LARGE DATA NETWORK SURVIVABILITY

by

Richard A. Woynicz

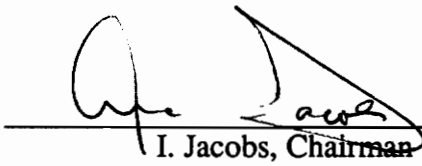
Project submitted to the Faculty of the
Virginia Polytechnic Institute and State University
in partial fulfillment of the requirements for the degree of

MASTERS OF SCIENCE

in

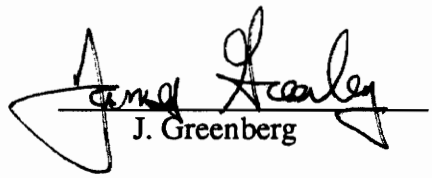
Systems Engineering

APPROVED:



I. Jacobs, Chairman

B. Blanchard



J. Greenberg

April 21, 1990

Blacksburg, Virginia

LARGE DATA NETWORK SURVIVABILITY

by

Richard A. Woynicz

Committee Chairman: Ira Jacobs
Electrical Engineering

(ABSTRACT)

Components of a typical data communications network are identified and reliability for each component is determined. Transmission systems, access and long haul, are identified and their reliabilities are determined. Long haul network reliability is analyzed using various factoring theorem algorithms.

These results are then compiled to determine end-to-end reliability for various access methods and network types. Conclusions are drawn on methods to increase network reliaibility.

TABLE OF CONTENTS

SECTION	PAGE
1.0 Introduction	1
2.0 Review of Literature	2
3.0 Materials and Methods	4
3.1 Scope	4
3.1.1 General Model of a Communications Network	4
3.2 Network Reliability Mathematics	6
3.2.1 Assumptions	6
3.2.2 Reliability Function	8
3.2.3 Series, Parallel, and K out of N Systems	9
3.2.4 Availability	11
3.2.5 Other Factors Effecting Reliability	12
3.3 Equipment Reliability	12
3.3.1 Access Equipment	12
3.3.1.1 Analog Access Equipment	13
3.3.1.2 Digital Access Equipment	16
3.3.2 Data Switching Equipment	18
3.3.2.1 Packet Switching Equipment	18
3.3.3 Concentration and Multiplexing Equipment	19
3.3.3.1 Fiber Optic Terminal (FOT)	24
3.4 Transmission	24
3.4.1 Local Exchange Carrier	24
3.4.1.1 LEC Architecture	27
3.4.1.2 LEC Switch Reliability	28
3.4.1.3 Alternative Local Carriers	31
3.4.2 InterExchange Carriers	31
3.4.3 Transmission Systems	33
3.4.3.1 Analog Access	33
3.4.3.2 Digital Access	36
3.4.3.3 High Speed Digital Transmission	36
3.4.3.4 Other Transmission Methods	39
3.4.3.4.1 Microwave	39
3.4.3.4.2 Switched 56 Kbps Data	40
3.4.3.4.3 Switched T1 Data	42
3.4.3.4.4 Satellite	42
3.4.4 Tariff Options	43

SECTION		PAGE
	3.5 Model for Network Reliability	43
	3.5.1 Network Terminology	44
	3.5.2 Classes of Network Problems	45
	3.5.3 Reliability Algorithms	47
	3.5.3.1 Factoring Theorem	48
	3.5.4 Simulation of IXC Network - Undirected Graph	51
	3.5.4.1 Undirected to Directed Graph Conversion	53
	3.5.5 Simulation of IXC Network - Directed Graph	56
	3.5.6 End-to-End Reliability	56
4.0	**Results**	61
	4.1 Equipment Reliability	61
	4.2 Transmission Reliability	61
	4.3 Modeling Results	61
5.0	**Discussion**	64
	5.1 Discussion of the Results	64
	5.2 Deficiencies in the Model	65
	5.3 Validity of Reliability Numbers	66
	5.4 Failure Mode and Effect Analysis	67
	5.5 Software Reliability	67
6.0	**Conclusion**	70
7.0	**Summary**	71
8.0	**Literature Cited**	72
	8.1 Additional References	73
	8.1.1 Reliability Algorithms	74
	8.1.2 General Articles on Reliability	75
	8.1.3 Component Reliability	75

SECTION	PAGE
Appendix A Packet Switch Reliability Calculations	76
Appendix B Channel Bank Reliability Calculations	80
Appendix C Intelligent Multiplexer Calculations	82
Appendix D Program Results	84
Appendix E End-to-End Model Calculations	88

1.0 Introduction

The purpose of this project is to describe and model the reliability of today's large data networks. Systems engineering practices are applied through reliability calculations and systems modeling. This report presents both the real life implementation and the mathematical modeling required to design network survivability.

There are many areas of reliability design that impact network survivability. This project and report covers some of those areas and develops models that can be used to determine the global reliability of a data communications network.

Before designing the models, reliability mathematics are reviewed and model components are identified. Model components include reliability of equipment and transmission facilities. Modeling techniques are then be applied to integrate these components.

2.0 Review of Literature

The history of network analysis and, more specifically, network reliability dates back to the 1950s. Some of the initial work in the field of mathematical reliability began with von Neumann during 1952 in the study of biological systems [1]. Von Neumann believed that the reliability of the system can be greater than the reliability of the individual parts, because of redundancy that can be built into the system. In 1956, Moore and Shannon [1] provided the mathematics to justify this belief and applied it to the reliability of relay circuits. They also introduced the concept of the reliability polynomial.

The 1950s brought reliability studies to the fields of computers, missiles, and the space program through systems engineering. In the 1960s reliability mathematics was applied to networks. Through this work it was realized that network reliability calculation is a very complex mathematical problem. In 1966, Steiglitz, Weinger, and Kleitman [1] introduced the procedure of designing networks at a minimum cost with minimal connectivity constraints.

Network reliability analysis emerged as a distinct discipline in the 1970s. It was applied to large networks such as oil and gas networks, information networks, and power networks. Some of the advances during the 1970s were made by Wilkov, Frank, and Fish [2, 3], who introduced the factoring theorem to network reliability; by Fratta and Montanari [4] who introduced Boolean algebra methods for reliability; and by Rosenthal [1] who showed that calculating network reliability required finding a polynomial algorithm for the problem.

The 1980s brought continued analytical research on classification of problems and algorithms to speed up or estimate the solution to reliability problems. Two of the major groups of contributors were Wood and Satyanarayana [5] who classified problems that are

solvable in polynomial time; and Ball and Provan [6] who determined that the all-terminal problem was NP hard.

Today, analyzing reliability continues, but with a better understanding of the complexity of some networks. Current research continues to search for easier cases (or reductions of complex problems into solvable forms), by setting bounding limits, and by finding more efficient methods and algorithms for estimating reliability.

In addition to the analytical aspects of network reliability, there has been an increased interest in lowering the risk of large network outages. Current articles [7] have been written on fiber optic transport architectures that incorporate increased network survivability. High capacity transmission media and the potential for large network outages have made the network designer and the user more cognizant of the frailty of their network and the potential for disaster.

3.0 Materials and Methods

3.1 Scope

This project has a broadly defined scope. It begins with conceptual ideas that can be comprehended by a non-engineer and converges to concrete network analysis understood by mathematicians. This project determines the generic components of a typical data communications system. It then provides a high-level description of the components of the model and determines the specific reliability for each component. The project then reassembles the components into a model and calculates network reliability for different architectures and access methods. The underlying problem this project is to answer is how to increase network reliability.

3.1.1 General Model of a Communications Network

To understand data communications network survivability, one must understand the data communications network from both practical and theoretical perspectives. Data communication networks can be modeled as shown in Figure 1. Customer premise equipment (CPE) connects to the network at the network interface (NI). Traffic then traverses from the customer source site to the long distance carrier point-of-presence (POP), through the local access provider. From there data travels though a long distance network to the destination site and through another local access provider. In this project the long distance network is modeled as a 4x4 meshed network. Each component of this general model has many subsystems that effect the reliability of the end-to-end circuit. These subsystems are investigated in the report.

The remaining chapters look at subsystems of the general model. Once determined, the components are combined into a comprehensive model for reliability. The remainder of

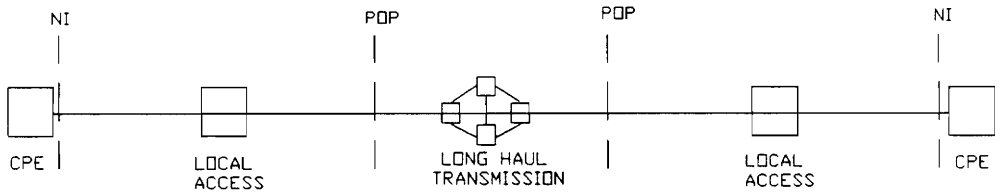


FIGURE 1 - GENERAL MODEL OF A COMMUNICATIONS NETWORK

Section 3 is divided into the following topics:

- o Mathematics
- o Equipment
- o Transmission
- o Modeling

3.2 Network Reliability Mathematics

Communication systems include numerous components. By decomposing the system into pieces and through use of combinatorial mathematics, global system reliability can be calculated.

Much research has been done calculating communications network reliability, particularly with respect to the reliability of early packet switched networks such as the ARPANET developed under the DARPA contract in the 1970s (and still used today). The following sections describe the basic mathematic tools needed to calculate reliability for subsystems. The equations listed can be found in many text book references such as Hiller and Lieberman's *Introduction to Operations Research.* [8]

3.2.1 Assumptions

Most telecommunications and data communications equipment is composed of electronic circuits. The reliability of electronic circuitry can be modeled as shown in Figure 2.[9] In the beginning of the life cycle, the electronic device has a decreasing failure rate due to manufacturing or material defects. The operational period shows a constant failure rate. The end of the life cycle shows an exponentially increasing failure rate as the electronics deteriorate due to age. This report assumes that the components studied exhibit a constant failure rate, thus they are in the operational period of their life cycle. Equipment reliability is calculated on a single circuit basis. Multiple circuit and equipment failure

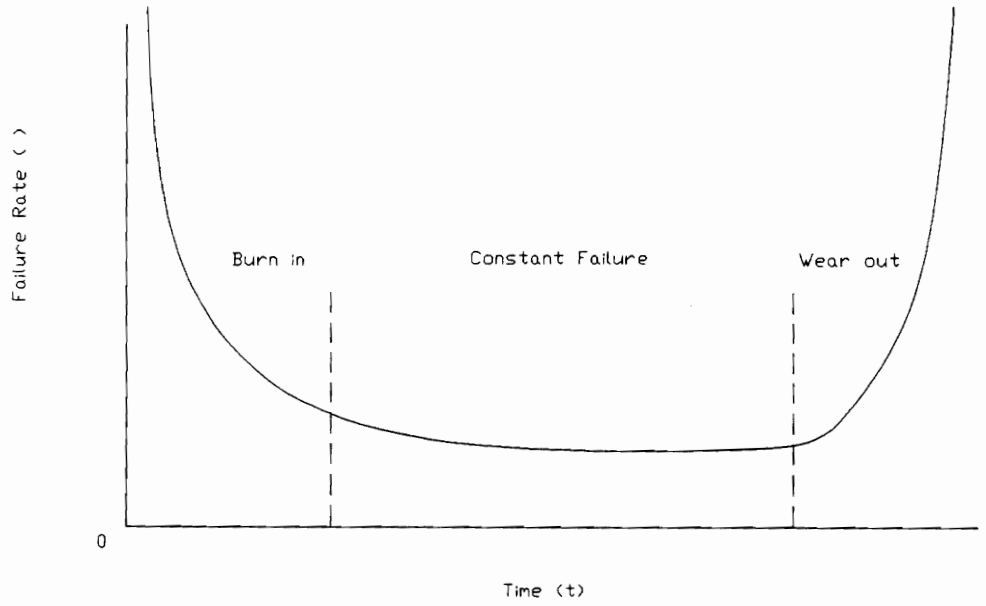


FIGURE 2 - ELECTRONIC CIRCUIT FAILURE

impact is covered in Section 5.0, Discussion.

The calculations also assume that all subsystems are stochastic binary systems (SBS).[6] SBS systems are ones in which the components fail randomly (stochastically) and that the system is either operational (state=1) or has failed (state=0).

The models in the paper assume independence between the subsystems, that is the failure of one component does not affect the operation of another. If independence is not assumed, then the mathematical equations become complex and go beyond the scope of this general model. The models presented also adhere to the assumption that the components have no historical knowledge of their past performance. Their failure rate is not dependent on operational time. Since we are adhering to an SBS system, this can be assumed.

3.2.2 Reliability Function

There are two definitions of the reliability function commonly used. The first form is shown in Equation 1. This form of the reliability function defines the probability that a system will be operating at a specific time (t). It describes the reliability of the components as an exponential function of a constant failure rate of one over the Mean Time Between Failure (1/MTBF). Though this form is very useful for determining the dynamic properties of electronic equipment, it is not very useful for network reliability calculations since it does not consider the fact that the system can be repaired and placed back into service.

$$R = e^{-\lambda t} \qquad (1)$$

$\lambda = 1/MTBF$ = Average failure rate in hours

t = Time

To include in the repair rate (Mean Time to Repair = MTTR) in the reliability function and to average reliability over time, a second equation is used. It is preferred for

network analysis (see Equation 2). This form of reliability is similar to the definition of availability and is defined as the probability that the system will be operational.

$$p = \frac{\frac{1}{\lambda}}{\frac{1}{\lambda} + \frac{1}{\mu}} \qquad \mu = 1/MTTR = \text{Average repair rate in hours} \qquad (2)$$

$$p = \frac{MTBF}{MTBF + MTTR}$$

3.2.3 Series, Parallel, and K out of N Systems

Series systems can be compared to a string of old style Christmas tree lights: when one bulb burns out, the whole string is out. This is because each light is dependent on the operation of the preceding light. If one component fails the whole system fails.

In a parallel or redundant configuration, failure of one parallel component does not result in system failure. An example of this would be residential home lighting systems. In a home, when one light bulb burns out, the entire house does not go dark. This is because residential lighting systems are typically wired in parallel.

In a K out of N system, K of N parallel components are needed for the system to operate properly. An example of a K out of N system is car tires. With 5 tires (4 plus 1 spare) 4 out of 5 must be usable in order to operate the car.

The reliability of a series system of n components is equal to the product of the reliabilities as shown in Equations 3 and 4.

$$p_{sys} = p_1 * p_2 * p_3 * \ldots * p_n \qquad (3)$$

or

$$p_{sys} = \prod_{i=1}^{n} p_i \quad (4)$$

where n = the number of series components in the system

If all n units were identical then the series reliability would reduce to Equation 5.

$$p_{sys} = p^n \quad (5)$$

When parallel or redundant components are used in the system, the reliability is found by using the expression:

$$p_{sys} = 1 - (1-p_1)(1-p_2)(1-p_3)...(1-p_n) \quad (6)$$

or

$$p_{sys} = 1 - \prod_{i=1}^{n} (1-p_i) \quad (7)$$

where n = the number of parallel components in the system

If all units were identical, then the parallel reliability would reduce to Equation 8.

$$p_{sys} = 1 - (1-p)^n \quad (8)$$

The unreliability of the system is given as:

$$q_{sys} = 1 - p_{sys} \quad (9)$$

K out of N redundancy is calculated as shown in Equation 10. It is used in systems that require a set number of components to operate in order for the system to operate. The resulting equation considers that the random variable states of the system have a binomial distribution of parameters n and i. In this project, Equation 10 is also used to model X:Y

(X for Y redundancy), where K=X-Y and N=X. Again, the components are assumed to have identical reliability for mathematical simplicity ($p_1=p_2=p_3=...p_n$).

$$p_{sys} = \sum_{i=K}^{N} \binom{N}{i} p^i (1-p)^{N-i} \qquad \binom{N}{i} = \frac{N!}{i! * (N-i)!} \tag{10}$$

This equation states that the system will survive or be operable if K, K+1, K+2, ... N-1, or N units are operating correctly.

3.2.4 Availability

Availability is a measure of the probability that a system or group of components being operational over the period of time with repairs (usually 1 year).

$$A = \frac{\text{Time System is Operational}}{\text{Total System Time Operational and Not Operational}} \tag{11}$$

In the communications industry, MTTR is usually defined as the time between when the device fails and when the device is back in operation. A 4-hour MTTR objective is commonly used in the communications industry. [10] A more realistic objective can be as long as seven hours. This considers more complex systems like fiber optics and the industry trend towards less operations personnel, resulting in longer response times. Even with this higher MTTR, actual repair times may vary from the MTTR depending on whether the failure is close to manned sites and other factors such as operations personnel training. This project will use various measures of MTTR based on the component complexity and assumed troubleshooting tools.

Unavailability is the opposite of availability. It is calculated from availability by:

$$\overline{A} = 1 - A \tag{12}$$

To equate the unavailability to a more comprehensible number, multiply the unavailability by 8,760 (number of hours in a year). The new number is the number of

hours per year that the system will be down. This project uses a year as the standard period of time for all calculations.

3.2.5 Other Factors Effecting Reliability

Other measures of reliability that this project does not specifically address in the Materials and Methods section are network capacity, software reliability, and reliability considering other performance measures like delay, quality (error rate), and cost. Some of these additional factors are considered in Section 5.0, Discussion.

3.3 Equipment Reliability

Since the divesture of AT&T in 1984, there has been an increase in the number and types of equipment used in data communications networks. This has added complexity and confusion to determining network reliability.

In general, most data communications networks, whether they are IBM SNA type networks, packet switched networks, circuit switched networks, or other types of network, have three general types of devices:

- o Access or interface devices - Modems, DSUs, CSUs
- o Switching devices
- o Concentrating or multiplexing devices

Access devices are used with data communications equipment to interface to public telecommunications networks. Switching devices are used for routing (switching) traffic to destinations through addressing or predetermined routing. Concentration or multiplexing devices are used to combine traffic for more economic use of transmission facilities.

3.3.1 Access Equipment

There are two primary methods to gain access to data communications networks:

through analog facilities or through digital facilities.

3.3.1.1 Analog Access Equipment

Analog facilities require use of modulator/demodulators to convert the digital output of the CPE devices into analog signals. Modems convert the digital input (e.g., EIA-232D) to analog signals that can be transmitted on analog facilities such as copper, analog microwave, or satellite. They accomplish this conversion through modulation of the digital signal. Voice grade analog facilities used by modems support a 3,000 Hz bandwidth (300-3,000 Hz).

Modems are most often used in three applications (see Figure 3):

- o 2-wire dial-up mode
- o 4-wire dedicated leased line mode
- o Multidrop mode

Modems are commonly used to gain access to public networks such as US Sprint's Public Data Network (previously called Telenet). Access is gained by using 2-wire dial-up modems. The user dials a local call to the public network (rotary). Today 2-wire access is limited to speeds of 9,600 bps and below though compression algorithms are increasing throughput. Though throughput may appear full-duplex, most 2-wire access is actually limited to half-duplex because of the frequency bandwidth limitations of the 2-wire transmission path. Transmission facilities for 2-wire access are provisioned under the Local Exchange Carrier Switched Access tariffs.

A modern example of a 2-wire modem is the recent CCITT standard V.32 modem. V.32 modems achieve 9,600 bps throughput (full-duplex) by modulation schemes such as Quadrature Amplitude Modulation (QAM) or Trellis Coding and echo cancellation.

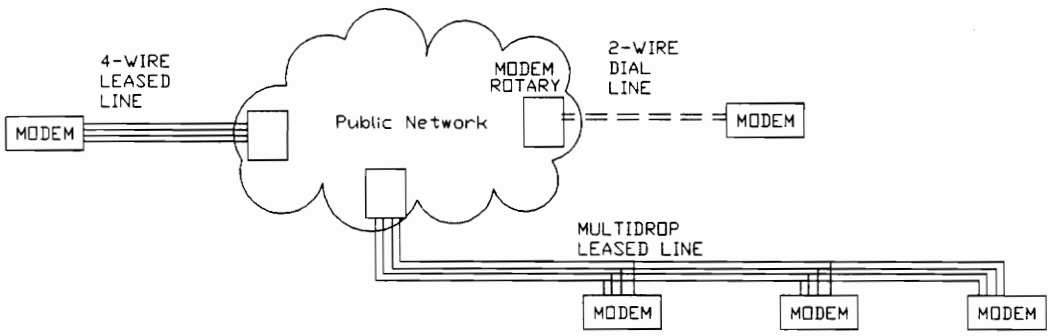


FIGURE 3 - MODEM APPLICATIONS

The 4-wire leased line mode of access is for high speed, full-duplex access and requires dedicated lines to the network. Through advanced compression algorithms and modulation schemes, 4-wire analog modems today can reach speeds up to 34,800 bps (full-duplex). Dedicated 4-wire access is provisioned through the Special Access tariffs of the Local Exchange Carriers. Depending on the modems and line quality, some additional line conditioning may be required for high speed modems.

Multidrop is a special case of 4-wire access and is very common in IBM networks. This access method is useful when the terminals (users) are clustered in small areas. A typical application would be Automatic Teller Machines (ATM) where bank branches are usually within the same locale. Testing multidrop circuits require more sophisticated modems and technical training.

The reliability of modems depends on the complexity of the device. Very simple modems (e.g., Bell 212A compatible) provide only simple modulation and demodulation of digital signals. Many modems today are becoming increasingly complex. Modern modems include dial memory, multiplexing options, error correction/ detection protocols, echo cancellation, automatic line equalization, and network management (for improved MTTR). As these modems become more complicated, there is a greater probability of hardware or software errors and failure of the device. In addition, modems, since they must interface to analog facilities, require more active, failure-prone devices such as relays and transformers.

Typical MTBF of a modem is 30,000 hours for stand alone modems and 60,000 hours for rack mount modems. [11] The difference between stand alone and rack mount modem reliability is due to the more robust and redundant power supplies often found in rack mount units. For this project, we will assume the network supports stand alone units

only.

Leased line reliability can be increased by use of an automatic dial backup unit (DBU) (see Figure 4). Some modems come with a built in DBU, others require an external device. These DBUs can be programmed to either automatically or manually dial around a dedicated leased line failure by accessing the circuit switched network. Dial backup unit reliability can be approximated at 50,000 hours. [11]

3.3.1.2 Digital Access Equipment

Digital facilities convert the digital output of CPE to digital signals that can be transmitted across communications networks. Digital facilities require interface devices called Data Service Unit and Channel Service Unit (DSU/CSU). Theses are simple electronic devices that primarily provide testing and interface to the transmission facility. They, unlike modems, do not use modulation. They transmit digitally on copper wires that are conditioned for digital electrical signals instead of voiceband analog signals. The DSU/CSU's primary functions are to provide:

- o Clock recovery
- o Loopback
- o Interface to DTE equipment signal levels (CCITT V.35 or EIA-RS-232)
- o Convert DTE signals to network baseband bipolar
- o Interface to network 4-wire digital circuit

Because of the simplicity of the DSU/CSUs, they have a very high reliability. A typical stand alone DSU/CSU has a reliability of over 50,000 hours. [11]

Stand alone CSUs are used to interface to the network at high speed digital rates (1.544 Mbps). These units provide some of the functions listed above for DSU/CSUs.

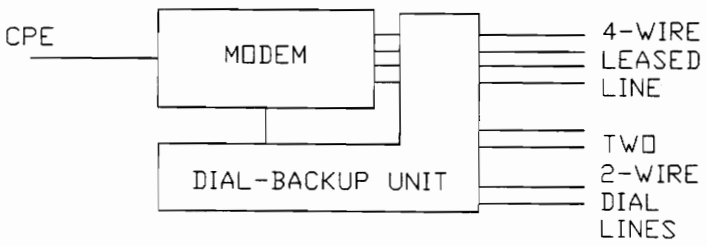


FIGURE 4 - MODEM WITH DIAL BACKUP UNIT

Channel Service Units that interface to the network have a reliability of over 60,000 hours. [11]

3.3.2 Data Switching Equipment

In general, most data switching equipment employ frame switch technology and architectures. Some examples of data switching equipment include data private branch exchanges, IBM front end processors, ISDN switches, and packet switches. Switch functions in a data communications network may include:

- o Protocol conversion
- o Speed conversion
- o Address translation
- o Routing
- o Testing
- o Network management

Technology is rapidly expanding the role of data switching equipment. Today's simple packet switches may be replaced by more sophisticated broadband switches using a frame relay or high speed broadband protocol. However, much of the foundation of today's switches will be used in the future.

The following sections detail the specific reliability requirements for today's existing packet switches. The reliability of one of Telenet Communications Corporation's packet switch, the TP4/II, is discussed. The TP4/II switch is representative of traditional packet switch technology.

3.3.2.1 Packet Switching Equipment

Most packet switching equipment is built around the von Neumann type computer architecture. This architecture includes four components that operate serially, central

processor, bus, memory, and input/output processors. Telenet's TP 4000 Series II (TP4/II) processor has this architecture.

The operation of the TP4/II involves processing information into and out of the switch by line processing units (LPU) or I/O processors. These then communicate to the central processing unit (CPU). Communications between the LPU and CPU occurs across the bus under the control of the bus arbitrator (ARB). The CPUs and LPUs also access memory, again through the bus systems.

Telenet's TP4/II Packet Switch can be configured with four types of redundancy:

- Common Logic Redundancy (CLR) - Arbitrator, Shared Memory, Bus, and Central Processing Unit
- Line Processing Unit (LPU) N for M Redundancy (1:N used in this project)
- Power Systems Redundancy
- Load Line Redundancy

The CPU, arbitrator, and shared memory, can each have a backup unit that is automatically switched into service when the active unit fails. The arbitrator, buses, and memory units are treated as a single unit (AMU). A single failure of any one of theses devices causes a switch over of all three units to the backup units.[12]

The reliability of the TP4/II subsystems is shown in Figure 5 and Table 1. TP4/II channel reliability is greater than 200,000 hours. Detailed hardware reliability calculations for the TP4/II are shown in Appendix A.

3.3.3 Concentration and Multiplexing Equipment

Data communication networks concentrate and multiplex traffic for more economical use of transmission media. Concentration allows multiple channels to use the same transmission facility. The sum of the bandwidth of the input channels is greater than the output bandwidth of the transmission facility. Concentrators or statistical multiplexers

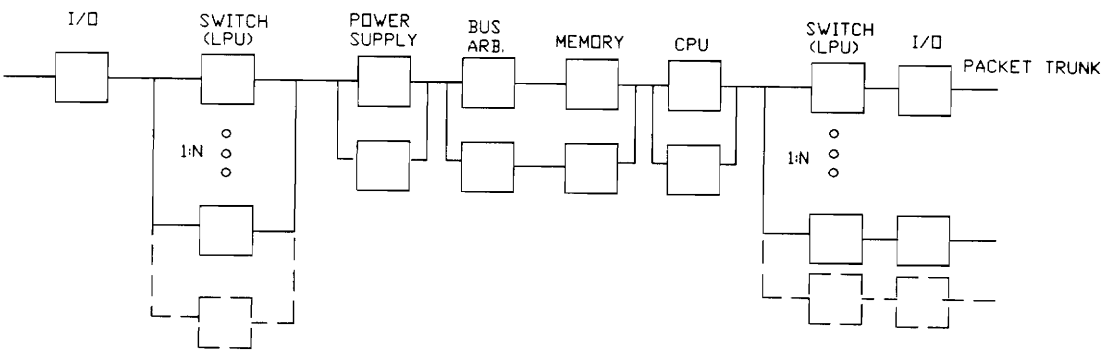


FIGURE 5 - TP4/II SUBSYSTEM MODEL

TABLE 1 - TP4/II SUBSYSTEM RELIABILITY

Subsystem	MTBF(hours)	P (MTTR=7 hours)
CPU	26,386	0.999735
Power Supply (TPPS-2)	23,581	0.999703
ARB/Bus	59,959	0.999883
Memory	26,824	0.999739
LPU (HSLPU)	11,922	0.999413
I/O (HI I/F)	447,066	0.999984

are examples of such network devices. Multiplexing is done by time-division multiplexers such as channel banks or intelligent multiplexers. Multiplexer input channel bandwidth is equal to or less than the output bandwidth.

A typical concentrator has an architecture similar to that of a packet switch (i.e., von Neumann). Concentrators are typically built to be inexpensive with less redundancy than switches. Concentrators do not usually concentrate large volumes of traffic. A small, non-redundant concentrator (Telenet TP3010) has a MTBF of 6,133 hours. [13]

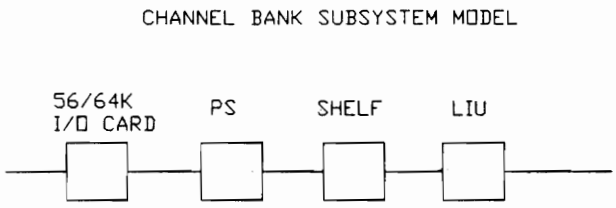
Time-division multiplexers come in many forms. The majority of these multiplexers conform to the North American digital hierarchy (see Figure 11 in Section 3.4.3.3). Included in this family of network equipment are:

- o Channel banks (Multiplexer 1/0 {M10})
- o Intelligent multiplexers (intelligent channel banks)
- o M13 multiplexers

Channel banks are typically non-redundant, but highly reliable as a system with an MTBF of approximately 200,000 hours on a channel basis. A subsystem model for a typical channel bank is shown in Figure 6. Channel bank reliability calculations are shown in Appendix B. [14]

Intelligent multiplexers are a private network outgrowth of channel banks. A typical intelligent multiplexer in a redundant configuration is shown in Figure 6. A typical redundant, intelligent multiplexer has a MTBF of over 40,000 hours. Calculations are shown in Appendix C. [15]

A higher traffic multiplexer a M13 (multiplex 28 DS1s to 1 DS3) has a MTBF of 82,000 hours. With redundancy and protection switching, the MTBF is calculated at over 3.6 million hours. [16]



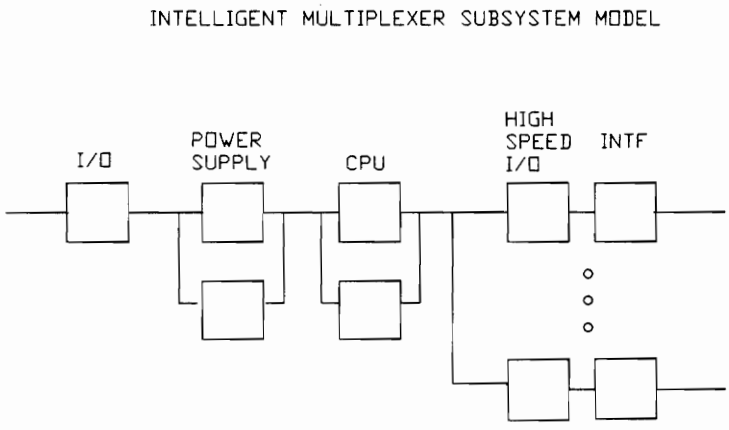


FIGURE 6 - CHANNEL BANK & INTELLIGENT MULTIPLEXER SUBSYSTEM MODEL

3.3.3.1 Fiber Optic Terminal (FOT)

Fiber optic terminals (FOT) are a special class of multiplexers. Fiber optic terminals are the lowest network device of the physical transmission network. A FOT that transmits data at 2.4 Gigabits per second supports over 32,000 voice grade or DS0 channels. A typical FOT has a Mean Time Between Outage (MTBO) in a 1:1 protected configuration of over 2 million hours.[17]

3.4 Transmission

Telecommunications and data communications systems in the United States support a hierarchy of transmission systems. These systems are broken into two major pieces (and service providers), the Local Exchange Carrier (LEC) and the InterExchange Carrier (IXC).

When considering diversity and survivability both LEC and IXC portions of the transmission path must be considered. The LEC potentially has worse availability than the IXC because of the differences in their architectures.

3.4.1 Local Exchange Carrier

Almost all domestic LECs support a tree-like architecture, as shown in Figure 7. The subscriber or user is served from a single end office. The end office provides feeder and distribution cable to the subscriber. [18] Historically this transmission facility consisted of copper facilities, but more recently, copper is being replaced by fiber optics. More feeder and distribution cable will be fiber in the future, though this is highly dependent on the cost of fiber waveguide and optical electronics.

As shown in Figure 8, the feeder and distribution facilities are bridge-tapped to provide service to the customer. It is intuitive that these facilities and the local end office are a major survivability issue. Most telecommunications and data communications users

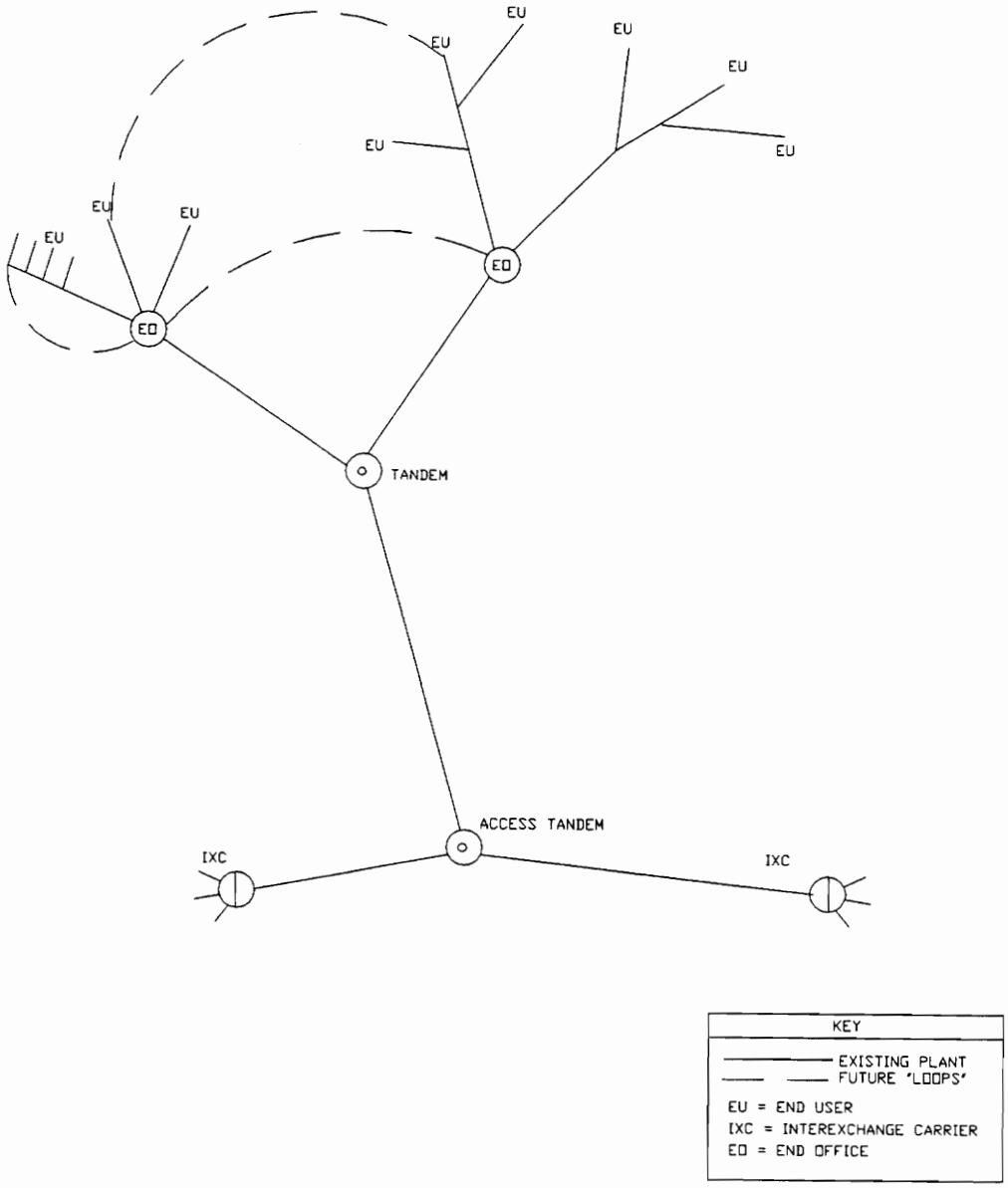


FIGURE 7 - TREE STRUCTURE OF LEC DISTRIBUTION

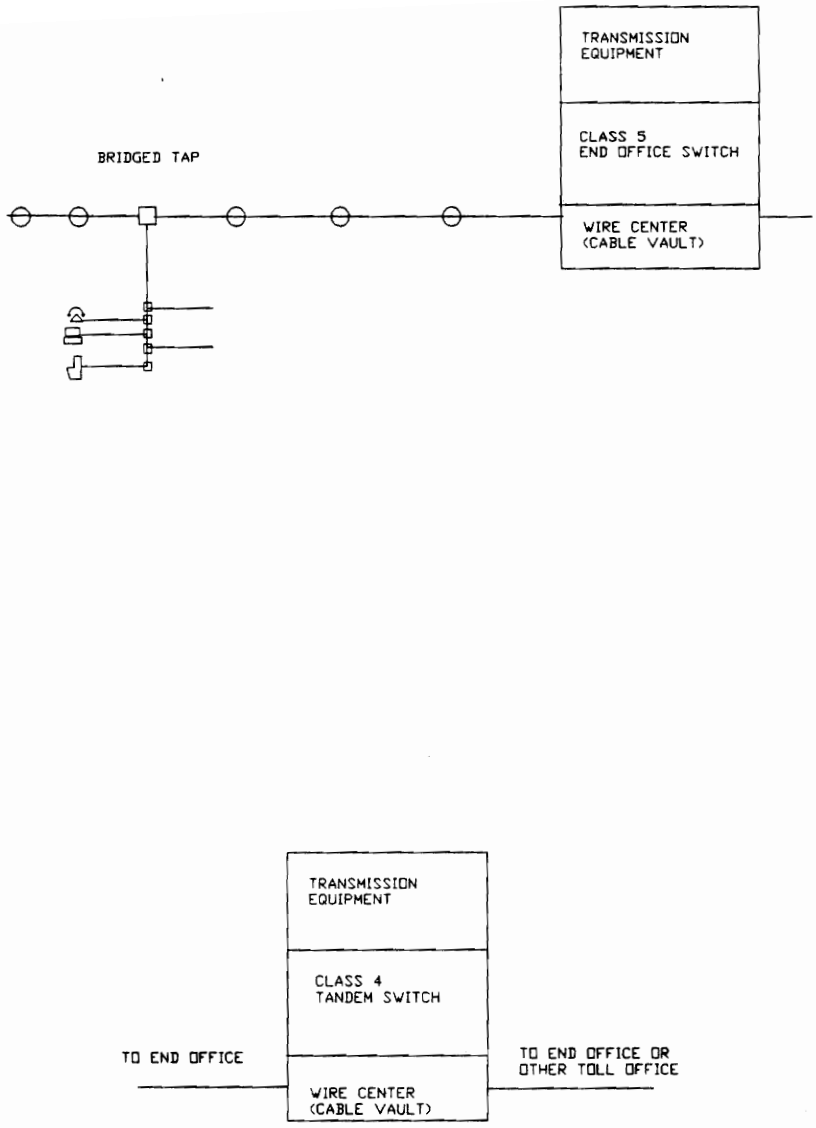


FIGURE 8 - END OFFICE AND TANDEM OFFICE CONFIGURATIONS

have no choice but to be served by a single end office.

The end office, or central office, usually supports a serving wire center, class 5 circuit switch, and other transmission equipment (see Figure 8). [19] This switch provides dial tone for telephony circuits and dial-up data communication users. It then provides digit translation and routes the call to the appropriate switch, either another end office switch or to a class 4 switch (tandem). Tandem or toll switches do not provide dial tone. They only switch traffic at very high speeds.

In the United States, the telecommunication system has been broken up into sections called LATAs (local area and transport areas). The LECs are restricted to providing only service within their predetermined LATA. They provide only intra-LATA service. The LECs are required to provide special access for a customer to the IXCs. This segregation of transmission facilities has increased competition in the long distance (IXC) market, but until recently has not stimulated competition in the LEC markets. One of the reasons is that the cost for LEC facilities (installation, right-of-way) is much higher since local service is provided to every subscriber. Pricing regulation of the LEC also limits the services the LEC can offer competitively.

3.4.1.1 LEC Architecture

Local transmission facilities, either switched or dedicated, are provided by the local exchange carrier (LEC). As shown in the previous section, the end office, serving wire center, and central office are critical single points of failure in network designs.

It is fortunate that most end office facilities are designed to be highly reliable. Unfortunately many of the end offices are sparsely connected to higher toll offices (this is because of traffic and economies). Though the probability of a complete failure of an end office is small, if the office fails the entire community of service of the end office fails. A

disastrous CO failure occurred on May 8, 1988 in Hindsdale, IL. The local CO (also a gateway to IXC traffic) caught fire and the 1AESS class 4 switch servicing 42,000 subscribers was destroyed. Many of these subscribers were without service for weeks. [20]

With this disastrous outage, many of the LECs and their customers have become more aware of the survivability issues of a single LEC service. Many LECs, seeing these issues as well as competition from alternative local carriers, are "closing" their tree-based local access with loops (see dotted lines on Figure 7). Many LECs are marketing survivability as a value added feature.

For this project, LEC-dedicated access transmission reliability is assumed to be 99.925%. This assumption is made for both switched and dedicated transmission. The user (corporation) is assumed to be served in a large city area which would be directly connected to the IXC (access CO). If this were not the case, then the transmission reliability would be worse for dedicated access and better for switched access because there would be diverse switched paths to traverse to the IXC.

3.4.1.2 LEC Switch Reliability

Bell Communications Research provides generic technical recommendations for the local Bell Operating Companies (BOCs) (all BOCs are LECs, but not vice versa) on what the reliability objectives of their switching systems should be. The BOCs do not publicly release reliability statistics and information nor do they tariff any reliability measures.

Table 2 lists several generic numbers that can be used to provide a basis for determining local access switch reliability. [21] These reliabilities are also shown in Figure 9. The worse case outage will cause a 28-minute outage which translates to a reliability of 99.995% for the LEC switch.

TABLE 2 - LEC SWITCH RELIABILITY MEASURES

Mean Time to Repair (MTTR) -	includes dispatch time and repair time = 4 hours (on site dispatch = 0 > MTTR = 2 hours).
Individual Line Down (ILD) -	28 minutes per year. This is due to hardware, software, and procedural errors in switch, not local access outside plant, etc. Results in loss of dial tone.
Simultaneous Line Down (SLD)-	15 minutes per year (worse case). This could be due to hardware, software, and procedural errors in switch, not in outside plant, etc. This number for 500-2000 line switch, performance better for larger switches.
Total System Down (TSD) -	3 minutes per year. Central office switches are designed to be highly redundant and reliable. There is very little probability of a hardware failure causing the complete loss of a switch. A more common problem with the more modern central offices (Stored Program Control Systems) is outages that occur due to software reloads. The worse case outage objective is for all cases.
Inter office trunk groups down -	20 minutes per year. This defines time down between CO switches. For switched access calls and trunks this is of little concern since there are usually many trunks to support the calls (120 or more trunks). This number can be also be applied to dedicated interoffice dedicated lines (i.e., T1, DS0).

Other disasters are possible such as fires, floods, earthquakes and are not covered by guidelines in the LSSGR.

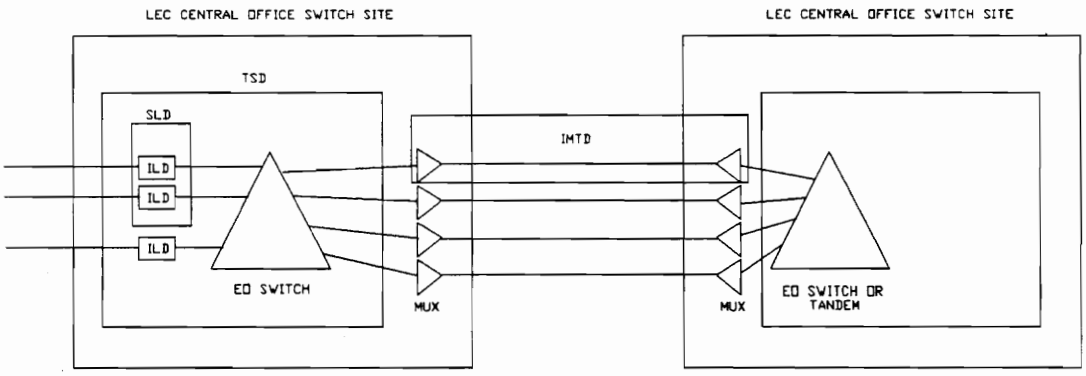


FIGURE 9 - LEC SWITCH RELIABILITY MODEL

Since the divestiture of AT&T in 1984, competition in the LEC market has slowly been increasing. Competition is primarily in large cities where large concentrations of business voice and data communication requirements exist. The competition has come from alternative carriers (also called bypass carriers). Because these carriers do not have the millions of dollars of installed copper facilities that the LECs have, bypass carriers usually provide transmission facilities that are fiber optic, coax cable (CATV), or digital microwave based. Some of the more prominent alternative local carriers and their serving cities are shown in Table 3.

Alternative local carriers usually design their networks with either multi-ring or tree topologies. The multi-ring has superior reliability, but is usually more costly and thus limits the service area of the carrier. Because of limited funding (usually investor-backed), these alternative local carriers are financially limited to servicing only buildings with large voice and data communication requirements. In time and as requirements grow, the alternative carriers will expand and service more users and eventually provide true competition in the local market. Typically, alternative local carriers with ring architectures and fiber optic transmission facilities support a NI to POP reliability of 99.995% or greater.

3.4.2 InterExchange Carriers

As described above, interexchange carriers (IXCs) provide transmission between LATAs. The three major interexchange carriers today are:

- o AT&T
- o MCI
- o US Sprint

TABLE 3 - ALTERNATIVE LOCAL CARRIERS

TABLE 3 - ALTERNATIVE LOCAL CARRIERS

Alternative Carrier	Service Area	Architecture
Institutional Communications Corporation	Washington, DC	Tree
Metropolitan Fiber Systems	Chicago, IL Houston, TX San Francisco, CA Minneapolis, MN Boston, MA Baltimore, MD Dallas, TX Pittsburgh, PA	Multi-Ring
Teleport	New York, NY Boston, MA San Francisco, CA	Multi-Ring
Diginet Communications	Milwaukee, WI New York, NY Chicago, IL	Tree
Eastern Telelogic	Philadelphia, PA	Hybrid
Intermedia Communications	Tampa, FL Miami, FL Orlando, FL	Ring
Bay Area Teleport	San Francisco, CA	Star (microwave)
LOCATE	New York, NY	Star (microwave)
Western Union, ATS	Many	Hybrid Ring

The interexchange carriers design their networks on efficient long-haul transmission systems. Past technologies have included copper, coaxial, microwave, and satellite services (see Figure 10).

Today all of the major long distance carriers are installing and converting their networks to digital and often fiber optic-based transmission because of the virtually limitless bandwidth and the economies it provides. Because of limited right-of-ways and limited diverse routes, conversion of existing transmission facilities to fully fiber optic systems can decrease reliability. Truly diverse routing of fiber systems are needed to ensure reliability.

Interexchange carriers publish their reliability measures. These measures are not guaranteed by the IXCs, but are objectives by which their quality can be compared and trouble circuits can be isolated. Table 4 shows a summary of carrier performance statistics. IXC POP-to-POP reliability of a single dedicated circuit is assumed to be 99.85%.

3.4.3 Transmission Systems

3.4.3.1 Analog Access

Analog transmission systems are typically used to carry voice traffic. As described in previous sections, they can also be used to transmit data, if used in conjunction with modems that modulate data to voice band frequencies. Analog transmission typically is provisioned on copper facilities, though analog microwave and satellite systems are still common. Analog data transmission speeds range from 300 bps to 38,000 bps.

Because of the inherent noise problems (crosstalk, impulse noise, distortion, etc.) and economics associated with analog transmission, the carriers (LEC and IXC) install most new services with digital equipment. Analog services are provided on digital facilities through analog-to-digital conversions in channel banks or multiplexing equipment.

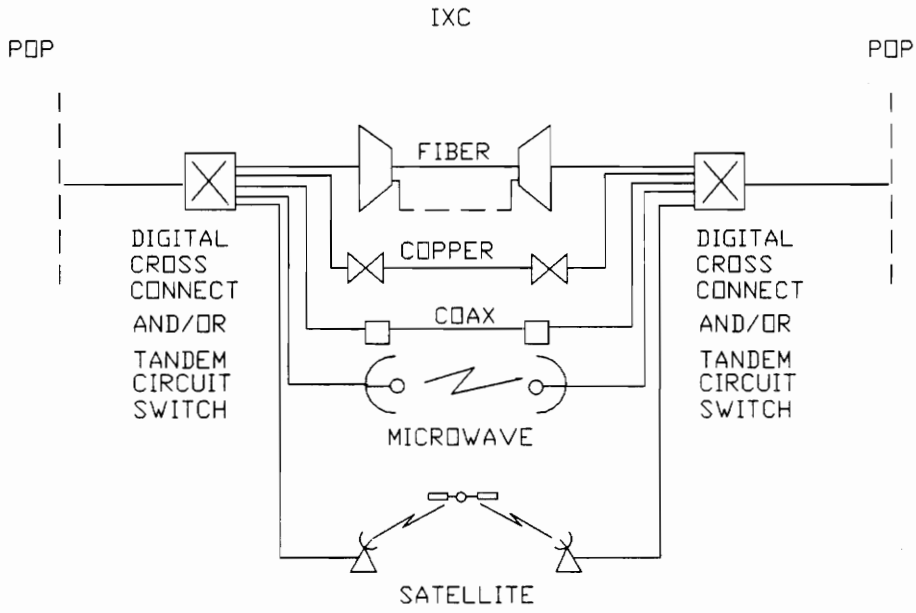


FIGURE 10 - INTEREXCHANGE CARRIER TRANSMISSION TECHNOLOGIES

TABLE 4 - CARRIER PERFORMANCE STATISTICS

SERVICE	REF. DOC.	AVAILIBILITY			ERROR FREE SEC.			SEVERLY ERROR SEC.			DELAY (MSEC)
		NI-NI	POP-POP	NI-POP	NI-NI	POP-POP	NI-POP	NI-NI	POP-POP	NI-POP	ABSOLUTE 1 WAY
AT&T DDS 56	PUB 62310	99.9%			99.5%						
AT&T ASDS 56	TARIFF	99.7%	99.85%	99.925%	99.79%	99.79%	99.875%	50	50	4	
AT&T ACCUNET T1.5	TR 62411	99.7%	99.85%	99.925%	96.80%				50	4	60
USS DS-0 SERVICE	FUND PLAN	99.7%	99.85%	99.925%	1E-05 (BER)						50 (80% OF TIME)
USS CLEARLINE DDS	FUND PLAN	99.7%	99.85%	99.925%	96.5%	99.00%	99.925%				
USS CLEARLINE 1.5	TP 10001	99.7%	99.85%	99.925%	96.5%	99.0%	98.75%	70			
USS DS-3	FUND PLAN		99.85%			99.9%(BURST EFS)			1E+08 (BER)		
ALT. LEC (ICI)	PROD. SPEC.			99.995%			99.50% (BER 1E+09)				

3.4.3.2 Digital Access

Digital circuits, in contrast to analog or voice grade circuits, provide transmission of information though binary 1 and 0 combinations.

Low speed digital offerings are available through digital data services (DDS). Digital access is presently available in the following speeds:

2,400 bits per second (bps)
4,800 bps
9,600 bps
14,400 bps (some)
19,200 bps (some)
56,000 bps
(some at 64,000 bps or 72,000 bps)

DDS is offered by the LECs and by many of the IXCs. In order to have a DDS circuit, the subscriber location must be served by the DDS-capable LEC central office. This means that the central office must be specially equipped to support clocking derived from the Bell Systems Reference Frequency Supply (BSRFS). This network synchronization ensures accurate, synchronized data transmission through the DDS networks.

3.4.3.3 High Speed Digital Transmission

Through advances in electronics, switching systems, and fiber optics, most carriers are in the process of converting analog transmission systems to digital systems. Digital systems have advantages over analog systems in that they are less prone to noise interference, are synchronized, and are more easily and economically multiplexed to higher rates. Figure 11 shows the North American digital hierarchy.[18] Figure 12 shows the newly proposed SONET international standards for synchronous optical multiplexing at higher rates.[22]

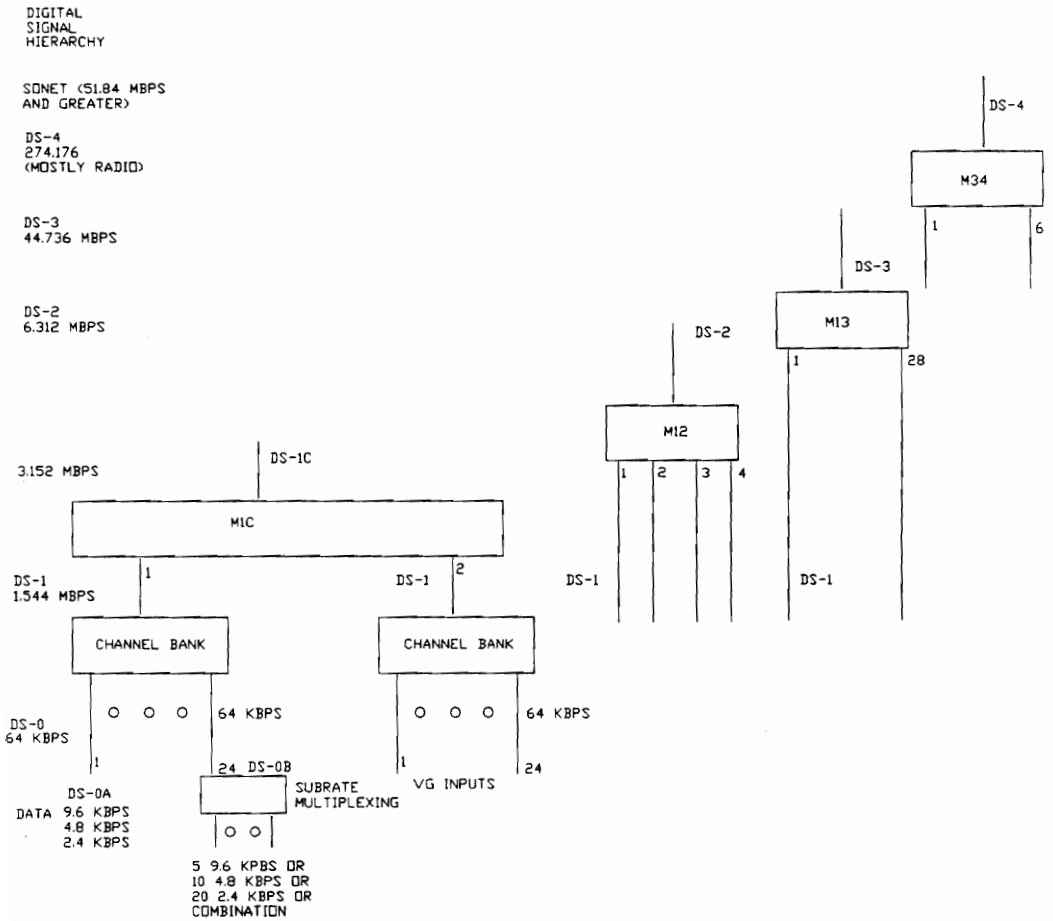


FIGURE 11 - NORTH AMERICAN DIGITAL HIERARCHY

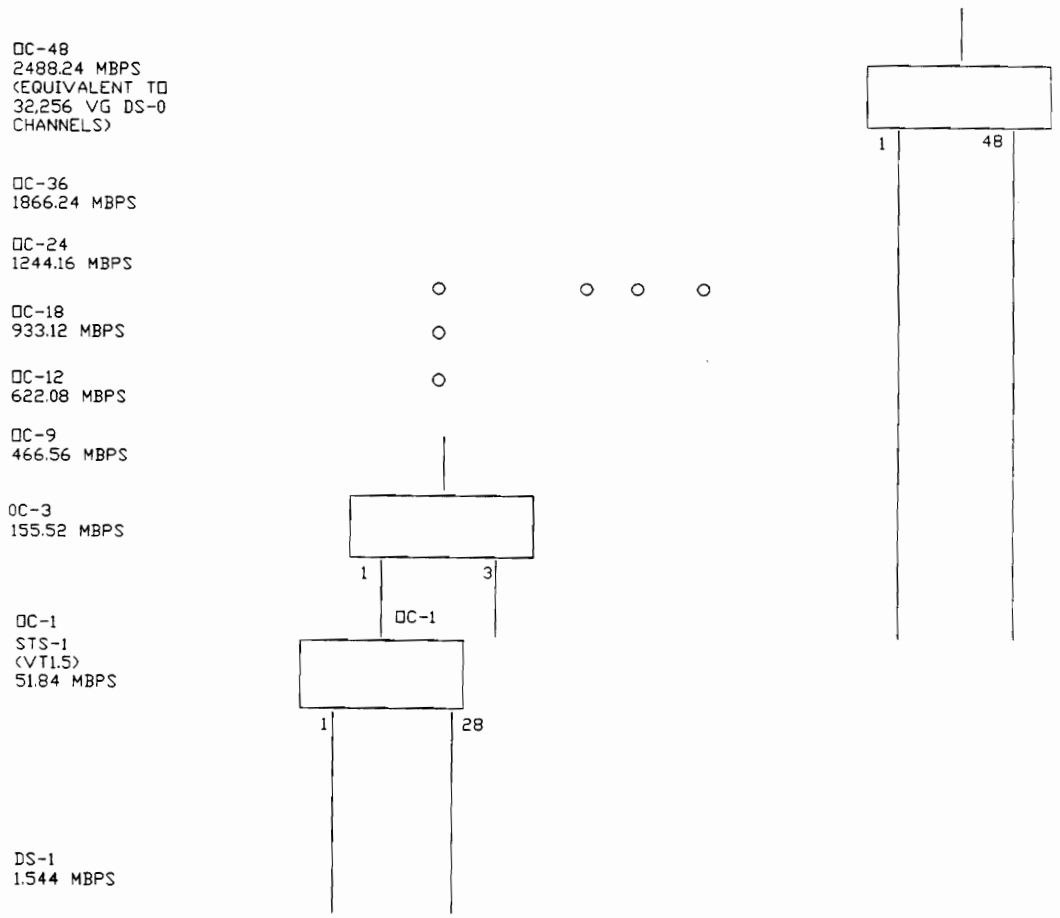


FIGURE 12 - SONET DIGITAL HIERARCHY

The disadvantage of these high rate multiplexing schemes is that they increase the impact of network failures. Loss of a single multiplexer has a greater impact on the overall network reliability than loss of a single channel. Highly robust and redundant transmission equipment is needed in order to maintain high network reliability.

3.4.3.4 Other Transmission Methods

Though not included in the modeling section of this report, the following sections describe other transmission methods that can be used to increase survivability and reliability in communications networks.

3.4.3.4.1 Microwave

One option to ensure diversity is the use of short-haul digital microwave systems, often referred to as bypass microwave systems. Microwave systems can support from one DS1 to DS4-level traffic. Long distance microwave systems are being used less because of superior fiber technology and because of maintenance required for long-haul microwave systems. However, short-haul systems are growing in popularity.[23, 24]

Some of the advantages to a short-haul microwave system are:

- Versatile (movable to other locations if necessary)
- Alternative CPE access
- Disaster recovery
- Alternative IXC access
- Simplistic installation and maintenance
- Fully redundant systems available
- High reliability/availability (99.910 - 99.997% dependent on location/rate rain fall per hour and other measures)
- Modular maintenance
- Avoids right-of-way issues associated with cable installations

Some of the disadvantage of microwave systems are:

- o Deep Fading transmission impairment caused by Multipath propagation, rain, or atmospherics.
- o FCC Licensing is required for all locations. If the system is leased, licensing is typically included in the installation. If the system is purchased, then the installer must pursue licensing.
- o Microwave systems have the appearance of being an inferior technology when contrasted to new fiber optic systems.

3.4.3.4.2 Switched 56 Kbps Data

Switched data provides switching of clear channel 56 Kbps (64 Kbps) data through intra and interlata networks. Switched 56 Kbps service can be used to access multiple locations and aid in disaster recovery.

Switched 56 is a tariffed offering that provides 56 Kbps switched digital service. Only AT&T and some LECs offer Switched 56 service, though other carriers are beginning to offer their versions of Switched 56.

Two types of access are possible with Switched 56 service, switched access and special (dedicated) access. These two methods are shown in Figure 13. For disaster recovery, switched access is preferred over dedicated access. This is intuitive as switched access has the ability to bypass some LEC failures.

Two transmission methods are available: Circuit Switched Digital Capacity (CSDC) developed by AT&T and DataPath developed by Northern Telecom Inc. A third method based on echo cancellation has been proposed by CCITT. Access and transmission methods used by the LECs and IXCs varies throughout the country. At present, Switched 56 data has not been a successful product. Only isolated islands, mainly in metropolitan areas, support any Switched 56 service. Switched 56 may evolve to ISDN (Integrated Services Digital Network) which offers digital packet switched and circuit switched services on existing copper transmission facilities.

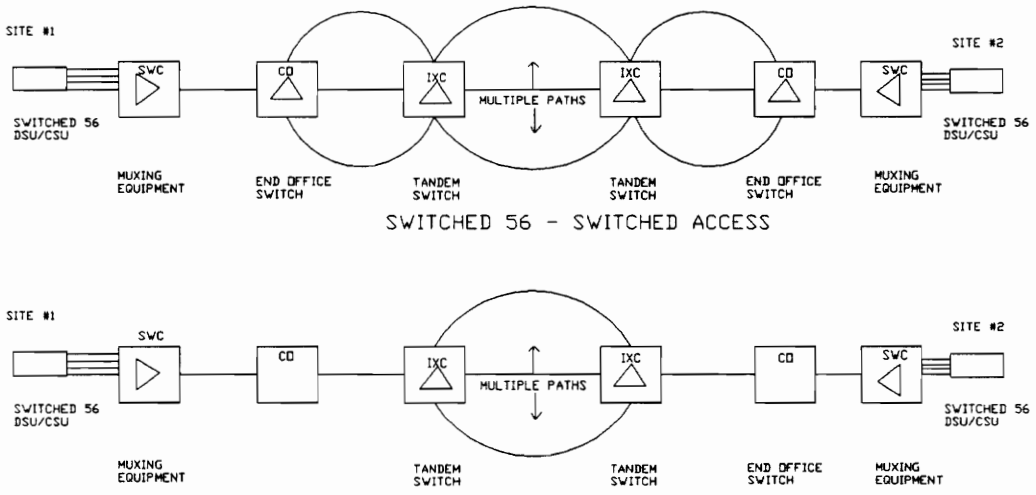


FIGURE 13 - SWITCHED 56 ACCESS

3.4.3.4.3 Switched T1 Data

Some carriers now offer high speed "near" switched digital T1 data. AT&T offers this service as a dedicated T1 offering that is available on a time/reservation basis. Under this ACCUNET Reserved tariff offering, a user must have dedicated DS1 tails to the nearest AT&T ACCUNET Reserved office. With 24-hour notice, AT&T will connect these two (or more for multidrop) locations at a specified time.

Emergency setup for disaster recovery is available; however, the minimum restoral time can be expected to be as great as 30 minutes. Many short duration outages are over in the time it may take AT&T to provide their restoral service. Another disadvantage of AT&T's offering is that it provides no protection from an outage in the local loop. The same local access is required (through the LEC) as for non-ACCUNET Reserved services.

3.4.3.4.4 Satellite

Other specialized backup transmission services are available today, such as GTE Spacenet's Certain T1. This offering is a backup, on-demand T1 and fractional T1 service. This service differs from AT&T's ACCUNET Reserved offering in that a Very Small Aperture Terminal (VSAT) earth station is located on the customer premise. Use of the VSAT transmission media provides for a true diversity, even in the local loop.

GTE's VSAT offering provides this economical, reserved system from the fact that users share pools of capacity on the satellites (transponders). In this configuration there is a probability that in a disaster where many users of the Certain T1 service are effected, there may not be enough capacity to meet the demand.

Even though GTE's offering is superior from a diversity perspective, it still has at least a 30-minute MTTR period (Mean-Time-To-Restore service - time to bring up satellite circuit).

3.4.4 Tariff Options

Today's communications networks and carriers, in general, do not offer a highly redundant transport service. Many of the smaller carriers cannot afford the capital expenditures required to ensure redundancy diversity of their network. For this reason, it is up to the network designer to attempt to assure maximum diversity when designing a network.

One way to increase diversity is through use of alternative carriers as previously described. Another way is to request special, diverse circuits from the LEC. Diversity from the LEC is often very difficult to obtain. All LECs (and some IXCs) will provide the user with a circuit layout record (CLR) or design layout record (DLR). These paper records show the exact facility routing that ordered circuits travel, including equipment, facilities, offices, and other information depending on the carrier. CLRs and DLRs are requested on the order form at the time the circuits are ordered and should be requested by all designers.

When requesting diverse LEC circuits, the network designer must specify what kind of diversity is being requested. Diversity and avoidance is tariffed by all the LECs. The definitions of diversity and avoidance are described below.[25]

- o Diversity: Two or more services must be provided over not more than two different physical routes.
- o Avoidance: A service must be provided on a route which avoids specified geographical locations.
- o Cable-only: Certain VG services are provided on cable-only facilities to meet particular needs of a customer.

3.5 Model for Network Reliability

The past sections have discussed the reliability modeling of equipment and transmission systems. This section will attempt to combine these subsystems into a model

to determine global network reliability.

Modeling network reliability requires understanding the complex relationships between three major factors: cost, capacity, and reliability. An ideal model would consider all three areas and optimize each, however, no comprehensive model exists today that can incorporate all three areas. The only option available to designers today is to design network reliability concentrating on one of the three major areas.

In this report, reliability was chosen to be the design factor of highest importance (over cost and capacity). A number of algorithms exist that can be used to determine reliability. Some of theses are discussed briefly, but are discarded due to their limitations. The factoring theorem was chosen to model reliability because of its versatility (edge and vertex reliability), however, it too has limitations.

3.5.1 Network Terminology

Networks are composed of equipment and transmission lines. In analytical terminology, equipment is called nodes or *vertices* (v) and transmission lines called arcs or *edges* (e). The *set of vertices* in a particular graph (G) is notated as V. Likewise, the *set of edges* in graph G is notated as E. Two vertices are given special notations, they are the *source vertex* (s) and the *termination vertex* (t). The entire network is called a *graph* (G) and is composed of n vertices and m edges.

When all the vertices in a graph can communicate with each other, then the graph is termed *connected.* If for any reason one vertex of the graph is isolated or cannot talk to every other vertex in the graph, then the graph is termed *disconnected.*

Graphs can be further defined as either *directed* or *undirected. Directed* graphs allow traffic to pass in one direction (unidirectional or simplex). *Undirected* graphs allow traffic to pass in both directions (duplex). Figure 14 shows an undirected and a directed

graph.

A *subgraph* is a portion of a graph. Subgraphs are often used in *series-parallel reductions* (to be covered later in this section) that attempt to simplify a complex network.

A *spanning tree* is a connected subset of a network that contains all the vertices of the network and a set of edges of the network so there is exactly one path between any vertex. Not all edges in graph G need be included in a spanning tree. Spanning trees (and graphs) can be assigned weights by placing numbers on the edges that represent capacity or throughput. The *minimum spanning tree* is the tree that has the lowest total weight of all the spanning trees of the network.

A *cut* results when one or more edges are removed. A *cutset* is a set of edges that if removed from the graph will disconnect the graph (one vertex cannot communicate to another). The *minimum cut* is the cutset of edge that has the lowest total weight. A *minimal cut* is a cut that reconnects the graph if any of its edges are replaced.

The *degree* of a vertex is equal to the number of edges that terminate (or originate) on the vertex. A vertex is *adjacent* to another vertex if the same edge terminates on both vertices. [26]

3.5.2 Classes of Network Problems

It is appropriate to classify the complexity of reliability problems. The scheme chosen relates network size to the computational time required to calculate reliability. Through simple series and parallel reliability models, we learned that these models produce reliability equations that can be solved by polynomial algorithms. Polynomial algorithms can generate solutions to problems in a period of time proportional to a polynomial function of the size of the problem. These problems are termed complexity type P. A second

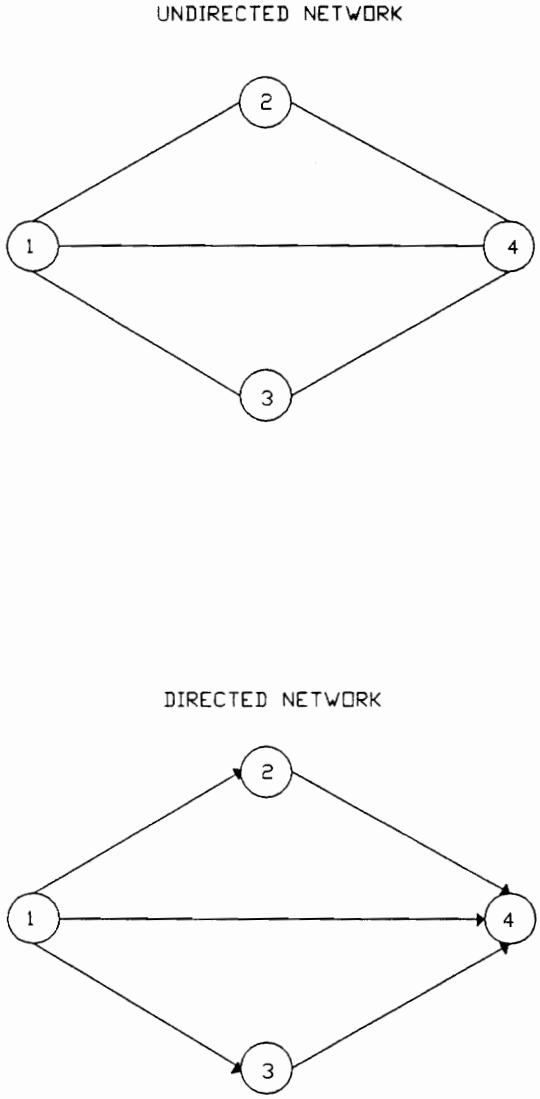


FIGURE 14 - UNDIRECTED AND DIRECTED GRAPHS

category of problems is complexity class NP. NP problems can be shown to satisfy a certain property (i.e., determining whether graph is connected or not) in polynomial time. It is much easier to test a problem for a property than to solve the problem (NP problems are easier than P problems). Another category of problem classes is called NP-complete. This class of problems is defined such that if a polynomial algorithm exists for these problems then one exists for all problems of the class NP. No polynomial time algorithm exists (to date) to solve these types of problems. NP-hard problems refer to the class of problems that are at least as hard as the NP-complete problems. Ball in [6] shows that reliability problems are of class NP-hard.

When solving for network reliability there are a few common measures that can be used. The most general is the K-terminal problem, where there is a source vertex s such that there are paths to every vertex in set of vertices (K). A more specific problem is the 2-terminal problem (where K = 2). This problem investigates the probability that there exists a path between 2 vertices, s and t. A third network reliability problem is the all-terminal reliability, where reliability is calculated such that all terminals have paths to all other terminals (K = all). [6]

3.5.3 Reliability Algorithms

Algorithms, step-by-step procedures, are used to simplify the network or the calculations required to either find exact or approximate reliability. There are many different algorithms that can be used to determine or estimate reliability. Some of the algorithms are discussed below.

Monte Carlo algorithms are used to approximate reliability of vertices and edges of a network. It takes samples of network reliability and computes approximate reliability and upper/lower bounds on reliability.

Markov chains are state-space analysis techniques that can be used to model the reliability of a network based on the states that the network takes (failed, being repaired, fault detected, working, partially working, etc.). The Markov chain process is best used when a small number components are in the network or when exact state analysis is needed (e.g., hardware component or software module reliability analysis).

Mincut or minpath algorithms compute the minimum cutset or pathset for a given network then determine reliability polynomials for the graph. The system will fail only if all the components in the minimum cut fail. These algorithms result in a polynomial with 2^r-1 terms in the reliability polynomial. These types of problems lead to further analysis on the complexity of the problem (can large network reliability be solved at all). Enumeration or counting problems determine the complexity of the problem by counting number of pathsets or cutsets.

The factoring theorem uses series-parallel reductions to simplify the graph and then removes the links (edges) of the graph to simulate the random failure properties of the links. In this project the factoring theorem was chosen because of the extensive literature written on the process and the availability of software to run both undirected and directed network reliability scenarios.

3.5.3.1 Factoring Theorem

The factoring theorem is a recursive algorithm that involves graph simplification through reduction then removal of edges to determine network reliability.

The basic graph reduction techniques used for undirected graphs are:

- 1-degree reduction
- 2-degree reduction
- Parallel reduction

A 1-degree reduction removes any vertex that has a degree of one (single edge

to/from network). This vertex does not contribute to the available paths of the network thus is not considered in the application of factoring theorem.

A 2-degree reduction (or series) and parallel reductions are shown in Figure 15. In a 2-degree reduction, a vertex with degree two (two edges to/from graph) can be reduced (under the assumption of no vertex failures in an undirected graph) to single edge. In a parallel reduction, two edges are reduced to a single edge. There are other reduction methods than can be used to simplify the network, but the series-parallel reductions described above are the most common. The purpose of graph reduction is to simplify the application of the factoring theorem.

Once the graph is reduced as much as it can be, the factoring theorem is applied. The theorem is listed below:

$$Rel(G) = p\ Rel(G_e) + (1-p)\ Rel(G_{-e})$$

where : G = an undirected network composed of a set of vertices and a set of edged G=(V,E).

Rel()= the reliability of graph ().

p = the reliaibility of edge e.

G_e = subgraph of G obtained when the edge e is *deleted* (vertex u and v remain).

G_{-e} = subgraph obtained when e is *collapsed* (vertex u and v are combined into a single "supervertex").[5]

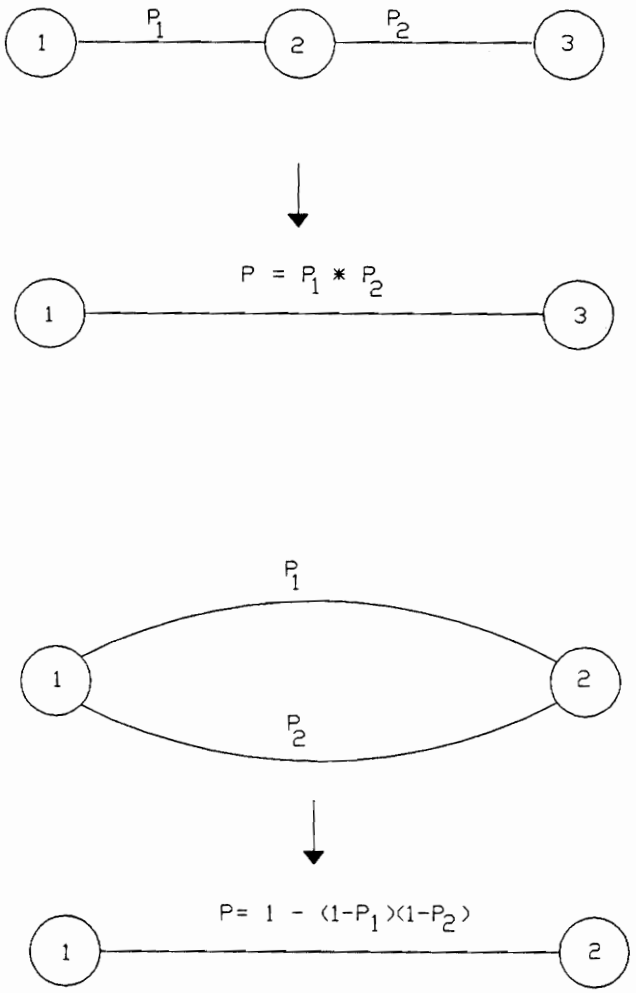


FIGURE 15 - 2-DEGREE AND PARALLEL REDUCTIONS

In the application of the factoring theorem, an edge e is selected from the set of edges in the graph (E). This edge is deleted from the original graph G, creating a subgraph G_e. When e is *deleted*, the two vertices that e originally connected remain as part of the graph. An example of edge deletion is seen in Figure 16 if P_1 were deleted. In this case vertex 1 and 2 remain, but vertex 2 would be of degree one (single connection P_2).

When edge e is *collapsed*, not only is edge e removed, but the edges that were on the two connecting vertices (1 and 2) are terminated on a supervertex. Again a new subgraph of the original G is formed. Edge deletion and collapse is analogous to short and shunt analysis applied to electrical circuits in analysis of electronic networks.

Factoring theorem is applied for every edge in network, but only for one edge at a time. Reduction of the network occurs before, during, and after application of the factoring theorem. The graph reliability is the result of this algorithm. The total number (enumeration) of edge states or number of times the factoring theorem may have to be applied is 2^m states (where the number of edges in G is m).

For directed graphs, a similar application of the factoring theorem is used. However, because the graph is directed, more care is need when applying reduction techniques. The reliability of the original graph must not be effected by the reductions. 2-degree and parallel reductions can occur for specific edge-vertex configurations as well as special 1-degree and directed reductions (see Figure 17).

3.5.4 Simulation of IXC Network - Undirected Graph

The carrier network reliability was calculated by applying the factoring theorem algorithm. A computer program, Reduce&Factor, developed by L.B. Page and J. E. Perry at North Carolina State University was used to apply the factoring theorem to undirected and directed networks.[27]

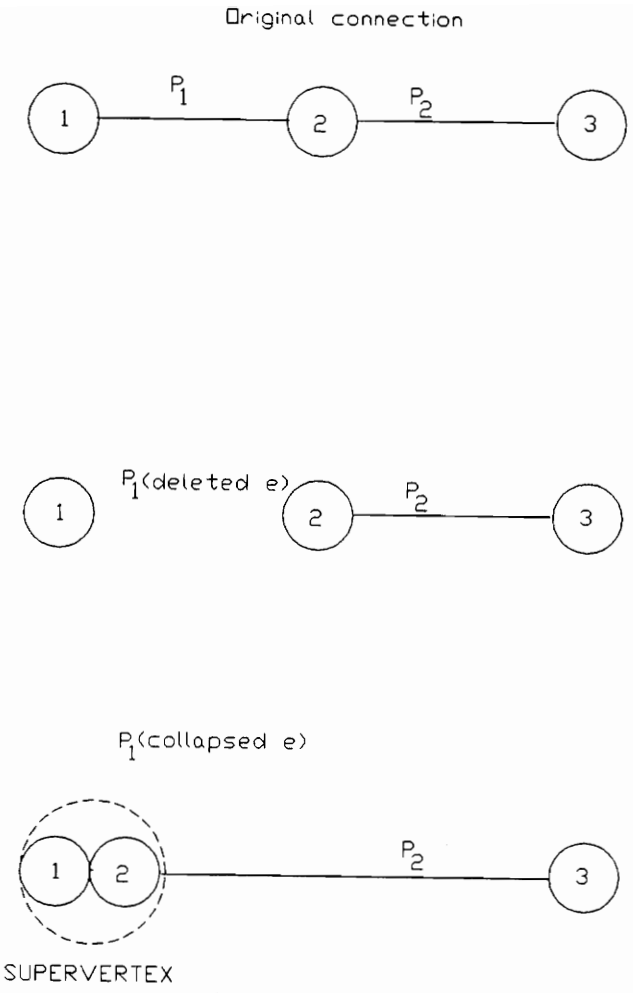


FIGURE 16 - EDGE DELETION AND EDGE COLLAPSE

The first application of the factoring theorem to simulate a carrier (POP-POP) network was done using the undirected graph version of the Reduce&Factor program. The network initially simulated was a 4x4 fully meshed network as shown in the upper half of Figure 18. A symmetrical, fully meshed network was used to represent a typical IXC network because it can approximate the reliability of any vertex to any vertex reliability independent of the s-t vertex locations. A non-symmetrical architecture would require reliability to be calculated for all s-t vertex pairs, then the reliabilities would have to be averaged or the worse case chosen to approximate global network reliability.

A POP-to-POP edge reliability of 99.85% from Table 5 (IXC reliability) was used. The program, results shown in Appendix D, computed a s-t reliability of 99.9999999323...%. The undirected graph reliability does not consider node (vertex) failure. To further refine this model and to incorporate vertex failure, a directed graph version of the factoring theorem program was used. In order to use this program, the undirected graph in the upper half of Figure 18 was converted to a directed graph.

3.5.4.1 Undirected to Directed Graph Conversion

The algorithm to convert an undirected graph to a directed graph with vertex to edge conversion, while still maintaining the reliability measures of the graph is listed below. It should be noted that this algorithm provided undirected to directed graph conversion, but no algorithm is known to go from directed to undirected. [26]

1. Each vertex is replaced by a pair of vertices (e.g., vertex u to vertices u and u+n {where n is the number of vertices in the initial undirected graph}).

2. A directed edge is placed from vertex u to u+n.

3. If vertex u was connected to vertex v in the undirected graph, the vertex u+n is connected to v in the directed graph. The direction of this new edge is from u+n to v.

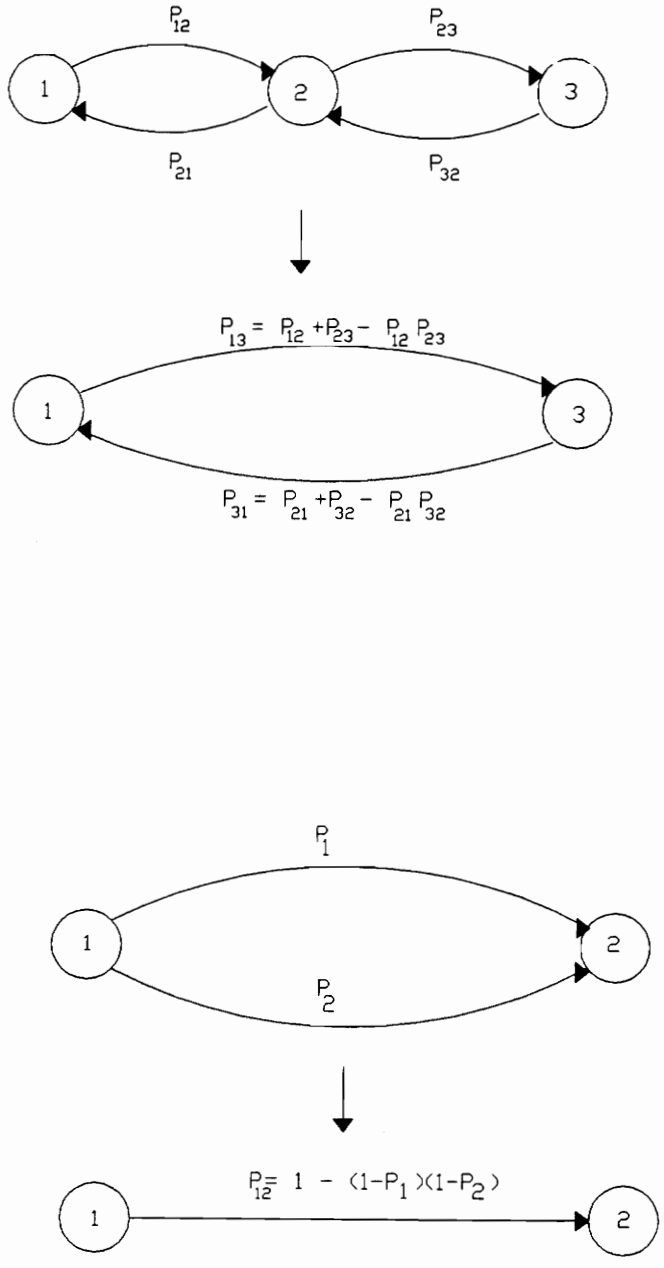


FIGURE 17 - DIRECTED 2-DEGREE AND PARALLEL REDUCTIONS

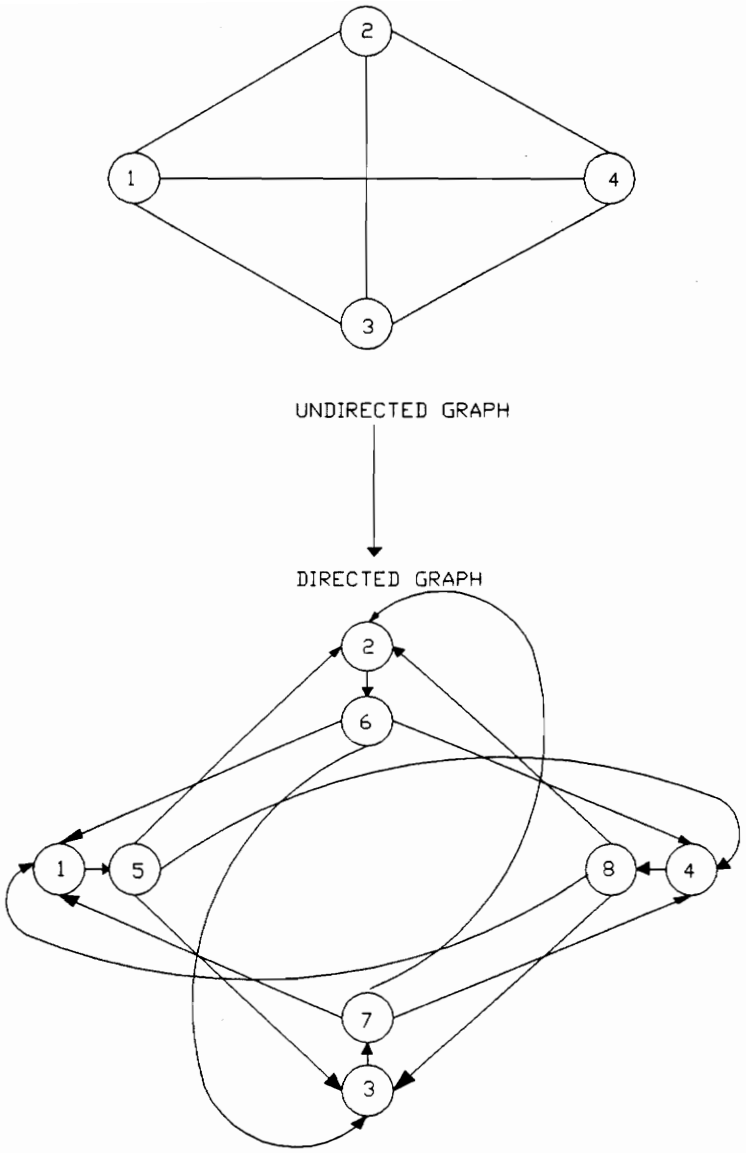


FIGURE 18 - UNDIRECTED AND DIRECTED 4X4 MESHED NETWORKS

4. In the final directed graph, all incoming edges should be attached to u and all outgoing edges should be attached to u+n (except the u to u+n edge).

3.5.5 Simulation of IXC Network - Directed Graph

Applying the undirected to directed graph conversion to the 4x4 fully meshed IXC produced a directed graph that was used to simulate the carrier reliability (see lower half of Figure 18). The transformation was done to simulate not only edge failures, but also vertex failures. Vertex reliability is incorporated into the graph by assigning the vertex reliability to the edge between u and u+n vertices. This vertex was transformed into a very short edge.

Using the directed graph program, also developed by Page and Perry, IXC network reliability was computed. [28] For an edge reliability of 99.85% and a transformed vertex reliability of 99.9966% (packet switch vertex), the resulting s-t reliability was computed to be 99.9966...%.

It should be noted that the output in Appendix D shows that the transformed edge reliability is 1.0000 not 0.999966 as was input. This is because the output program rounds off to only four significant digits. The value 0.999966 was input and used in computations. Reliability is calculated in the program using extended integer variables with 80 bit representations.

The same network was input to the program using an intelligent mux as the switching device, not a packet switch as had been done previously. The results of the computations with an edge reliability of 99.85% and a transformed vertex reliability of 99.9834% was an s-t reliability of 99.9834...%.

3.5.6 End-to-End Reliability

The components of the general communication model have been analyzed and their reliabilities calculated. The components are combined to form models of communication

networks. Figure 19 shows the various different models used to calculate end-to-end reliability. As seen in the figure, equipment, access methods, and IXC networks were varied to model different types of networks. The results of these models are listed in Table 6 in Section 4, Results.

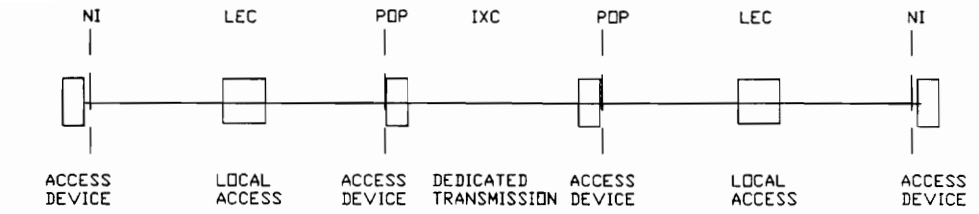
Model #1 shows a dedicated access network with a dedicated IXC network (no switching). This type of network represents a typical clear channel network that "nails up" or dedicates a channel through the network. It is the least reliable network because it has no ability to reroute traffic.

Model #2 shows a dedicated network with some IXC switching capabilities. In this model calculations were done for modem, DSU/CSU, and DSU with channel bank access devices. Both packet switched and IMUX IXC network calculations were done. The DSU with channel bank configuration was calculated because many IXC carriers use DS-1transmission facilities for access. Using modems with channel banks provided no increase in reliability, since modems would still be needed at the channel bank side of the circuit (DSU built into the channel bank).

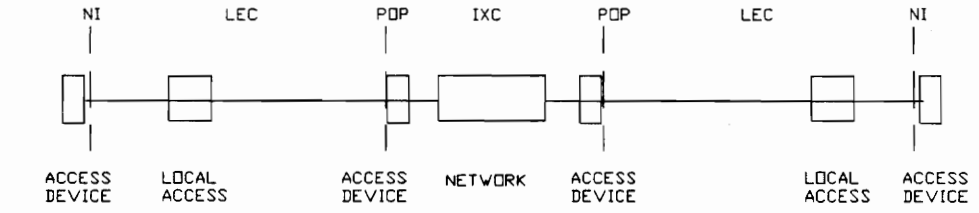
Model #3 is similar to model #2 except that the access method is switched access as opposed to dedicated access as used in model #2. This model simulates a network where the user dials into the network through a dial-up modem.

Model #4 incorporates model #2's dedicated access with a secondary diverse alternative local access carrier. This model assumes that the customer device (host/terminal) and the IXC network have the intelligence to switch to either the LEC dedicated access line or the alternative local access carrier line.

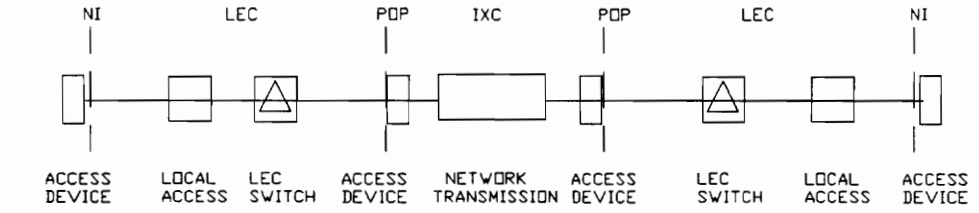
Model #5 incorporates the alternative local carrier of model #4 as well as an alternative IXC carrier. This model assumes that the customer device (host/terminal) has



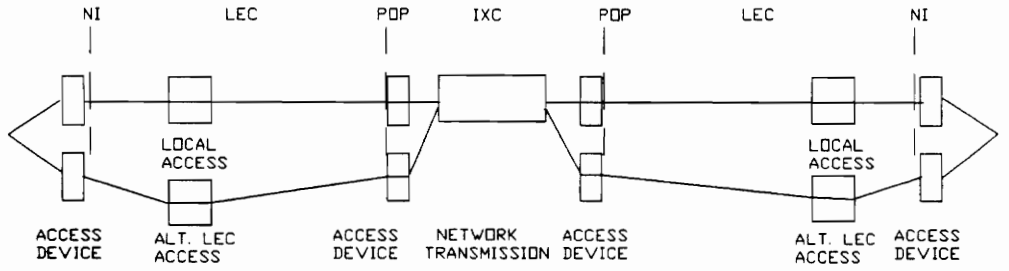
MODEL #1 - DEDICATED ACCESS, DEDICATED TRANSMISSION



MODEL #2 - DEDICATED ACCESS, NETWORK

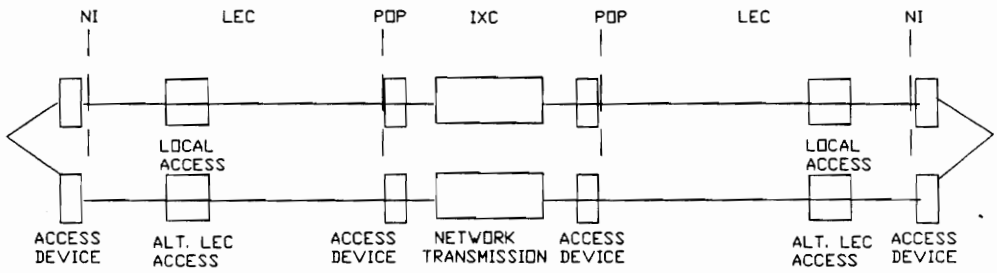


MODEL #3 - SWITCHED ACCESS, NETWORK

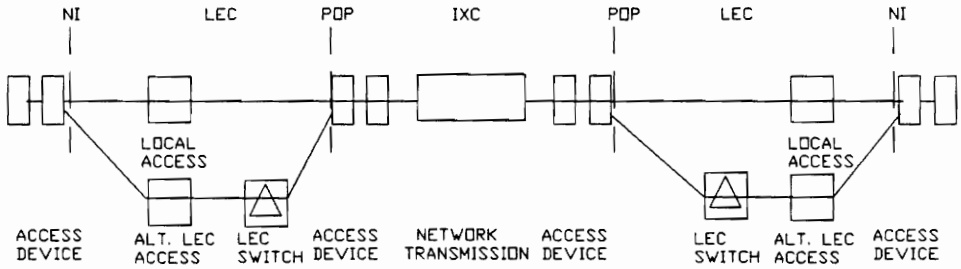


MODEL #4 - DEDICATED ACCESS - ALT. ACCESS, NETWORK

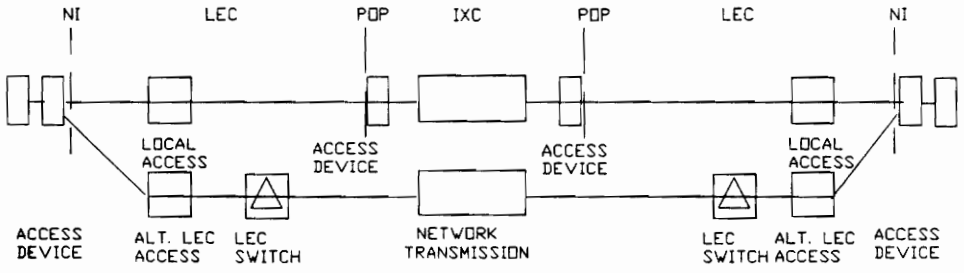
FIGURE 19 - END-TO-END RELIABILITY MODELS



MODEL #5 - DEDICATED ACCESS - ALT. ACCESS, ALT. NETWORK



MODEL #6 - DEDICATED ACCESS - DIAL BACKUP



MODEL #7 - DEDICATED ACCESS, DIAL BACKUP NETWORK

FIGURE 19 - END-TO-END RELIABILITY MODELS (CONT'D)

the intelligence to switch between the two transport methods.

Model #6 represents a dedicated access network as in model #2, but adds dial backup capabilities to the local access portion of the model. Since digital (DSU) dial backup capabilities are not universally available, only analog (modem) access equipment was modeled.

Model #7 uses a network similar to model #6 except that in this model dial backup is allowed through a separate IXC network. The dial backup IXC network is assumed to have the same reliability as the IXC packet network (for both the packet and IMUX cases).

4.0 Results

4.1 Equipment Reliability

The equipment components of the communications network were determined and analyzed. The three device types investigated were access, switching, and concentration/multiplexing equipment. The reliabilities were calculated or determined for these device types and are summarized in Table 5.

4.2 Transmission Reliability

The transmission components of the communications network were determined and analyzed. LEC, alternative LEC, and IXC transmission systems were analyzed and reliabilities were determined. A summary of transmission reliabilities were shown in Table 4 of Section 3.4.2.

4.3 Modeling Results

The IXC network was modeled using a factoring theorem algorithm computer program. A 4x4 vertex network was modeled using an undirected network representation for the IXC network. Next a directed network model was used. The directed network model presented a more realistic model because it included vertex as well as edge failures. Models were determined for packet and intelligent multiplexer IXC networks.

Having determined both equipment and transmission reliabilities, the end-to-end model was calculated. Reliability for various access equipment types, access methods, and IXC networks were computed. The end-to-end results are summarized in Table 6.

TABLE 5 - EQUIPMENT RELIABILITY SUMMARY

Equipment	HW MTBF(hours)	p (MTTR = 7 hours)
Modem	30,000	0.999767
Dial Backup Unit	50,000	0.999860
DSU/CSU	50,000	0.999860
Packet Switch (redundant)	205,877	0.999966
Concentrator	6,133	0.998860
CSU (D4 - 1.544 Mbps)	60,000	0.999883
Intelligent Mux (redundant)	42,162	0.999834
Channel Bank	199,995	0.999965
M13 (non-redundant)	82,000	0.999915
M13 (redundant)	3.6 M	0.999998

TABLE 6 -END-TO-END MODEL SUMMARY

Model #	Access Device	IXC Network	p_{sys}
1	Modem	Dedicated	0.996074
1	DSU	Dedicated	0.996445
1	DSU-channel bank	Dedicated	0.996421
2	Modem	Packet	0.997536
2	Modem	IMUX	0.997405
2	DSU	Packet	0.997908
2	DSU	IMUX	0.997776
2	DSU-channel bank	Packet	0.997884
2	DSU-channel bank	IMUX	0.997752
3	Modem	Packet	0.997437
3	Modem	IMUX	0.997305
4	Modem	Packet	0.999964
4	Modem	IMUX	0.999832
4	DSU	Packet	0.999864
4	DSU	IMUX	0.999832
5	Modem	Packet	0.999997
5	Modem	IMUX	0.999997
5	DSU	Packet	0.999999
5	DSU	IMUX	0.999998
6	Modem	Packet	0.999218
6	Modem	IMUX	0.999886
7	Modem	Packet/packet	0.999251
7	Modem	IMUX/packet	0.999251

Dedicated IXC network reliability = 99.85%
Packet IXC network reliability = 99.9966%
IMUX IXC network reliability = 99.9834%

5.0 Discussion

5.1 Discussion of the Results

In modeling the IXC packet and IMUX networks, the fact that the vertices were fully connected resulted in a high reliability for the network. The reliability of the IXC network became dependent on the vertex equipment (packet switch and IMUX) and less dependent on the transmission facilities and the network connectivity.

The end-to-end modeling verified some intuitive hypotheses. The end-to-end modeling showed that use of any IXC network (packet or IMUX) resulted in superior reliability over a dedicated IXC network (switching increases reliability). In general, a packet switching IXC network was more reliable than an IMUX IXC network because the reliability of the packet switch was higher. Intuitively packet switching has greater reliability because of its addressing/switching capabilities and because of the greater number of input/output lines (n=10). Digital transmission (DSU access device), because of its simplicity, was more reliable than analog transmission (modem access). Channel bank access was slightly less reliable than DSU access because of the increased equipment required. In reality this may not be true as the LEC often uses a channel bank to multiplex and demultiplex DSU-DSU circuits. If the LEC did use this additional equipment, then the 99.925% reliability assumed for DSU-DSU circuits would not be a correct assumption.

Switched access had a lower reliability than dedicated access because more equipment (switch) increased the failure potential. This however can vary based on the actual LEC network. In some cases (e.g., when user is far from LEC-IXC access point), switched access may be more reliable because the LEC has a network between the customer and the IXC. In this case the LEC's network could be modeled like IXC network using factoring theorem.

Another result from the end-to-end modeling was that dial backup increases reliability the greatest when used to backup the entire network, not just the local access portion of the network.

5.2 Deficiencies in the Model

One of the deficiencies with this project was that the existing algorithms could not incorporate the multivariables required to properly calculate reliability. The factoring theorem algorithm was flexible in that by converting from undirected to directed graph, vertex reliability could be considered. However, other measures of reliability must be considered in order to obtain a more realistic model.

In the packet switching environment, delay is a critical measure of reliability. Because packet switching adheres closely to the M/M/1 queuing model (Markov arrival, Markov service, single server), delay is closely tied to the available line capacity. Delay, when it becomes extensive, directly impacts the availability and thus the reliability of the line. This is shown in the delay equation below: [26]

$$T = \frac{1}{\mu C - \lambda} \qquad (14)$$

where λ = arrival rate
μ = service rate
C = available line capacity
T = transmission delay

As seen above, transmission delay goes to infinity as the line capacity goes to zero . The availability goes to zero as the delay goes to infinity.

For dedicated networks, such as in the intelligent multiplexer network that was also computed, capacity is even more critical as availability is directly related to available bandwidth to reroute traffic. If line capacity is not present and no queuing occurs, then the customer availability is zero. The only way that the factoring theorem is applicable to

calculating reliability is if the network has no, or very little traffic on it (which is not practical).

One addition that might be included in future research would be to modify the factoring theorem to incorporate capacity constraints. One implementation of capacity might be to allow multiple edges between vertices representing available capacity. Failure of these edges could simulate lost capacity in the network. However, multiple edge failures would have to occur and this violates one of the assumptions of the factoring theorem.

Some of the minimum path algorithms consider capacity in reliability calculations. One example of a minpath algorithm is shown in reference 29. However, these algorithms are limited because they cover specific network types and models (directed graphs, with no directed loops).

The reliability models presented in this project did not consider network cost. Additional algorithms have been developed that specifically address the inverse relationships between network cost and network reliability. These algorithms become optimization algorithms that optimize both cost and reliability, or one or the other based on an expected performance level. Unfortunately many of these cost /reliability algorithms are missing other critical reliability factors such as delay and vertex failure.

5.3 Validity of Reliability Numbers

Because the results are highly sensative to the equipment reliability (see packet or IMUX example), consistent calculations are required to produce accurate results. Though standards were used to calculate the MTBF numbers (MIL-HDBK-217 and Bellcore specifications), there seems to be some discrepancies in the manufacture's published results. For example, one manufacturer stated that the MTBF for a Channel Service Unit (CSU) was 60,000 hours, however, another manufacturer stated its CSU had an MTFB of

over 400,000 hours. It is true that there were differences in the CSUs, but not so vast differences to be almost an order of magnitude difference in MTBF. This discrepancy can only be explained by inaccurate application of the standards or use of different assumptions during calculations.

LEC and IXC numbers are suspect too, as they are averages and may not be applicable to the availability of an individual line.

5.4 Failure Mode and Effect Analysis

Another deficiency in this project was in considering the impact of particular outages. For example, the failure of a single modem has less impact on a computer network than does the loss of a channel bank or even loss of a carrier. To illustrate the impact beyond the analytical analysis presented requires a Failure Mode and Effect Analysis of the communications system. This FEMA is shown in Table 7.

The FEMA is a more subjective approach to systems analysis of network reliability. The table shows which components potentially have the greatest impact on reliability. As shown in Table 7, the largest impact area is transmission (lowest MTBF, highest lines effected).

5.5 Software Reliability

Equipment and transmission facilities are becoming more intelligent (i.e., from channel bank to intelligent multiplexer). Technology complexity is decreasing with respect to hardware and increasing with respect to software. This is because software is much more flexible than hardware and provides more opportunity to incorporate features. Because of this increase in software, software reliability is beginning to have an impact on equipment and transmission performance.

Software failures can be categorized in two ways; software failures due to hardware

TABLE 7 - FEMA OF A COMMUNICATIONS NETWORK

Failure Mode	Maximum Number of Lines Effected (DS0 channels)	Mean Time Between Failure (MTBF)	Possible action to avoid failure or increase MTBF
EQUIPMENT			
Loss of Modem	1	30000	Dial backup, modem sparing
Loss of IMux	>24	42000	Redundancy or spare
Loss of High Order Mux (M13)	672	82000	Redundancy [MTBF 3.6 M hours]
Loss of FOT (2.4 Gbps, OC-48) and fiber	32256	2M (MTBO)	Alternative transmission equipment
TRANSMISSION			
Loss of Dedicated Access Line	1	5329 *	Alternative Carrier/dial backup
Loss of IXC	>10000	2663 **	Alternate IXC
Loss of LEC (switch access)	>2000	80000 ***	Alternative Carrier /Bypass System

* Assumes 4 hour MTTR with circuit availability of 99.925%
** Assumes 4 hour MTTR with circuit availability of 99.85%
*** Assumes 4 hour MTTR with switch availability of 99.995%

and software failures due to faulty code. Hardware-instigated software failures may result from failed hardware (such as memory hardware) or from outside influence on hardware (such as electromagnetic interference [EMI]) that disrupts or corrupts software or firmware. Software failures due to faulty code are typically "bugs" in the software that were not located in the test period of the product life cycle.

Software reliability of equipment and transmission facilities can be increased by:

- Including software error checking such as Cyclic Redundancy Checking (CRC) and checksum calculations.
- Designing equipment with automatic software reload capabilities.
- Thorough testing of software from predesigned software test plans to locate and isolate software 'bugs' during the development portion of the systems life cycle.

Future reliability models must consider software reliability as an integral component of the system.

6.0 Conclusion

This report presented large data network reliability from both practical and theoretical perspectives. The componets of a data communications network were described and reliabilities determined. These components were assembled into comprehensive models and their end-to-end reliaibilty was determined.

Some of the conclusions that can be drawn from this project and report about data communications network reliability and reliability modeling are:

- o Both practical and theoretical concepts must be considered when modeling reliaiblity.
- o Networks, that are highly connected, have a high reliability. The network reliability becomes dependent on the reliability of the switching devices.
- o End-to-end reliability can be greatly increased by using alternative local and alternative IXC carriers for diversity and survivability.
- o Dial backup of local access has little effect on end-to-end reliability compared to dial backup of the entire network through an alternative IXC.
- o Network reliability can be increased by limiting the use of large capacity equipement (such as FOTs), by increasing equipment redundancy and sparing, and by using diverse equipment technologies (FOT and bypass microwave).
- o Actual reliability/availability calculations may produce meaningless results unless all reliabilty measures are determined using the same standards. By understanding the network design and physical equipment and transmission technologies, network reliability can be ensured.
- o Additional algorithm research is needed to incorporate capacity, cost, and software considerations into network reliability calculations. No universal algorithm covering all factors of reliability exists today.

7.0 Summary

A general model for a large data communications network was developed. The model was composed of equipment and transmission facilities. Equipment was divided into three categories: access, switching, and concentration. Transmission facilities were divided into subsystems of local and long haul transmission.

Models were determined for IXC networks. Reliability for 4x4 fully meshed networks were computed using a factoring theorem algorithm .

Equipment and transmission reliability were incorporated into comprehensive models for various access methods and networks. End-to-end network reliability was computed.

8.0 Literature Cited

[1] Johnson, Rubin, "Some Combinatorial Aspects of Network Reliability," University of California, Berkeley, memorandum no. UCB/ERL M28/14, March 16, 1982.

[2] Styke, R.Van and Frank, H., "Network Reliability Analysis: Part I," Networks, Vol. 1, 1972, pp.279-290.

[3] Wilkov, Robert S., "Analysis and Design of Reliable Computer Networks," IEEE Transactions on Communications, Vol. 20, No.3, June 1972, pp.660-678.

[4] Fratta, Luigi and Montanari, U. G."Synthesis of Available Networks," IEEE Transactions on Reliability, Vol. R-25, No. 2, June 1976, pp. 81-87.

[5] Satyanarayanan, A. and Chang, Mark K., "Network Reliability and the Factoring Theorem," Networks, Vol. 13, 1983, pp. 107-120.

[6] Ball, Michael O., "Computational Complexity of Network Reliability Analysis: An Overview," IEEE Transactions on Reliability, Vol. R-35, No.3 August 1986, pp. 230-239.

[7] Conlisk, James K. "Topology and Survivability of Future Transport Networks," IEEE Globecom '89 Conference, September 1989, pp. 0826-0834.

[8] Hiller, Fredrick and Liberman, Gerald, Introduction to Operations Research, Holden-Day, 1980, pp. 594-611.

[9] Blanchard, Benjamin S. and Fabrychy, Wolter J., Systems Engineering and Analysis, Prentice-Hall, 1981, pp.322-369.

[10] "Methods and Procedures for Systems Reliability Analysis," SR-TSY-001171, Bell Communications Research, Issue 1 January 1989.

[11] Case/Datatel Reliability Calculations of Case Products, internal memo.

[12] Telenet Communications Corporation, TP4 Hardware Systems Functional Description, GF-0026-3, January 1987.

[13] Telenet Network Planning Considerations class material, 1986 (internal).

[14] Leichter, LLoyd L., "Telco Systems Basic Route-24 MTBF Prediction," TRI-L Associates, Dec. 1989.

[15] "Design MTBF Data (calculated from MIL-HDBK-217D)," Timeplex Communication Corporation, internal memo PMO #88-06.

[16] "AT&T DDM-1000 Dual DS-3 Multiplexer," Product Specification 2454B MCO, AT&T Network Systems, June 1989.

[17] Rockwell International LTS-1565 Systems Brochures, Rockwell Intl., 1989.

[18] Transmission Systems for Communications, Bell Telephone Laboratories (AT&T Bell Labs), 1982.

[19] Zorpette, Glenn, "Keeping the Phone Lines Open," IEEE Spectrum, June 1989, pp.32-36.

[20] Wilson, Carol, "Hindsale's Aftermath: COs at Risk," Telephony, March 20, 1989, pp 21-25.

[21] "Reliability - LATA Switching Systems Generic Requirements (LSSGR)," TR-TSY-000512, Bell Communications Research, Issue 2 July 1987.

[22] Ballart, Ralf and Ching, Yau-Chau, "Sonet: Now It's the Standard Optical Network," IEEE Communications Magazine, March 1985, pp.8-15.

[23] Rush, J.W., "Microwave Path Availability at 19 and 23 GHz," Microwave Journal, Aubust 1989, pp.165-169.

[24] Cooper, Walter A., "The Private Microwave Renaissance," Business Communications Review, May 1989, p. 43-47.

[25] "Special Facilities Routing of Access Service," FCC Tariffs, Section 11, 1989.

[26] Tanenbaum, Andrew S., Computer Networks, Prentice-Hall, 1981.

[27] Page, Lavon B. and Perry, Jo Ellen, "A Practical Implementation of the Factoring Theorem of Network Reliability," IEEE Transactions on Reliability, Vol. 37, No. 3, August 1988, pp. 259-267.

[28] Page, Lavon B. and Perry, Jo Ellen, "Reliability of Directed Networks Using the Factoring Theorem," IEEE Transactions on Reliability, Vol. 38, No. 5, December 1989, pp. 556-562.

[29] Aggarwal, K.K., Chopra, Y.C., ..., "Capacity Consideration in Reliability Analysis of Communication Systems," IEEE Transactions on Reliability, Vol. R-31, No.2, June 1982, pp.177-181.

8.1 Additional References

The following references, though not specifically cited in this project, provide useful information on work that has been done in the area of computer network reliability.

8.1.1 Reliability Algorithms

Agarwal, Yogesh K., "An Algorithm for Designing Survivable Networks," AT&T Technical Journal, May/June 1989, pp. 64-76.

Agrawal, Avinsh, "Network Reliability Analysis Using 2-Connected Digraph Reductions," Networks, Vol. 15, 1985, pp. 239-256.

Aggarwal, K.K., "A Fast Algorithm for the Performance of a Telecommunication Network," IEEE Transactions on Reliability, Vol. 37, No.1, April 1988, pp.65-69.

Aggarwal, K.K., "Integration of Reliability and Capacity in Performance Measure of a Telecommunications Network," IEEE Transactions on Reliability, Vol. R-34, No.2, June 1985, pp.184-186.

Ayanoglu, Ender and I, Chih-Lin, "A Method of Computing the Coefficients of the Network Reliability Polynomial," IEEE Globecom '89 Conference, September 1989, pp. 0331-0337.

Ball, Michael O., "Complexity of Network Reliability Computations," Networks, Vol. 10, 1980, pp.153-165.

Ball, Michael O. "Computing Network Reliability," Operations Research, Vol. 27, No. 4, July-August 1979, pp.823-839.

Bern, Marshall W. and Graham, Ronald L., "The Shortest-Network Problem," Scientific American, January 1989. pp. 84-89.

Colbourn, Charles J. and Harms, Daryl D., "Bounding All-Terminal Reliability in Computer Networks," Networks, Vol. 18, 1988, pp.1-12.

deMercado, J., Spyratos, N., ..., "A Method for Calculations of Network Reliability," IEEE Transactions on Reliability, Vol. R-25, No. 2 June 1976, pp.71-76.

Fishman, George S., "A Monte Carlo Sampling Plan for Estimating Reliability Parameters and Related Functions," Networks, Vol. 17, 1987, pp.169-186.

Kubat, Peter, "Estimation of Reliability for Communication/Computer Networks-Simulation/Analytic Approach," IEEE Transactions on Communications, Vol. 37, No. 9, September 1989, pp.927-933.

Neufeld, Eric M. and Colbourn, Charles J., "The Most Reliable Series-Parallel Networks," Networks, Vol. 15, 1985, pp. 27-32.

Pattavina, Achille, "Reliability-Constrained Dimensioning of Transmission Resources in Packet Switched-Networks," IEEE Transactions on Reliability, Vol. 34 No.4, October 1988, p. 434-442.

Raghavendra, C.S. and Makam, S.V. "Reliability Modeling and Analysis of Computer Networks," IEEE Transactions on Reliability, Vol. R-35, No. 2 June 1986, pp. 156-160.

8.1.2 General Articles on Reliability

Bell, Trudy E.,"Engineering a Minimum-Risk System," IEEE Spectrum, June 1989, pp.24-27. See also other articles in same issue.

Haverlock, Peter M. "The Formula For Network Immortality," Data Communications, August, 1988 pp.112-122.

Kuenh, Richard A."Planning for Disaster Recovery," Business Communications Review, July-Aug 1988, pp. 50-53.

8.1.3 Component Reliability

"Component Reliability Assurance Requirements for Telecommunications Equipment," TR-TSY-000357, Bell Communications Research, Issue 1, December 1987.

MIL-HDBK-217E, "Reliability Prediction of Electronic Equipment," October 27, 1986.

MIL-HDBK-338, " Electronic Reliability Design Handbook," October 15, 1984.

"Reliability and Life Testing," ITT Reference Data for Radio Engineers, Howard Sams & Co. 1977.

"Reliability Prediction Procedure for Electronic Equipment," TR-TSY-000332, Bell Communications Research, Issue 2 July 1988.

Appendix A - Packet Switch Reliability Calculations

Appendix A - Packet Switch Reliability Calculations

The following section describes in detail the mathematical calculations required to determine the reliability of a channel in a packet switch. See Figure 5 and Table 1 for the subsystem model and reliability of the subsystems.[12]

Example of CPU Reliability Calculations

MTBF = 26,386 hours

MTTR = 7 hours

$$p_{CPU} = \frac{MTBF}{MTBF + MTTR}$$

$$p_{CPU} = \frac{26386}{26386 + 7}$$

$$p_{CPU} = 0.999735$$

With a redundant CPU subsystem:

$$p_{CPU\,||} = 1 - (1 - p_{CPU})^2 \qquad (|| = \text{parallel})$$

$$p_{CPU\,||} = 0.999999$$

Other Subsystem Reliabilities

$p_{PS\,||} = 0.999999$

$p_{ARB/MEM\,||} = 0.999999$

$$p_{HSLPU\,1:7} = \sum_{i=6}^{7} \binom{7}{i} p^i (1-p)^{7-i}$$

$$\text{where} \binom{7}{i} = \frac{7!}{i!(7-i)!}$$

$$= 7p^6 - 6p^7$$

$p_{HSLPU\ 1:7} = 0.999993$

$p_{HSLPU*I/O\ 1:7} = 7p^6 - 6p^7$ (where $p = p_{HSLPU} * p_{I/O}$)

$p_{HSLPU*I/O\ 1:7} = 0.999992$

Packet Switch System Reliability

$p_{sys} = p_{I/O} * p_{HSLPU1:7} * p_{PS||} * p_{ARB/MEM||} * p_{CPU||} * p_{HSLPU*I/O\ 1:7}$

$p_{sys} = 0.999984*0.999993*0.999999*0.999999*0.999999*0.999992$

$p_{sys} = 0.999966$

$$MTBF = \frac{MTTR\ (p)}{(1-p)}$$

$$= \frac{0.999966*7}{(1-0.999966)}$$

MTBF = 205,877 hours (hardware failure)

Soft Failures

Complex computer equipment, like packet switches, have failures that do not register as a failure, but do impact the operation of the switch. These failures are termed soft failures. A detailed description of each of the soft failure scenarios is listed in Table 8.[12] This table shows the results of a change of an online failed unit to a redundant standby unit. These soft failures, though they effect service availability, are very short duration outages compared to the longer transmission outages measured in hours. These soft failures highlight the reload problems of centralized architecture verses distributed architecture systems and problems with switching that is not glitchless.

TABLE 8 - TP4/II PACKET SWITCH DETAILED FAILURE SCENARIOS

Failure	Result
AMU	All virtual circuits disconnected. Backup AMU switched in and TP reload required. Mean-time-to-restore is 5 to 15 minutes to complete reload from NCC.
CPU	All virtual circuits disconnected. Backup CPU switched. MTTR less than 1 minute.
LPU Redundancy	LPU N-for-M (1:N used in this project) redundancy is available for LPU groups (N=10 max.). When and LPU fails, the master operating system can automatically (or through NCC intervention) activate logic switches, which transfers the lines to the backup LPU. The local memory of the backup LPU is loaded from shared memory in less than 30 seconds. All calls originating and terminating on the LPU will be lost and must be reestablished by the user on the backup LPU.Virtual circuits (VCs) transmitting the failed LPU will be automatically recovered through the reconnect feature. Once the backup LPU is in service, failure of another LPU will result in total loss of the second failed LPU. The backup LPU must be hardware strapped to match all other LPUs that it supports.
Power Supply	Load sharing supplies. No effect on TP, however should not be run for greater than 72 hours on one supply. The TPPS-2 (AC supply) and TPPS-7 (DC supply) supplies individually provide internal redundancy for +5V modules and hot standby for the triple output modules (+5, +12, and -12V) and the control module. In addition, when used in a redundant configuration, the power supplies provide redundancy between units.

Appendix B - Channel Bank Reliability Calculations

Appendix B - Channel Bank Reliability Calculations

The following section details the mathematical calculations required to determine the reliability of a channel in a channel bank. See Figure 6 for the subsystem model.[14]

Subsystem Reliability

Component	MTBF	p(MTTR = 7 hours)
56/64kbps I/O Card	504,745	0.999986
Power Supply (DC)	2,042,901	0.999997
Shelf	7,380,074	0.999999
LIU	403,051	0.999983

Channel Bank System Reliability

$p_{sys} = p_{56/64} * p_{PS} * p_{Shelf} * p_{LIU}$

$p_{sys} = 0.999986*0.999997*0.999999*0.999983$

$p_{sys} = 0.999965$

$$MTBF = \frac{MTTR\ (p)}{(1-p)}$$

$$= \frac{0.999965*7}{(1-0.999965)}$$

MTBF = 199,995 hours (system hardware failure)

Appendix C - Intelligent Multiplexer Reliability Calculations

Appendix C - Intelligent Multiplexer Reliability Calculations

The following section details the mathematical calculations required to determine the reliability of a channel in an intelligent multiplexer. See Figure 6 for the subsystem model.[15]

Subsystem Reliability

Component	MTBF	p (MTTR = 7 hours)
I/O	43,000	0.999837
Power Supply (AC)	10,000	0.999300
CPU	80,192	0.999913
HS I/O	43,422	0.999839
INTF	56,560	0.999876

Intelligent Multiplexer System Reliability

$$p_{sys} = p_{I/O} * p_{PS||} * p_{CPU||} * p_{HSI/O*INTF||}$$

$$p_{sys} = 0.999837*0.999999*0.999999*0.999999$$

$$p_{sys} = 0.999834$$

$$MTBF = \frac{MTTR\ (p)}{(1-p)}$$

$$= \frac{0.999834*7}{(1-0.999834)}$$

MTBF = 42,162 hours (system hardware failure)

Appendix D - Program Results

Appendix D - Program Results

Reduce&Factor Input for 4x4 Mesh, Undirected IXC Network

```
1 2 3 4
1 2 .9985
1 3 .9985
1 4 .9985
2 3 .9985
2 4 .9985
3 4 .9985
```

Reduce&Factor Output for 4x4 Mesh, Undirected IXC Network

```
*** 4x4 mesh ***   Reduce&Factor
Nodes in K --> 1 2 3 4
  1 -----  2     rel =   0.9985
  1 -----  3     rel =   0.9985
  1 -----  4     rel =   0.9985
  2 -----  3     rel =   0.9985
  2 -----  4     rel =   0.9985
  3 -----  4     rel =   0.9985
0.999999986484903556 = probability
Number of calls = 8
Time = 0.0 seconds
Number of parallel edge reductions          2
Number of one-degree vertex reductions      2
Number of two-degree vertex reductions      3
Number of times factoring theorem is used   1
```

Reduce&Factor Input for 4x4 Mesh, Directed IXC Packet Network

```
1 4
5 2 .9985
5 3 .9985
5 4 .9985
6 1 .9985
6 4 .9985
6 3 .9985
7 1 .9985
7 4 .9985
7 2 .9985
8 2 .9985
8 3 .9985
8 1 .9985
1 5 .999966
2 6 .999966
3 7 .999966
4 8 .999966
```

Reduce&Factor Output for 4x4 Mesh, Directed IXC Packet Network

```
*** 4x4 mesh packet ***   Directed Network Program
Source vertex = 1   Sink vertex = 4

  5 ----  2   rel =   0.9985
  5 ----  3   rel =   0.9985
  5 ----  4   rel =   0.9985
  6 ----  1   rel =   0.9985
  6 ----  4   rel =   0.9985
  6 ----  3   rel =   0.9985
  7 ----  1   rel =   0.9985
  7 ----  4   rel =   0.9985
  7 ----  2   rel =   0.9985
  8 ----  2   rel =   0.9985
  8 ----  3   rel =   0.9985
  8 ----  1   rel =   0.9985
  1 ----  5   rel =   1.0000
  2 ----  6   rel =   1.0000
  3 ----  7   rel =   1.0000
  4 ----  8   rel =   1.0000
Number of edges = 16   Number of vertices = 8
0.9999659929331188O2 = probability
Time = 0.03 seconds
Number of source/sink reductions          5
Number of chain vertex reductions         6
Number of times factoring theorem is used 3
```

Reduce&Factor Input for 4x4 Mesh, Directed IXC IMUX Network

```
1 4
5 2 .9985
5 3 .9985
5 4 .9985
6 1 .9985
6 4 .9985
6 3 .9985
7 1 .9985
7 4 .9985
7 2 .9985
8 2 .9985
8 3 .9985
8 1 .9985
1 5 .9998
2 6 .9998
3 7 .9998
4 8 .9998
```

Reduce&Factor Output for 4x4 Mesh, Directed IXC IMUX Network

```
*** 4x4 mesh - IMUX ***   Directed Network Program
Source vertex = 1   Sink vertex = 4

  5 ----  2   rel =   0.9985
  5 ----  3   rel =   0.9985
  5 ----  4   rel =   0.9985
  6 ----  1   rel =   0.9985
  6 ----  4   rel =   0.9985
  6 ----  3   rel =   0.9985
  7 ----  1   rel =   0.9985
  7 ----  4   rel =   0.9985
  7 ----  2   rel =   0.9985
  8 ----  2   rel =   0.9985
  8 ----  3   rel =   0.9985
  8 ----  1   rel =   0.9985
  1 ----  5   rel =   0.9998
  2 ----  6   rel =   0.9998
  3 ----  7   rel =   0.9998
  4 ----  8   rel =   0.9998
Number of edges = 16   Number of vertices = 8
0.9997999991386049575 = probability
Time = 0.03 seconds
Number of source/sink reductions          5
Number of chain vertex reductions         6
Number of times factoring theorem is used 3
```

Appendix E - End-to-End Model Calculations

Appendix E - End-to-End Model Calculations

The following are the calculations used to determine end-to-end reliability for models #1 - #7.

Model #1

Modem, Dedicated:

p_{sys} = 0.999767 * 0.99925 *0.999767* 0.9985*0.999767 * 0.99925 *0.999767

p_{sys} = 99.6074%

DSU, Dedicated:

p_{sys} = 0.999860 * 0.99925 *0.999860* 0.9985*0.999860 * 0.99925 *0.999860

p_{sys} = 99.6445%

DSU-channel bank, Dedicated:

p_{sys} = 0.999860 * 0.99925 *0.999883*0.999965* 0.9985*0.999965*0.999883*

0.99925 *0.999860

p_{sys} = 99.6421%

Model #2

Modem, Packet:

p_{sys} = 0.999767 * 0.99925 *0.999767* 0.999966*0.999767 * 0.99925 *0.999767

p_{sys} = 99.7536%

Modem, IMUX:

p_{sys} = 0.999767 * 0.99925 *0.999767* 0.999834*0.999767 * 0.99925 *0.999767

p_{sys} = 99.7405%

DSU, Packet:

p_{sys} = 0.999860 * 0.99925 *0.999860* 0.999966*0.999860 * 0.99925 *0.999860

p_{sys} = 99.7908%

DSU, IMUX:

p_{sys} = 0.999860 * 0.99925 *0.999860* 0.999834*0.999860 * 0.99925 *0.999860

p_{sys} = 99.7776%

DSU-channel bank, Packet:

p_{sys} = 0.999860 * 0.99925 *0.999883*0.999965* 0.999966*0.999965*0.999883*

0.99925 *0.999860

p_{sys} = 99.7884%

DSU-channel bank, IMUX:

p_{sys} = 0.999860 * 0.99925 *0.999883*0.999965* 0.999834*0.999965*0.999883*

0.99925 *0.999860

p_{sys} = 99.7752%

Model #3

Modem, Packet:

p_{sys} = 0.999767 * 0.99925*0.99995 *0.999767* 0.999966*0.999767 *0.99995*

0.99925 *0.999767

p_{sys} = 99.7437%

Modem, IMUX:

p_{sys} = 0.999767 * 0.99925*0.99995 *0.999767* 0.999834*0.999767 *0.99995*

0.99925 *0.999767

p_{sys} = 99.7305%

Model #4

Modem, Packet:

p_{sys} = {1-[1-(0.999767 * 0.99925 *0.999767)]*[1-(0.999767 * 0.99995 *0.999767)]}*

0.999966*{1-[1-(0.999767 *0.99925 *0.999767)]* [1-(0.999767*0.99995 *0.999767)]}

p_{sys} = 99.9964%

Modem, IMUX:

p_{sys} = {1-[1-(0.999767 * 0.99925 *0.999767)]*[1-(0.999767 * 0.99995 *0.999767)]}*

0.999834*{1-[1-(0.99976 *0.99925 *0.999767)]*[1-(0.999767 * 0.99995 *0.999767)]}

p_{sys} = 99.9832%

DSU, Packet:

p_{sys} = {1-[1-(0.999860* 0.99925 *0.999860)]*[1-(0.999860 * 0.99995 *0.999860)]}*

0.999966*{1-[1-(0.999860 * 0.99925 *0.999860)]*[1-(0.999860*0.99995 *0.999860)]}

p_{sys} = 99.9864%

DSU, IMUX:

p_{sys} = {1-[1-(0.999860 * 0.99925 *0.999860)]*[1-(0.999860 * 0.99995 *0.999860)]}*

0.999834*{1-[1-(0.999860* 0.99925 *0.999860)]*[1-(0.99986 *0.99995 *0.999860)]}

p_{sys} = 99.9832%

Model #5

Modem, Packet:

p_{sys} = {1-[1-(0.999767*0.99925*0.999767*0.999966*0.999767 * 0.99925 *0.999767)]

*[1-(0.999767*0.99995 *0.999767*0.999966*0.999767 * 0.99995 *0.999767)]}

p_{sys} = 99.9997%

Modem, IMUX:

p_{sys} = {1-[1-(0.999767*0.99925 *0.999767*0.999834*0.999767 * 0.99925 *0.999767)]

*[1-(0.999767 * 0.99995 *0.999767*0.999834*0.999767 * 0.99995 *0.999767)]}

p_{sys} = 99.9997%

DSU, Packet:

p_{sys} = {1-[1-(0.999860 * 0.99925 *0.999860*0.999966*0.999860*0.99925 *0.999860)]

*[1-(0.999860 * 0.99995 *0.999860*0.999966*0.999860*0.99995 *0.999860)]}

p_{sys} = 99.9999%

DSU, IMUX:

p_{sys} = {1-[1-(0.999860 * 0.99925 *0.999860*0.999834*0.999860*0.99925*0.999860)]

*[1-(0.999860 * 0.99995 *0.999860*0.999834*0.999860* 0.99995 *0.999860)]}

p_{sys} = 99.9998%

Model #6

Modem, Packet:

p_{sys} = 0.999767*0.999860*{1-[1-(0.99925)]*[1-(0.99925*0.99995)]} *0.999966*{1-[1-

(0.99925)]*[1-(0.99925*0.99995)]}*0.999767*0.999860

p_{sys} = 99.9218%

Modem, IMUX:

p_{sys} = 0.999767*0.999860*{1-[1-(0.99925)]*[1-(0.99925*0.99995)]} *0.999834*{1-[1-

(0.99925)]*[1-(0.99925*0.99995)]}*0.999767*0.999860

p_{sys} = 99.9086%

Model #7

Modem, Packet/Packet:

p_{sys} = 0.999767*0.999860*{1-[1-(0.99925*0.999767*0.999966*0.999767*0.99925)]

*[1-(0.99925*0.99995*0.999966*0.99995*0.99925)]}*0.999860*0.999767

p_{sys} = 99.9251%

Modem, IMUX/Packet:

p_{sys} = 0.999767*0.999860*{1-[1-(0.99925*0.999767*0.999834*0.999767*0.99925)]

*[1-(0.99925*0.99995*0.999966*0.99995*0.99925)]}*0.999860* 0.999767

p_{sys} = 99.9251%