration is not available, the time to recover will significantly increase.

The collected disaster recovery plan information is located in the Appendices in the form of spreadsheets. In the future, after the procedures can be explicitly defined, the spreadsheet information should be organized with the procedures in a more formalized manner.

Chapter 4: CONCLUSIONS

I. Summary

Although many sources claim a similar methodology for creating a disaster recovery plan, the plan must be heavily customized to the specifics of an organization. This may involve disregarding or combining multiple disaster recovery development phases. Development of such a plan requires access to a large knowledge base. One must have access to a network topology, services, administration, and users. Access to these resources yields a wealth of information that is useful in disaster recovery plan development. The success of a plan depends on its readability just as much as its comprehensiveness. An outdated or inaccurate disaster recovery plan can be more costly than not having one at all. Therefore, it is extremely important that a plan continues to be tested and maintained.

II. Interpretation

The preliminary disaster recovery plan that I developed is very preliminary. The next two phases, creating procedures and developing documentation strategy, require a significant amount of time to accomplish. When creating procedures, it may be necessary to meet with each of the individuals listed in the organizational chart (see Figure 4). The objective is to take each task one by one and evaluate procedures for bringing them back up in the case of failure. To facilitate this process surveys can be distributed before scheduled interviews with personnel.

When documenting the material and formalizing the disaster recovery plan the use of flow charts will greatly increase its readability. The document should start out with some sort of index giving easy access to any specific task procedure. The document should also contain disaster recovery plan maintenance and testing schedules. This allows for an easier evaluation as to whether the plan requires updating.

Based on the information already collected, the development of a finalized disaster recovery is well on its way. Most of the collected information can be found in the appendices of this report. I believe the tasks selected to be covered in the disaster recovery plan are comprehensive for the Network Systems department. However, at this stage in the plan the addition of tasks should be a safe process. Once the plan is fully functional, it can be integrated with the university-wide disaster recovery plan.

I chose not to include a large amount of Network Systems specific information in the main body of the report because I did not want the reader to get involved in the plan details. This project should be used as a guideline for developing future disaster recovery plans. However, the appendices show the amount of information collected and can be used as examples for the different phases in disaster recovery plan development.

III. Recommendations

Through my research and findings concerning the Network Systems department and the university network as a whole, I have found some potential problems with current network procedures and parts of the current network layout. I highly recommend the implementation of a disaster recovery plan as soon as possible for the Network Systems department as well as all departments of the university. I also encourage the maintenance and testing of the university-wide disaster recovery plan.

There appears to be a rather large congregation of computer network resources in Caruthers Hall, VL, and Gilmer. If a disaster were to strike any of these areas, and take down the entire building, the results would be horrendous. Most backup systems are located in the Caruthers Hall building. Consequently, if a disaster were to corrupt these systems recovering critical information would be severely hindered. Reevaluation of the university-wide topology should confirm these findings.

Another problem is with the offsite backups of the mail servers. Backups are taken off site every two to three weeks. Because the general recovery procedures require this backed up data, there is a large window open for disaster damage.

Lastly, I believe it is important to note that there is no way to completely prevent a disaster from occurring. We can only strive to minimize the potentially hazardous results. However by following the best practices mentioned earlier one can insure maximum protection against a disaster.

Annotated Bibliography

I. Disaster Recovery Information

Baseline Software. (1997). Information Security Policies Made Easy Reference Manual (Ver. 6). Sausalito, CA: Wood.

This manual provides an in depth report on security policies. It is broken down by topics.

Baxtor, Les A., Masood A. Shariff. "Steps Toward Successful Disaster Recovery." Telecommunications March 1995: 61-63.

Gives information as to what to consider in disaster recovery plan.

Brickates, Evanthia V. "Taking No Chances." Network World 20 Oct. 1997: 1-4.

Discusses failsafe networking implementations. Gives various real like examples and explains consequences of these example networks failing.

Brown, Richard O. "What You Need to Know to Plan for Disaster." Networking Management April 1993: 25-27.

General disaster recovery techniques and examples of real disasters.

Buehler, Steve. "The Sky is Falling." PC Magazine 22 Oct. 1996: NE30-NE31

Consequences of not planning for a disaster. Recommends information sources and consulting firms.

Chernicoff, David P. "Planning to Fail: How to Sidestep Disaster." PC Week 21 Aug. 1995: N1-N3

Article discusses data-backup techniques.

Cotton, Dirk. "Don't blame lady luck when backup plans fail." Data Communications 15 Oct. 1990: 29-30.

Discusses several disaster recovery strategies upon which telecommunications managers can rely to protect their data transmission networks.

Disaster Recovery Services Inc. (1995). DR2000 for Windows Reference Manual.

This reference manual provides questions that should be asked when developing a disaster recovery plan. It lists the format of an example disaster recovery system which I use as a guide in developing my own.

DR2000 for Windows [Computer Software]. (1995). Disaster Recovery Services Inc.

The purpose of this program is to formulate a complete disaster recovery system. The user enters answers to various questions concerning the current situation, and in turn the program cranks out a disaster recovery plan.

Dryden, Patrick. "Automated Service Diagnoses Nets." Computerworld 26 Jan. 1998: 49-51.

This article gives information on NetOps Corp. a disaster recovery consulting company.

Eastwood, Alison. "End-users: The Enemy Within?" Computing Canada 4 Jan. 1995: 41-42.

Discusses LAN security issues and employee related problems.

Effgen, K. F. "Presenting the Business Case for a Network-Based Disaster Recovery Planning Program." Telecommunications 26 Nov. 1992: 28-31.

Discusses the funding issues of initially building a disaster recovery plan.

Fritz, Jeffrey. "Bulletproofing ATM: Part 1." Byte June 1997: 59-61.

Talks about designing techniques with ATM networks.

Hall, Jeff. "Adventures in Data Replication." Network Computing 1 March 1995: 134-138.

Database replication and its importance in redundancy.

Hunter, Phil. "Traffic Control." Computer Weekly 13 March 1997: 52-53

Talks about computer tools which aid in plan design.

Lawrence, Bill. "NetWare Mirror with a Twist" Byte March 1996: 103-105.

Specific redundancy information concerning NetWare.

Louderback, Jim. "Will You Be Ready When Disaster Strikes?" PC Week 6 Feb 1995: 130-131.

Gives examples of disasters and encourages back-up planning.

Name, Mark L. Van, Bill Catchings. "When Backups Can't Get Systems Backup Up."

PC Week 29 April 1996: N8-N9.

Describes best practices when backing up data. Discusses possible solutions to loss of backup situations.

Patterson, Richard A. "Clinch Valley College Audit Points." E-mail to Clinch Valley College. 30 Sept. 1997.

The email describes basic disaster recovery techniques. It advises Clinch Valley on how to comply with Virginia's security standards.

Phillips, Ken. "AIM/LAN 2000 1.1 Masters Disasters with a Comprehensive Recovery Plan." PC Week 22 May 1995: 18-19.

Talks about a consulting firm that helps develop a comprehensive recovery plan.

Romano, Catherine. "Is Your Business Protected?" Management Review Aug. 1995: 43-45.

An article encouraging disaster recovery plans and attempting to justify them.

Strauss, Paul, Tom McCusker. "Disaster Proofing? Don't Forget the WAN." Datamation 1 July 1994: 48-50.

Gives suggestions as to how to create a disaster recovery plan for WAN's.

Sugrue, Frank. "An Ounce of Prevention." LAN Magazine Aug. 1995: 36-37.

This article encourages the use of disaster recovery planning as a preventive method. Give hypothetical situations and asks the reader to relate it to their organization.

SunGard Recovery Services Inc. (1995). Action Plan for Disaster. Pennsylvania.

This is a comprehensive guide on how to create an effective disaster recovery system. It defines disaster recovery and raises important questions on how to deal with disasters.

Titch, Steven. "Dangers of a Narrow (Band) Mind." Telephony 26 Aug. 1996: 5-6.

Talks about the shortcomings of Bell Systems. Specifically their lack of bandwidth to support their growing customer population.

Tobin, Michael. "Keep A Network Disruption from Becoming a Workgroup Computing Disaster." Managing Office Technology Oct. 1995: 36-37.

Gives information on the types of disasters requiring computer system recovery services. Gives information relating to vulnerability.

Toigo, Jon. Disaster Recovery Planning: For Computers and Communication Resources. New York: John Wiley & Sons, Inc., 1996.

This book gives a comprehensive methodology on the disaster recovery planning process.

Wagner, Mitch. "UUnet to Offer Uptime Guarantee." Computerworld 3 Feb. 1997: 2-3.

Talks about UUnet and its service guarantee. Also discusses qualities to look for in Internet service providers (ISPs).

II. Information Technology & Communication Information (ITC)

Carr, John B. "Cisco Routers and Terminal Servers." E-mail to Mark Smith. 17 Oct. 1997

This email is a printout of the routers and terminal servers at UVA. It lists the location, model, serial number, and UVA asset number.

Commonwealth of Virginia Council on Information Management. "Information Technology Security Standard." <http://www.cim.state.va.us/Pubs/Standards/s-95-1.htm#Authority> (31 Jan. 1995).

This discusses Virginia's policy on network security. It is a standard that defines what should be considered secure data and how the data should be protected.

ITC Network. Map. Information Technology & Communication: Virginia, 1997.

This is an updated network map of the current UVA network. It includes the changes made for the ATM upgrade. It also includes upcoming changes to the network.

Information Technology & Information (ITC)a. "The 1996-97 Guide to Computing and Communication Services at UVA." <http://www.itc.virginia.edu/department/services/guide.html> (17 Oct. 1997).

This is a comprehensive guide to the services at UVA. I can obtain information about each service and categorize its priority in a disaster recovery plan.

Information Technology & Information (ITC)b. UVA Network Topology. Virginia: 30 May 1996.

This pamphlet discusses the Network Topology at UVA. It talks about the FDDI protocol and includes various maps of the layout. The backbone and Carruthers Hall communication room detail is also included.

OIT/ITC. Chart. Information Technology & Communication: Virginia, 1997.

This chart shows the basic ITC hierarchy of positions. This allows me to see the designation of responsibility in the organization. This should prove very helpful in locating valuable resources within ITC.

Patterson, Richard A. "Sample RISK ANALYSIS AND SECURITY PLAN."
Memorandum to Departmental Security Contacts. 28 Apr. 1997.

This is a memo describing UVA's approach to risk and analysis and security. These factors are an important aspect to consider for a complete disaster recovery plan. The memo also discusses possible impacts that disasters may have on the university.

Patterson, Richard A., Data Security Officer and Chief Contingency Planner,
Charlottesville, VA. Personal Interview. 10 Oct. 1997.

Richard talks about equipment inventory and approaches to designing an effective disaster recovery plan. He also talks about old disaster recovery plans and gives sources of disaster recovery and security information.

Smith, Mark. Network Maps. WWW: <http://holmes.acc.virginia.edu/~mjs/netmaps>
(23 Sept. 1997).

Mark Smith has placed network maps that describe the network topology at UVA here. This includes the old FDDI network, as well as, ATM the new network.

Smith, Mark J., Network Systems Manager, Charlottesville, VA. Personal Interview.
30 Sept. 1997.

Mark narrows down what my disaster recovery system should include. He also emphasizes important services that must be accounted for in the plan. Mark lays out the general network topology and problems that ITC is encountering.

Staff Report, (1997, Oct. 3). Internet2, the Next Generation, Is and Zooming at U.Va.
InsideUVA.

This article is about the Internet2 service that UVA provides. This service is one that must be considered in the disaster recovery plan.

University of Virginia. Finance & Endowment. WWW:
http://www.virginia.edu/Facts/Glance_FinanceEndowment.htm (22 March 1998).

This page lists University of Virginia revenue information.

III. Protocol and Other Background Information

Cisco Systems. “Documentation, A member of the Cisco Connection Family.”
CD-ROM. Mountain View, CA: 1996.

Cisco places its documentation on CD-ROM relating to its products. I am interested in the routing protocol information. These protocols include RIP, IGRP, and EIGRP.

Cisco Systems. Enhanced Interior Gateway Routing Protocol. WWW:
http://www.cisco.com/univercd/cc/td/doc/cisintwk/ito_doc/55182.htm (22 March 1998).

Web page gives EIGRP related information.

Cisco Systems. Interior Gateway Routing Protocol. WWW:
http://www.cisco.com/univercd/cc/td/doc/cisintwk/ito_doc/55182.htm (22 March 1998).

Web page gives IGRP related information.

Cisco Systems. Routing Information Protocol. WWW:
http://www.cisco.com/univercd/cc/td/doc/cisintwk/ito_doc/55024.htm (22 March 1998).

Web page gives RIP related information.

Appendix A: Contact Names, Information, and Roles

Name	Contact Information	Roles
Sandra Bryant	NOT TO BE PUBLISHED	Primary - Special Projects Primary - dialin authentication Backup - Router Configuration Backup - Unix server configuration Backup - ATM Configuration
David Buchanan	NOT TO BE PUBLISHED	Primary - PCMAIL Primary - ARA dialin Backup - ATM Configuration
Gina Bull	NOT TO BE PUBLISHED	Primary - news services Primary - desktop video Primary - ATM video (new service) Primary - Dialin software support
John Carr	NOT TO BE PUBLISHED	Primary - Hostmaster Primary - T1-line connections Primary - routing configuration Backup - Router configuration Backup - DHCP
Jerry Dodd	NOT TO BE PUBLISHED	Primary - Mainframe connectivity Primary - ftp server user accounts Primary - ESYS contact
Glen Draper	NOT TO BE PUBLISHED	Primary - Mainframe connectivity Primary - Continuing Education links Primary - Corporate Time Accounts

		Backup - Corporate Time Server
Richard Findlay	NOT TO BE PUBLISHED	Primary - dialin lines Primary - ACD phone info links Primary - PC Software Installers Backup - router configuration (training)
Jim Jokl	NOT TO BE PUBLISHED	Primary - Management Primary - Budget Primary - Corporate Time Server software Backup - Router Configuration
Ken Ruggaber	NOT TO BE PUBLISHED	Primary - mail gateway Primary - pmail unix server Primary - sendmail configuration Backup - CMS servers
Cleo Smith	NOT TO BE PUBLISHED	Primary - mainframe connectivity Primary - remote printing from mainframe
Mark Smith	NOT TO BE PUBLISHED	Primary - on-site management Primary - CMS servers Backup - Router configuraiton Backup - news servers Backup - ftp servers
Tang Tang	NOT TO BE PUBLISHED	Primary - ATM/FDDI network Primary - network management software Primary - DHCP Backup - DNS

OUTSIDE KEY CONTACTS		
Hamp Carruth	NOT TO BE PUBLISHED	Unix Systems manager
John Robertson	NOT TO BE PUBLISHED	Network Operations manager (Physical Network) (building hubs)
Bob Campbell	NOT TO BE PUBLISHED	Micro Systems Manager PCMAIL Novell backup
Jackie Daniel	NOT TO BE PUBLISHED	Purchasing Manager
George Payne	NOT TO BE PUBLISHED	Help Desk Manager
Sandra German	NOT TO BE PUBLISHED	Publications Manager
Virginia Bergland	NOT TO BE PUBLISHED	COO

Appendix B: Service Profiles

SERVICE	PRIORITY	PRIMARY MACHINE NAME	PRIMARY MACHINE LOCATION	BACKUP MACHINE NAME	BACKUP MACHINE LOCATION	OPERATION STATE W/ BACKUP	DATA/TAPE LOCATION	Comments
Dialin Access 28.8 1-hr		Cisco AS5200	Gilmer	1 day service agreement, other lines	n/a	Alternatives are slower or have different time restrictions	n/a	Dialin service available for a fee from various providers in the community should Gilmer be lost to major disaster users could contract for service individually to work around this outage.
Dialin Access 28.8 30-min		Cisco AS5200	Gilmer	1 day service agreement, other lines	n/a	Alternatives are slower or have different time restrictions	n/a	
Dialin Access 28.8 15-min		Cisco 5xx/USR Rack modems	Gilmer	Spare parts except for modems	Gilmer	Alternatives are slower or have different time restrictions, available 14.4 spare modems	n/a	
Dialin Access 28.8 department		Cisco AS5200	Gilmer	1 day service agreement, other lines	Gilmer	Alternatives are slower or have different time restrictions	n/a	
Dialin Access 14.4 1-hr		Cisco 5xx/USR Rack modems	Gilmer	spares to replace any one failure	Modems Fontana, Cisco 5xx Gilmer	Alternatives are slower or have different time restrictions	n/a	
Dialin Access 14.4 30-min		Cisco 5xx/USR Rack modems	Gilmer	spares to replace any one failure	Modems Fontana, Cisco 5xx Gilmer	Alternatives are slower or have different time restrictions	n/a	
Dialin Access ARA		Lanrovers	Gilmer	none, other lines	Modems, Gilmer, lanrover no spare	Service is on 2 devices, each can fail independently	Wilson Help desk has password files	Commercial dialin services don't provide ARA service.
Dialin authentication		uvaarpa	Carruthers	Backup constantly available.	Gilmer	Backup doesn't support adding or changing accounts	Carruthers	Operation from backup does not support adding new accounts or changing passwords. Spare Sparc 20 available in Carruthers which could be in place within 24 hours from total failure, 2 hours to swap processor.
PCMAail		sun.pcmail	Carruthers	any IPC would provide degraded access in	Carruthers		Carruthers	Available spare processor in Carruthers.

				a pinch				
PCMail		Novell Server	Carruthers	1 Spare on site	Carruthers		Carruthers	
Central Mail Service (IMAP/IMSP)		server1	Carruthers	server2	Carruthers	degraded; 8 hours to restore service; 48 hours to restore all folders	Carruthers	Assumes load can be supported on server2. Performance would be slow.
Central Mail Service (IMAP ONLY)		server2	Carruthers	none	n/a	n/a	Carruthers	No single machine available could replace this server.
Mail Gateway Service (includes Majordomo)		Primary Mail Server	Carruthers	Backup Mail Server using sparc 20 spare	Carruthers	degraded	Carruthers	
Electronic News		murdoch	Carruthers	Backup hardware in form of spare sparc 20, no backup to disks, non-UVA content not backed up	Carruthers	loss of data	Carruthers	Non-uva content would be lost in 5 days anyway due to expirations. Non-UVA content available from www.dejanews.com
		hearst	Carruthers	Backup hardware in terms of sparc20 or ipc	Carruthers/Forestry	Degraded, loss of data in transit	Carruthers	Configuration backed up, data in transit not backed up.
User Database (Whois)		debow.itc	Carruthers (Server room)	Juno.itc	Carruthers server room	(juno provided this service in the past.)	Carruthers	
Primary Unix Machine Access		Carruthers Router, 350T and 303 switches	Carruthers (Comm room)	Spares on site for 1 of everything, hot spare routing to network. Spare router in Gilmer.	Forestry, Gilmer, on-site, fontana	Degraded performance by swapping back to spare AGS+	netmon.itc has configurations saved (in carruthers)	
Mainframe Access		Routers in carruthers, Built-in network interfaces, 8323	Carruthers (Comm room, Unmanned room)	On site 5 available interfaces on the mainframe. Interfaces replaced when mainframe replace	Carruthers	Loss of test system access if one of them must be used to replace failed interface	Router configuration stored on netmon.	

				in case of total loss.				
Network path to Core Network Servers, ACCPUBLIC, Labs + Classrooms, Dorms		Carruthers Router, 350T and 303 switches	Carruthers (Comm room)	Spares on site for 1 of everything, hot spare routing to network. Spare router in Gilmer.	Additional spares Forestry, Fontana		Router configuration stored on netmon.	
Calendar Service		Server1/Server 2	Carruthers Comm Room	Same as CMS	See CMS	See CMS	Carruthers	Service could be restored by loading the databases on other machines and changing name server entries. Option to split to multiple Sparc 20s.
Help Desk Network		Router in Garrett, building switches	Garrett, Wilson	Available hubs/to replace the switch, Spare router in Gilmer	Gilmer, Forestry, Fontana			
Computerized Class Rooms Network Access		Same as Help Desk	See help desk	See help desk	See help desk	See help desk	See help desk	
Internet Access		UVA-internet router, Carruther Lightstream 1010 switch	Carruthers	Spare router in Gilmer, Spare 1010 in Forestry		Configurati on stored on netmon	Primary and backup internet in same router. If Carruthers lost, primary internet can be connected at VL using spare router and capacity on the VL 1010, or spare 1010. Automatic cut-over to 6Mb backup internet connection with loss of vBNS service if the fiber optic connection to Net.Work.Virginia is lost.	
Routing Protocols								Routing protocol is distributed across router configurations. Loss of a 7507 router may require redistributing parts of the configuration to other routers.
DNS		uvaarpa		juno, mars.itc, nom	nom - Gilmer; Juno - Carruthers; mars.itc - Carruthers	degraded; failure moves new host additions to maunal process		Cutover to nom and Juno are automatic on failure. Re-enabling service on mars.itc would require restoring from tape.

Mass Store Archive MAGGIE Access (SPECIAL CASE)		Maggie, archive	530 McCormick Road	NONE				This plan only considers access, this is a production service provided outside of normal computer rooms. Spares exist for all components from the backbone to forestry. Machine could be relocated in the event of an extended outage of network access in forestry.
Building Level Access	SEE	OTHER	TABLE	FOR	MORE INFO.			General comment: Adequate spares of routers/switches exist to reconfigure around loss of hardware components providing the service. Building premissis wiring and fiber optic backbone restoration may extend outages in some cases.
DHCP		nom	carruthers	heimdall.i tc	gilmer	failure prevents new DHCP address assignments		

Appendix C: Machine Details

MACHINE DETAILS

MACHINE NAME	MACHINE LOCATION	MODEL	MEMORY	DISK SPACE	SERIAL #	VENDOR	ADDITIONAL INFO.	ALTERNATE SUPPLIER
Primary Mail Server	Carruthers	Ultra Enterprise 3000 4x167 MHz processors	1 Gbyte	12x4.2G RAID			4 SCSI interfaces	
server2	Carruthers	Ultra Enterprise 3000 4x250 MHz processors	2.5 Gbytes	28x4.2G			4 SCSI interfaces	
server1	Carruthers	Ultra Enterprise 3000 4x250 MHz processors	1 Gbyte ??	16x4.2G			4 SCSI interfaces	
Uvaarpa	Carruthers	Sparc 20 2x60 MHz processors		2x4.2G				
Nom	Carruthers	Sparc 2	64Mb					
Debow	Carruthers	RS/6000						
heimdall.itc	Gilmer	Sparc 2	64 Mb					
mars.itc	Carruthers	Sparc 20	64 Mb	4.2G				
Odin.itc	Carruthers	RS/6000						
PCMAIL Servers	Carruthers	inhouse configured 486	128	2G			5 identical systems, on-site spare	
PCMAIL Gateways	Carruthers	inhouse configured 386/486	1M	Floppy			15 identical systems, on-site spare	

Appendix D: Selected Recovery Costs and Information

Selected Recovery Information

Device	Cost per Device (in thousands)	Number of Devices	Total Cost (in thousands)	Delivery Time (in days)	Setup Time (in days)	Total Time (in days)	Comments
Mail Servers	\$10	3	\$30	15	2	17	
News Servers	\$15	2	\$30	1	less than 1	2	
DNS	\$5	3	\$15	n/a	less than 1	1	
Routers	\$80	each	n/a	n/a	less than 1	1	
1010 ATM	\$40	each	n/a	n/a	less than 1	1	
Catalyst 5000	\$25	each	n/a	n/a	less than 1	1	
Dial Up Servers	\$18	7	\$126	n/a	less than 1	1	

Appendix E: Disaster Recovery Recommended Information Sources

- (BOOK) Disaster Recovery Yellow Pages, from Systems Audit Group (617-332-3496)
- Sections include: Consulting and Services, Hotsites, Emergency Equipment Resources, Software and Training
- 2700 U.S. Vendors w/ 300 Categories relating to disaster preparedness and recovery services. Including categories such as computer repair specialists, data and records recovery, new or used equipment, drying and dehumidification of paper and microfilm records, emergency mobile satellite dishes, and sandbag-filling equipment.
- (SOFTWARE) Advanced Information Management AIM/LAN 2000 by Saber Software Corp. Woodbridge, VA (703) 643-1002.
- (SOFTWARE) Palindrome Corp.'s Prepare
- (SOFTWARE) by Chi/Cor Information Management
- (SOFTWARE) by Comdisco
- (SOFTWARE) MiraLink's Off-Site Server replicates NetWare servers anywhere
- (SOFTWARE) Econet by Compuware
 - Tells which applications are consuming bandwidths, irrespective of the underlying LAN protocol and can identify which users are logged on to particular applications
- (SOFTWARE) Standby Server 32 by Vinca.
 - Netware Server Mirror Software
- (COMPANY) Netops Corp. www.netops.com
 - Consulting firm on disaster recovery support.
- (SOFTWARE) Octopus Real Time Data Protection by Octopus Technologies
 - Windows NT Server Mirror software.
- (SOFTWARE) Network Custodian by Network Custodian
 - Helps create a disaster recovery plan
- (COMPANY) UUNet – Internet Access Provider
 - Will refund up to a quarter of a monthly service fee if communications go down for about 43 minutes per month
- (COMPANY) Communication Assurance Services Inc. in Washington, D.C.
 - Specializes in security management. Provide multiphased methodology in which it works with network managers and internal audit staff to document network, identify potential points of penetration, and then develop plans to protect each point of vulnerability