NTIA Report 90-257

# Congestion-Reduction and Service-Restoration Strategies for Telecommunication Networks

**Robert F. Linfield**


**U.S. DEPARTMENT OF COMMERCE**
**Robert A. Mosbacher, Secretary**

Janice Obuchowski, Assistant Secretary
for Communications and Information

February 1990

# PREFACE

The Institute for Telecommunication Sciences (ITS) is conducting a series of projects concerned with the roles of advanced communication satellites in Integrated Services Digital Networks (ISDN) and the use of advanced satellite system technology to enhance rapid restoration of services provided by the Public Switched Network (PSN) following a natural or man-made disaster. Goals of this work are (1) to promote an effective integration of advanced satellite systems with future terrestrial broadband networks, (2) to perform studies that examine uses of advanced communication satellite systems to reduce national vulnerability to telecommunication outages, and (3) to identify and recommend interface and functional standards required for integrated services, such as ISDN, in a terrestrial-satellite broadband transmission and switching environment. The Institute is working with the National Communications System (NCS) and other Government and industry organizations to define and develop the necessary standards.

The purpose of this first task of technical investigations funded by the NCS is to conduct a survey of various telecommunication networks including long-distance common carriers, local exchange carriers, and private networks and to review their restoration capabilities during times of stress. The study includes a summary of restoration techniques used to alleviate traffic congestion in the networks that are currently in use or contemplated for the future. Emphasis is on network management, operations, and restoration procedures that currently are used to enhance network restoration, to reduce traffic congestion, or to restore service following disasters. The task has been limited to voice and data networks in the continental United States.

The views, opinions, and findings contained in this report are those of the author only, and should not be construed to be an official National Communications System, National Telecommunications and Information Administration, Institute for Telecommunication Sciences, or any other agency position, policy, or decision unless so designated by other official documentation.

CONTENTS

LIST OF FIGURES

LIST OF TABLES

# CONGESTION-REDUCTION AND SERVICE-RESTORATION STRATEGIES FOR TELECOMMUNICATION NETWORKS

R. F. Linfield*

This report covers the first task of a three-task effort designed to explore the potential of using advanced satellite system technologies to enhance the rapid restoration of telecommunication services that may be disrupted due to traffic congestion or natural or man-made disasters. The purpose of this first task is to survey the various strategies currently used to alleviate stress. The telecommunication networks included are long-distance common carriers, local exchange carriers, and private networks. Both preventive and corrective measures are covered. Preventive measures include prioritizing traffic using fault-tolerant systems, and implementing alternate routing procedures. Corrective measures include network reconfiguration, engaging bypass systems, using transportable equipment and interconnecting systems.

Key words: alternate routing; disaster recovery; fault detection; network reconfiguration; restoration; telecommunications

## 1. INTRODUCTION

This study is concerned with assessing the current technologies used to respond to telecommunications emergencies - including national, regional, and local. Emergencies may be caused by natural disasters such as hurricanes, earthquakes, or fires or by traffic overloads due to special events like Mother's Day and Christmas. They may cause actual damage to the telecommunications network or result in traffic levels that exceed capacity limits of the telecommunication facilities. This study reviews the methods currently available that can be implemented when these events occur. Some recent examples of major network disruptions are given below.

Thanksgiving Weekend (1982). A seventeen story office building in downtown Minneapolis was destroyed in a fire. The entire headquarters facilities of one of the largest banks in the city was lost. Hundreds of people had to be relocated and their communications (data and voice) links restored before they could resume business operations. See Moberg (1989).

---

*The author is with the Institute for Telecommunication Sciences, National Telecommunications and Information Administration, U.S. Department of Commerce, Boulder, CO 80303

February (1987). The AT&T main toll center switch, a 4 ESS, in Dallas, Texas went down because a circuit pack in a communications bus failed. A hot standby switch continued service for 30 minutes and then it, too, failed. See Morley (1987).

Mother's Day (1988). A shorted power cable in a ceiling mounted tray containing power and communications cable caused a fire in the central office of Illinois Bell in Hinsdale, IL. Service was disrupted to 35,000 residential and business customers, and to 680,000 long distance users with a loss of 3.5 million calls a day and hundreds of millions of dollars in revenue. See Zorpette (1989).

November (1988). A New Jersey construction crew digging a water line severed an optical-fiber cable that had been carrying 200,000 calls an hour. See NRC (1989).

These are just four examples of communications disasters. Others include floods, earthquakes, and even sabotage. In addition, the networks themselves are becoming increasingly vulnerable to service disruptions. A recent report prepared by the National Research Council (NRC, 1989) addressed the increasing problems in the network infrastructure due to new technologies. This includes increased vulnerability due to the following:

Fiber Optic Trunking. The higher capacity fiber results in fewer routes and, thus, major service disruptions occur when links do go down.

Concentrated Switching. Although more cost-effective and therefore more competitive, the concentration increases network vulnerability.

Customer Control. This is a concept that allows customer access to executable codes and data bases in order to reconfigure private network topologies and features. The easy access makes networks more vulnerable to hackers.

Several programs have already evolved from the recommendations of the National Security Telecommunications Advisory Committee (NSTAC) and National Security Decision Directive 97 (NSDD-97), formerly Presidential Directive 53 (PD-53).

The NSTAC was formed at the request of the President and was formally announced in Executive Order (E.O.) 12382 on September 13, 1982. The NSTAC consists of the chief executive officers of 28 of the largest telecommunication companies in the United States. The NSTAC provides the

President with advice on national security emergency preparedness (NSEP) telecommunication matters from the perspective of industry.

NSDD-97, which was issued June 13, 1983, declares that the surviving national telecommunications capability should comprise Government, commercial, and private facilities, systems, and networks, and mandates that the commercial resources be enhanced in support of the overall NSDD-97 objectives. As a result, the National Communications System (NCS) has been exploring ways to maintain service continuities in the Government sector.

In this report, we summarize some of the major ongoing programs that have evolved from these NCS efforts. This is followed by two major sections that describe measures taken to prevent traffic congestion and to restore service after a disruption occurs.

## 2. BASIC CONCEPTS AND DEFINITIONS

This section reviews some characteristics of telecommunications networks that currently are used in the United States. Based on these characteristics it is useful to characterize today's networks as a multilevel matrix consisting of public and private networks with local and regional elements. Within the public and private categories, the traffic overloads due to stress are either global or focused in the local access area, an entire region, or even several regions. The congestion-reduction or restoration procedures may be different for these conditions.

### 2.1 Network Architectures

A network's "architecture" defines the functions that the network components are to perform. The architecture provides the framework for routing traffic, end-to-end procedures for recovering data, message security, and protocols at all levels. Thus, the architecture is distinguished from a network's "implementation," which defines exactly what hardware and software is used. In this section we are concerned with the major network architectural concepts--namely the topology, switching hierarchy, and control signaling. First, we define some architectures that are either in current use today or are planned for the near future. Additional information on these networks is given in a related report by Nesenbergs (1989).

The Hierarchical Architecture

One network architecture commonly used is the hierarchical structure typified by the diagram in Figure 1. The switching nodes at each level in this hierarchy perform separate and distinct functions. The first and lowest level consists of the user terminals. These terminals (e.g., telephone handsets) connect to the next level via station loops. The network functions at this level are the familiar telephone loop functions (ringing, dialing, etc.). The next level in the architecture (Figure 1) involves the private automatic branch exchange (PABX), where the initial switching, processing and control functions take place. This is the level where service features seen by the users are generated. The PABX's are connected to the third switching level via local trunks. This third level involves central office switching and trunking to the long-haul networks. The long-haul switches are shown as level four. They serve as both toll and tandem switches. This structure is commonly used today by the Bell Operating Companies (BOCs).

An example of this type of hierarchical structure with even more levels is depicted in Figure 2 in a circular diagram. This is the familiar toll switching hierarchy of the public switched telephone network prior to the breakup of AT&T in 1984. This structure is described by Nesenbergs and McManamon (1983). Various circles, hexagons, triangles, and squares denote switching offices, centers, or points. The end offices are those serving either end subscribers or supporting lower level switching machines, such as PABX, remote switching units (RSUs), and other customer-owned terminal support or concentration facilities. The majority of subscribers are connected to these Class 5 End Offices (EOs). The EO's in turn can have trunks to just about every class of switching nodes, such as local tandem, EO plus local tandem, Class 4X Intermediate Point (IP), Class 4 Toll Center (TC), or Toll Point (TP), Class 3 Primary (P) Center or Point (P), Class 2 Sectional (S) Center, and at the tip of the hierarchy, to the Class 1 Regional (R) Center.

The general connectivity of the predivestiture toll network is not far removed from a star topology. At the loosely defined center of the star, the final route was provided through the regional centers R. There were 10 regions and 10 regional centers. The numbers of other class facilities are given in Table 1. A call may proceed (i.e., be routed) through just about all the switch classes, as directed by the common channel interoffice signal system (CCIS) and alternate routing arrangements. Alternate routing is

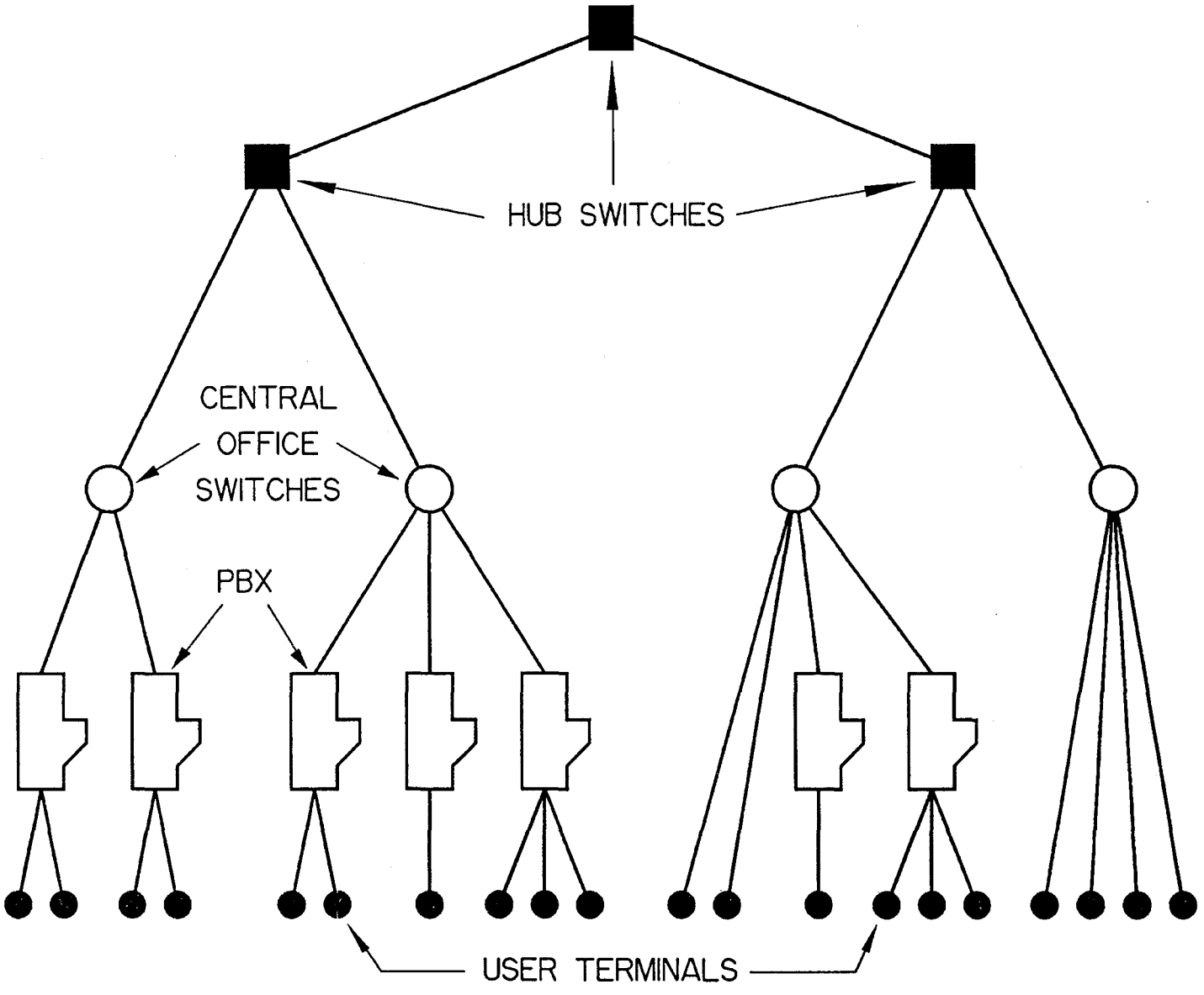



Figure 1. Typical hierarchical network implementation.

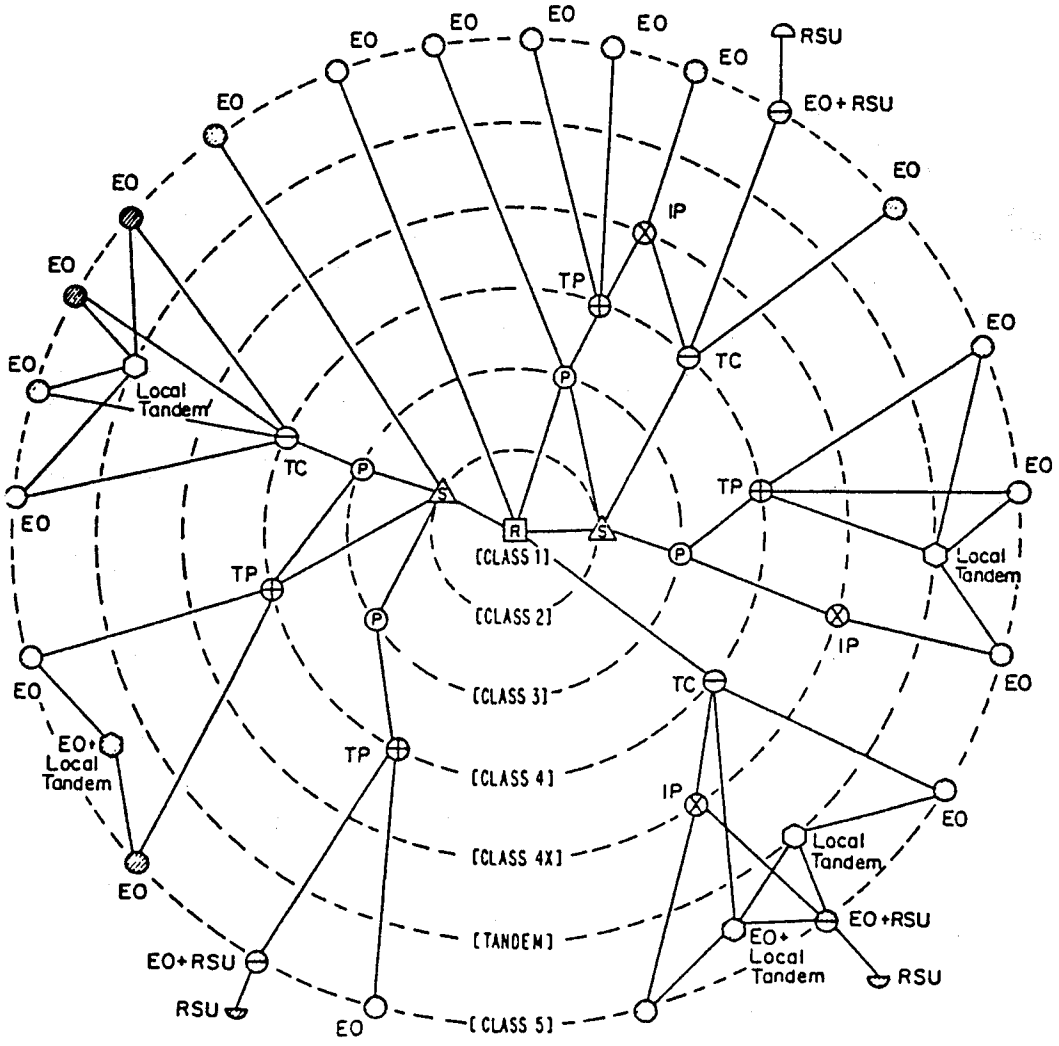



Figure 2. Intra- and interexchange network architecture, predivestiture.

Table 1. Toll Switching Centers, Predivestiture

| Class | Center Type | Number (1984) |
|---|---|---|
| 1 | Regional | 10 |
| 2 | Sectional | 63 |
| 3 | Primary | 204 |
| 4 | Toll | ~ 900 |
| 4X | Intermediate | ~ 9,000 |
| 5 | End or Tandem Office | ~ 10,000 |
| Total | | ~ 20,000 |

sometimes associated with the Least Cost Routing (LCR) "for the user," but that phrase is somewhat misleading. Alternate routing can be viewed instead as a method of alleviating trunk group congestion, improving interswitch blocking grade of service (GOS), carrying more traffic through the trunk network, bypassing damaged facilities, and thus producing more revenue for a given investment in the overall facilities. See Section 4.3.

Nonhierarchical Architectures

The multilevel hierarchical network in the United States is gradually being replaced by a network structure having two parts: a hierarchical part and a dynamic, nonhierarchical routing (DNHR) part. The basic structure is shown in Figure 3. The nonhierarchical nodes contain No. 4 ESS switches and common channel signaling. All switches perform equal functions. It is expected that the DNHR network in the 1990's will contain 140 such switches. The routing in the DNHR network is considered dynamic because routing can change as a function of the time of day. (See Section 4.3 for a description of DNHR.) Overall network efficiency is maintained as calling patterns change by re-routing calls through uncongested portions of the network.

Integrated Services Digital Network Architectures

The Integrated Services Digital Network (ISDN) is defined by the International Telegraph and Telephone Consultative Committee (CCITT) as a "network, in general, evolving from a telephony integrated digital network, that provides end-to-end digital connectivity to support a wide range of services, including voice and nonvoice, to which users have a limited set of standard multipurpose user-network interfaces". See CCITT (1985) and CCITT (1989).

Standards for various ISDN capabilities are in various stages of completion. Both national and international standards organizations have completed a substantial number of recommendations and standards concerning ISDN, and this process has now reached the point where a number of manufacturers are developing product lines to offer ISDN features, functions, and interfaces. These features, functions, and interfaces basically define the ISDN services and designs. They, along with perceived benefits and problems, are summarized below.

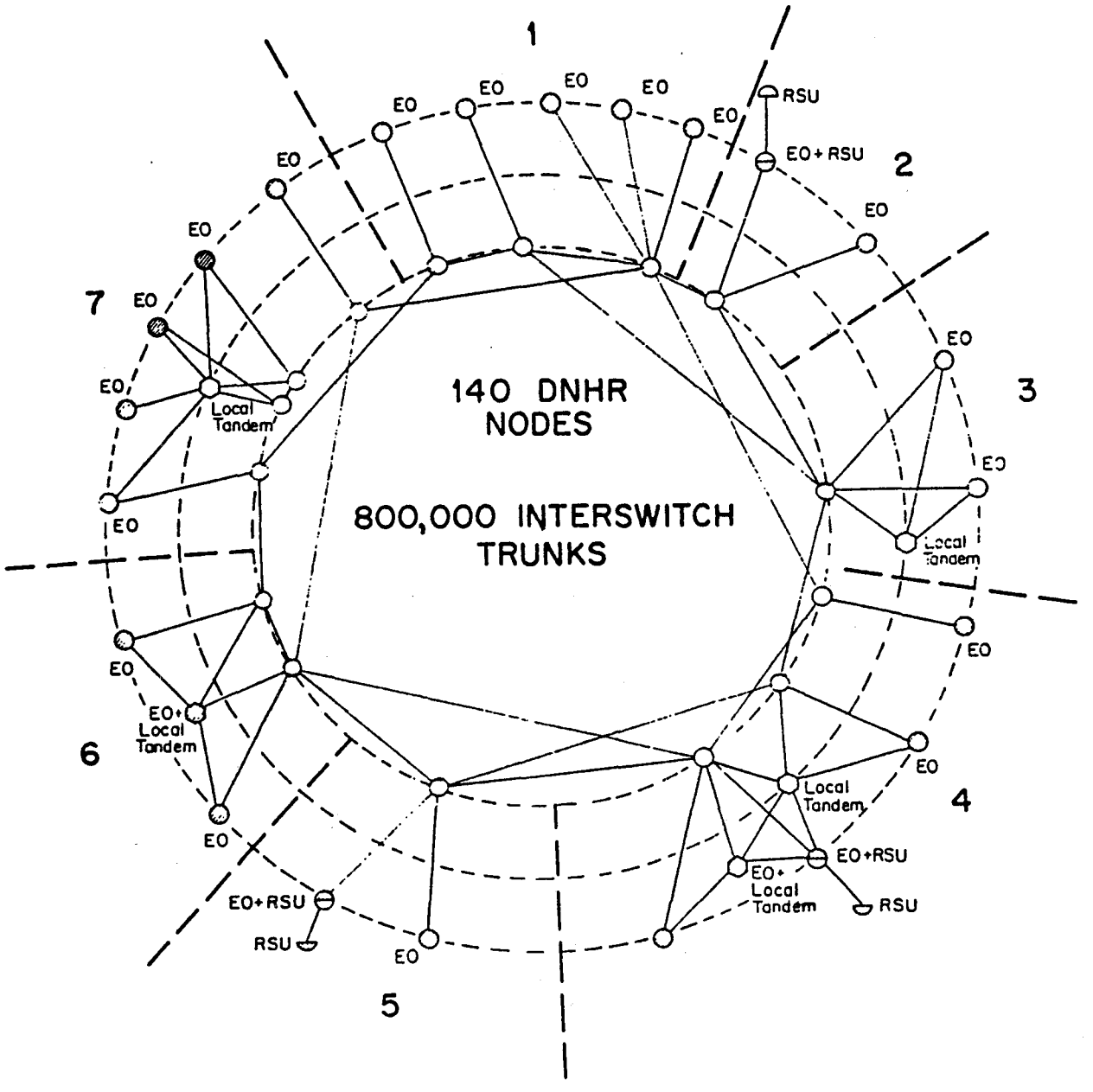



Figure 3. Intra- and interexchange network architecture, postdivestiture.

Features and functions associated with ISDN include:

- o end-to-end digital service.
- o standardized access interface structures.
- o 2B + D service (termed basic rate interface or BRI) for small users (B = 64 kb/s, D = 16 kb/s).
- o 23B + D service (termed primary rate interface or PRI) for large users (B = 64 kb/s, D = 64 kb/s).
- o defined basic bearer services and supplementary services.

Users perceive potential benefits such as:

- o faster and more complete information access, i.e., all types of information services through the same connecting plug.
- o increased productivity and better time management due to new services (e.g., voice mail).
- o easy addition of new services.
- o reduced cost due to voice and data integration in local access areas.
- o simplified network management and control.
- o reduced administration, operation & maintenance (AO&M) costs due to standardized system interfaces.

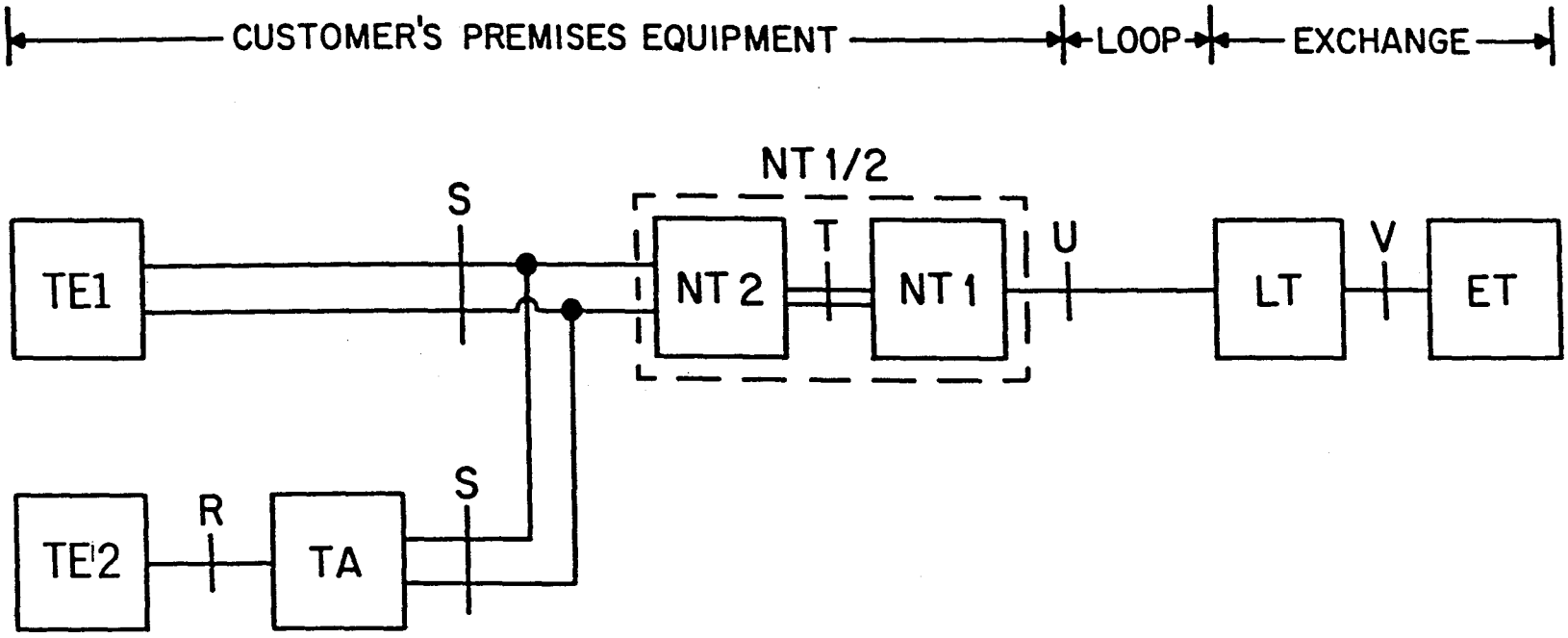
Some potential problems with narrowband ISDN are:

- o high development costs.
- o difficult evolution from voice networks.
- o potentially incompatible implementation for advanced LAN users.
- o narrowband ISDN may be leap frogged by a more advanced broadband ISDN is introduced.
- o vendor driven technology--not market driven technology.

The ISDN network termination equipment and interfaces are illustrated in Figure 4 and defined below:

TE1 - ISDN terminal equipment.

TE2 - Existing non-ISDN terminal equipment.




ET = Exchange Terminal
LT = Line Terminal
NT = Network Termination
TA = Terminal Adapter
TE1 = ISDN Terminal
TE2 = Non-ISDN Terminals

Figure 4. Illustration of ISDN network termination equipment and interfaces.

TA - Terminal adaptor for connecting TE2 to the ISDN S interface. (See interface descriptions below.)

NT1 - Network terminating equipment that converts a loop transmission (U interface) to an S or T interface.

NT2 - Network termination equipment that converts primary rate access (23B+D) to basic rate access (2B+D). (Examples are PBXs and LANs.)

NT1/2 - Single network termination that combines NT1 and NT2 functions.

LT - Line termination.

ET - Exchange termination.

The interfaces between terminals, network terminations, and the central offices (COs) are also indicated as R, S, T, and U. They are defined below for basic and primary rate access

R - Existing interface specifications (e.g., RS-232).

S - ISDN terminal or terminal adaptation interfaces characterized by 144 kb/s user access rates (2B+D). Up to 8 terminals can be connected on a single passive bus.

T - For primary rate access in the United States, the T-interface accesses 23B+D service (using 1.544 Mb/s); in Europe access is to 30B+D service. (Normally the same as the S interface for basic access.)

U - Primary rate transmission system (e.g., T-1 carrier interface). The basic rate U-interface uses an echo canceling hybrid for full duplex operation over 2-wire loops.

V - Basic rate interface between line and exchange terminals.

Terminal equipment (TE) includes devices that generate and receive information (e.g., a personal computer). Terminal adapters (TA) convert non-ISDN interfaces to an ISDN interface. Any TE2 can, therefore, be connected to ISDN through a suitable TA. Reference point R refers to the interface between the TE2 and the TA. Network terminations NT1 and NT2 provide distinct functions, but these functions may be combined in a PABX or LAN. NT2 refers to on-premises switching or other intelligence that is employed by the user

for communication. PABXs and LANs may contain NT2 functions. NT2 functions are separated from TA or TE1 functions by interface (reference point) S.

NT1 functions are restricted to connect the users' equipment to the digital subscriber transmission system. Reference point T designates this separation between NT1 and NT2 functions. NT1 and NT2 functions may be combined as a single functional group, which is designated as NT1/2. Such a configuration is indicated in Figure 4.

In the United States, the NT1 function is considered customer premises equipment, whereas in most other countries it is considered part of the network. Reference point U has been designated as the attachment between an NT1 and the digital subscriber line system. The V interface occurs in the local exchange.

In Section 5.4 we illustrate interconnecting networks for restoration or backup purposes. In our particular example the ISDN facilities are considered to be a private network. Public and private networks are characterized in the following paragraphs.

## 2.2 Public and Private Networks

There are many ways to characterize networks: switched or nonswitched, analog or digital, voice or data, narrowband or wideband, packet-switched or circuit-switched, leased or government-owned, etc. It is sometimes useful to separate networks into two domains--public and private. Each domain may be further subdivided into switched and nonswitched categories as depicted in Figure 5. The nonswitched category is usually only of interest to the private sector. The public and private domains may also be divided into four levels; the users level, local level, access level, and backbone level, as illustrated in Figure 6. Within each level various network elements may reside and the interconnections between levels may indicate both switched and nonswitched circuits. Examples of the network elements that may reside at each level are listed on the figure. In Section 5.4 the interconnections between public and private facilities are shown to be one potential method for restoring service to users in disrupted areas. Public networks are those networks where switching and transmission facilities are shared by the general public. The facilities of private networks are dedicated to a specific group of users. Private networks may be leased or independently-owned and operated.

| | PUBLIC | PRIVATE |
|---|---|---|
| SWITCHED | Switching and transmission facilities shared by public | Switching and transmission facilities dedicated to specific group |
| NON-SWITCHED | Transmission facilities shared by common users | Transmission facilities assigned to specific user |

Figure 5. Characterization of networks.

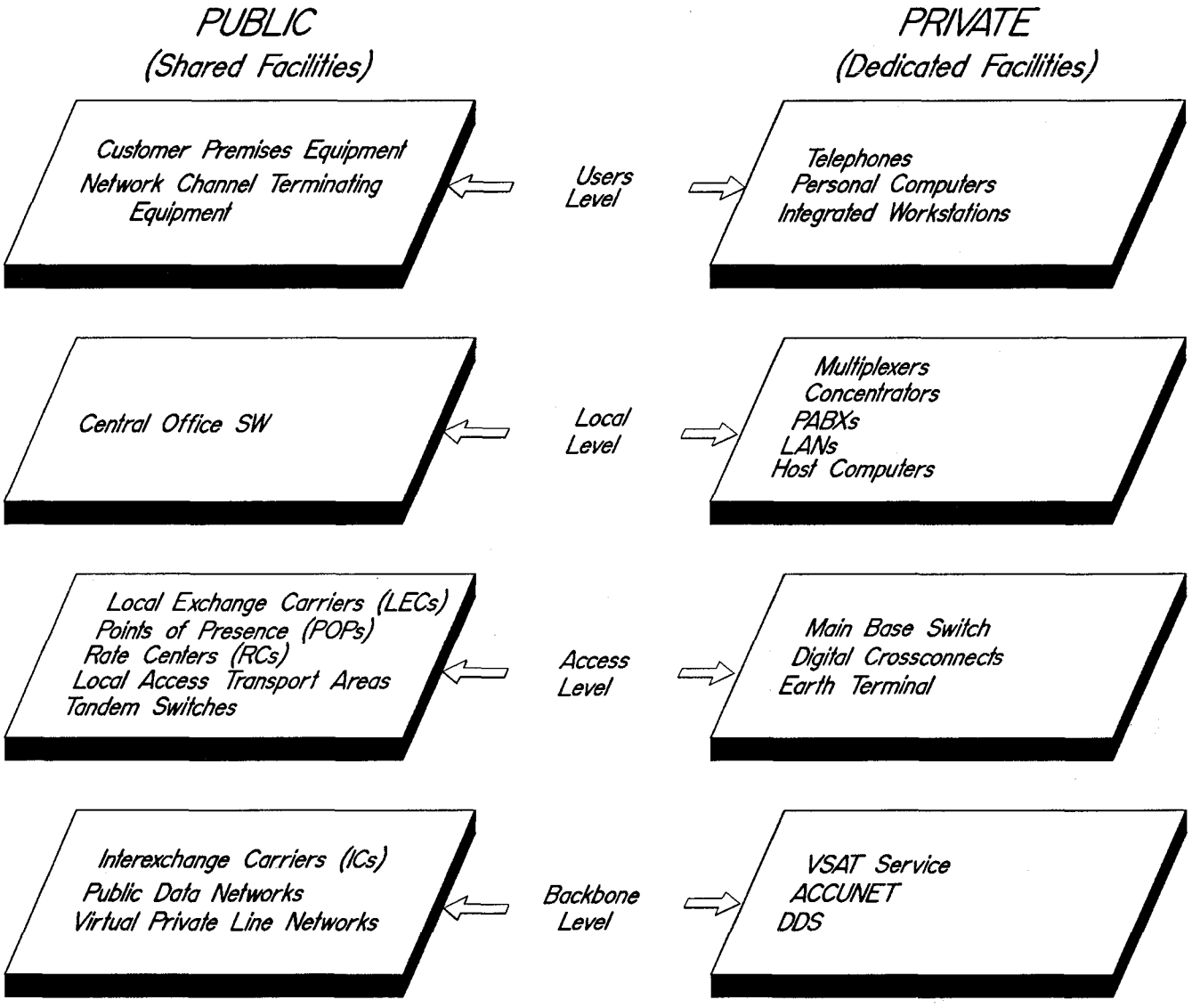



Figure 6. Multilevel structures of public and private networks.

Virtual private lines are actually apparent private lines (as opposed to dedicated private line) and fall in the public domain. Therefore, a virtual private line network (VPLN) only appears to be dedicated, but its facilities are shared since the VPLN is embedded (by software) in public facilities.

These distinguishing characteristics are important when considering restoration of facilities that are damaged. For example, there is probably no reason for attempting to use a VPLN to restore the public switched telephone network (PSTN) when damaged facilities affects both services that share facilities.

## 2.3 Hidden Networks

Inherent in any telecommunications network are a number of subnetworks or hidden networks. See Nesenbergs and McManamon (1983). The disruption or damage to a hidden network can often be as disastrous as if it occurred to the basic network providing communication services.

A good example of the hidden network within a network is the common channel interoffice signaling system (CCIS). CCIS provides the remote control of switching using a separate packet switching network that is separate from the voice network. In the future, the new standard common channel signaling system no. 7 (CCS-7) is expected to be implemented worldwide. A detailed description of CCS-7 can be found in CCITT (1989).

A disruption of enough signaling links or damage to signal transfer points in the separate signaling system could cause major disruption network service. There are currently 26 signal transfer points controlling the AT&T network in the United States.

Other "hidden" networks include the Bell System Reference Frequency (BSRF), Centralized Automatic Message Accounting (CAMA), Automated Intercept System (AIS), and Traffic Service Position System (TSPS) as well as a number of fault location and diagnostic networks. All perform critical telecommunication functions whose failure or disruption impacts the entire network.

## 2.4 Threat Scenarios

According to Zorpette (1989), no risk analysis has ever been conducted on the U.S. telephone network as a whole. This is because the network is too

large and complex for practical analysis. Risk management primarily relies on redundancy.

The military establishment, however, has defined a multilevel stress scenario. See Western Electric Company (1982). They include communications objectives for each scenario level in terms of blocking probability and delay. These stress conditions are summarized here since they do provide guidance for categorizing various methods for reducing traffic congestion and for restoring service under stress conditions.

The five levels of stress are:

1. Peacetime, readiness
2. Crisis and pre-attack
3. Early trans-attack
4. Massive nuclear attack
5. Post-attack

The first three levels have either no damage or only minor damage in the telecommunication network. The last two levels have major damage in the telecommunication network. Assured/endurable service is concerned with the first three levels of stress. For each of the first three stress levels, there are three possible network load conditions: no overload, focused overload, and general overload.

The objectives for the Defense Switched Network (DSN) in the United States are to provide assured service (essentially zero-blocking) for the precedence users when there is no damage and endurable service (essentially zero-blocking given connectivity) when there is minor damage, independent of the network load conditions. Furthermore, the average end-to-end delay involved in successfully setting up the calls under these three stress levels should be reasonably small (i.e., less than 10 s when there is no damage and less than 20 s when there is minor damage).

The communication objectives under these various conditions are summarized in Table 2. "Essentially nonblocking" implies a blocking probability of $p < 0.001$. Focused- and general-overload conditions were defined as two and eight times the normal load, respectively. These numbers are somewhat arbitrary.

Table 2. Defense Switched Network (DSN) Stress Scenarios

| Service | Stress Level | Damage | Overload | Example | End-to-End Blocking | End-to-End Delay (s) |
|---|---|---|---|---|---|---|
| Assured | 1. Peacetime, Readiness | No | No | Normal Business Day | Essentially Nonblocking | <10 |
| " | " | " | Focused | Air Crash | " | " |
| " | " | " | General | Mother's Day Mobilization | " | " |
| Assured | 2a. Crisis Pre-Attack | No | No | Military Event | Essentially Nonblocking | <10 |
| " | " | " | Focused | " | " | " |
| " | " | " | General | Cuban Missile Crisis | " | " |
| Endurable | 2b. Crisis, Pre-Attack | Minor | No | - | Essentially Nonblocking Given Connectivity | 15-20 |
| " | " | " | Focused | - | " | " |
| " | " | " | General | - | " | " |
| Endurable | 3. Crisis, Trans-Attack | Minor | No | - | Essentially Nonblocking Given Connectivity | 15-20 |
| " | " | " | Focused | - | " | " |
| " | " | " | General | - | " | " |

For the automatic voice network (AUTOVON) network, a priority system has been established using multilevel precedence and preemption levels. For these precedence users, the maximum busy hour traffic was only 5,000 Erlangs compared to about 1.5 million Erlangs for the nonprecedence users.

Other studies indicate that the maximum overload factors for nonprecedence users on a network under overload conditions would be 2 times the normal engineered capacity. For example, during a Los Angeles earthquake in 1971 the worst-case call attempt overload on a toll switch anywhere in the country including California was 100% (Macurdy, 1973).

### 2.5 Summary of Preventive and Corrective Measures

A primary purpose of this study is to conduct a survey of public and private networks and to summarize the techniques available to maintain service continuity during periods of traffic overload or network damage. It is useful, however, first to define the various strategies used by any network to maintain continuity of service or to restore disruptions of service. Two kinds of strategies can be defined; one is preventive, the other corrective. Preventive measures are automatically implemented during periods of stress. They become operative to alleviate traffic congestion whether it be caused by equipment failures or an excess of offered traffic. Corrective measures are only implemented when service is disrupted due to unforeseen network damage. They are not normally readily available.

Figure 7 illustrates these two strategy categories and lists the various measures used in each category for focused disruptive conditions and for more general disruptive conditions. Subsequent sections of this report describe in detail the more important preventive and corrective measures.

We begin Section 3 by briefly describing three programs currently supported by the NCS. The goal of these programs is to ensure services deemed essential to continuity of government during crisis periods. Then, in Sections 4 and 5 we explore preventive and corrective measures that are currently used to alleviate congestion on the network and to restore service.

## 3. NATIONAL SECURITY EMERGENCY PREPAREDNESS PROGRAM (NSEP)

The NCS program office has been exploring ways to alleviate service disruptions during periods of stress. Emphasis is on service survivability for government agencies that must respond during periods of crisis. The

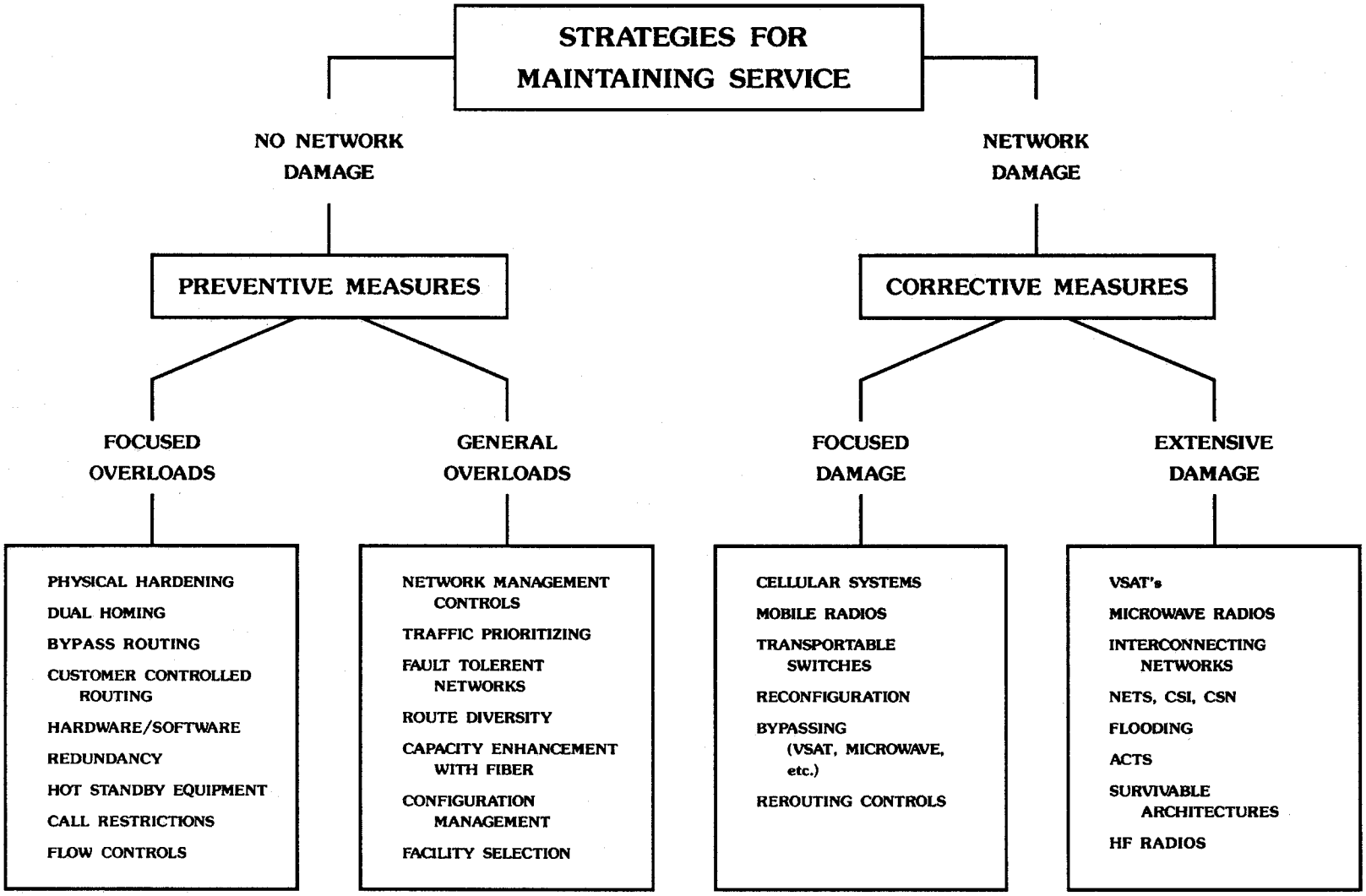



Figure 7. Strategies for maintaining service.

current approach is to utilize existing commercial facilities as much as possible. Currently there are three national level programs all directed toward improving the connectivity and survivability of the Public Switched Network (PSN). This is because the PSN is the principle provider of NSEP communication services, is already connected to all subscribers, and is fairly redundant. The three programs are designed to increase call completion probabilities during times of stress by increasing the number of routing options. The three programs are: the Nationwide Emergency Telecommunications Service (NETS) program; the Commercial Network Survivability (CNS) program; and the Commercial Satellite Interconnectivity program (CSI). These programs are complementary in that NETS enhances switching and control of the PSN while CSN and CSI focus on survivable transmission. See NCS (1988).

### 3.1 National Emergency Telecommunication Service (NETS)

NETS is described by NRC (1987). The NETS program is the largest of the three NSEP programs and is intended to provide survivable, switched voice, and data service by providing switches with enhanced restoration functions. NETS will be voice communications designed to function during and after massive attack when many higher level toll switches and much of the PSTN system is no longer functional. In high stress levels of military attack, much of the common channel interoffice signaling network will likely be destroyed along with the control databases. Normal routing methods will fail, but large portions of the public network facilities should survive.

Under NETS, voice communications would be established by adaptive, nonhierarchical tandem routing (with advanced switching and transmission compensation techniques) through local and toll offices over surviving transmission facilities in the Public Intertoll network. This would be accomplished using Call Control Modules (CCMs) at almost all switching offices to establish voice links adaptively over the surviving network. NETS users will access CCMs by dialing a special area code which the local office will recognize as a NETS call. Control of the call will be forwarded to a CCM which will employ a variety of routing techniques to complete the call. These include trying normal hierarchical routes and a variety of nonhierarchical routes that may be set up through a number of CCMs in tandem. Multistage crankback (whereby blocked calls are cranked back to the originated switch for rerouting) will be used with in-band signaling if calls fail. As a result,

regional information on network status, in terms of successful routing paths, can be exchanged between CCMs. Based on this information, routing tables could be adaptively updated to enable the system to maximize NETS call completion rates in times of increasing damage and reconstruction.

Call completion times could be lengthy (e.g., perhaps minutes), and the resultant transmission quality might be only minimal. Plans are for NETS to interface with most of the carriers, networks, and switch types. More details are given in NRC (1989).

A number of alternatives to NETS have been examined (NRC, 1987) but each has limitations or still depends on the PSN which has the most ubiquity, diversity, redundancy, survivability, and robustness. Alternatives considered include the following:

| | System | Comment |
|---|---|---|
| o | cellular systems | must access PSN |
| o | mobile systems | very localized |
| o | satellites | need many earth stations and large capacity |
| o | ISDN | relies on PSN |
| o | FTS 2000* | relies on PSN |

*FTS 2000 is the upcoming successor to the Federal Telecommunications System, a private network for use by government agencies.

### 3.2 Commercial Network Survivability (CNS)

The CNS program provides a limited number of links to connect user clusters to access points of surviving PSN switching nodes. Thus, it provides local connectivity as from user to node, whereas CSI provides long-distance connectivity between nodes. Together these programs offer major improvements to PSN survivability at relatively low cost.

There are two components to CNS. One is concerned with carrier interconnections that bypass damaged facilities. These interconnections may employ private facilities or existing government networks. The Federal Aviation Administration (FAA) network is one such network to be used. FAA-to-PSN interconnects require software and hardware modifications for the network control.

The second component involves mobile transportable facilities, primarily radio links to provide service for voice and low-speed data during adverse

conditions. A simulated earthquake disaster in 1987 in California provided one test of the concept. See NRC (1989). Transmission quality for voice was satisfactory over six links in tandem using older generation military radios for the links.

### 3.3 Commercial Satellite Interconnectivity (CSI)

The objective of the CSI system is to augment the connectivity of AT&T's interexchange network following a nuclear attack on the Continental United States (CONUS). The links provided by CSI are T1 carriers (24 digitally-encoded voice channels) between specific 4E toll switches within the PSN. The CSI concept is based on commercial earth stations that are within a certain radius of these switches providing a satellite communications link to reconstruct specific long-haul portions of the PSN. Figure 8 illustrates this concept. See NCS (1988).

The CSI system consists of several enhanced earth stations, several Low Cost Terminals (LCTs) and two enhanced control facilities. Since the system will consist of earth stations owned and operated by different carriers, two of the main tasks are to insure that CSI plans and procedures are common to all carriers and that CSI enhancements are implemented in a compatible (i.e., interoperable) manner at the earth stations.

The CSI program is an evolutionary program that is being planned in two phases. Phase I is limited to C-band satellites that have CONUS coverage and are owned and operated by U.S. companies. The associated earth stations are comprised of those owned and operated by commercial carrier companies, but may also include privately-owned and government-leased facilities.

Phase II is the subject of an architectural study that will address the evolution of the CSI program in response to new and emerging user requirements as well as the continuing changes in commercial satellite technologies. The wide proliferation of very-small-aperture-terminal (VSAT) systems, increased use of Ku-band, the introduction of Ka-band resources, and new technology such as mobile satellite terminals, radio determination satellite service (RDSS), and cellular telephone will all influence the development of an updated CSI architecture.

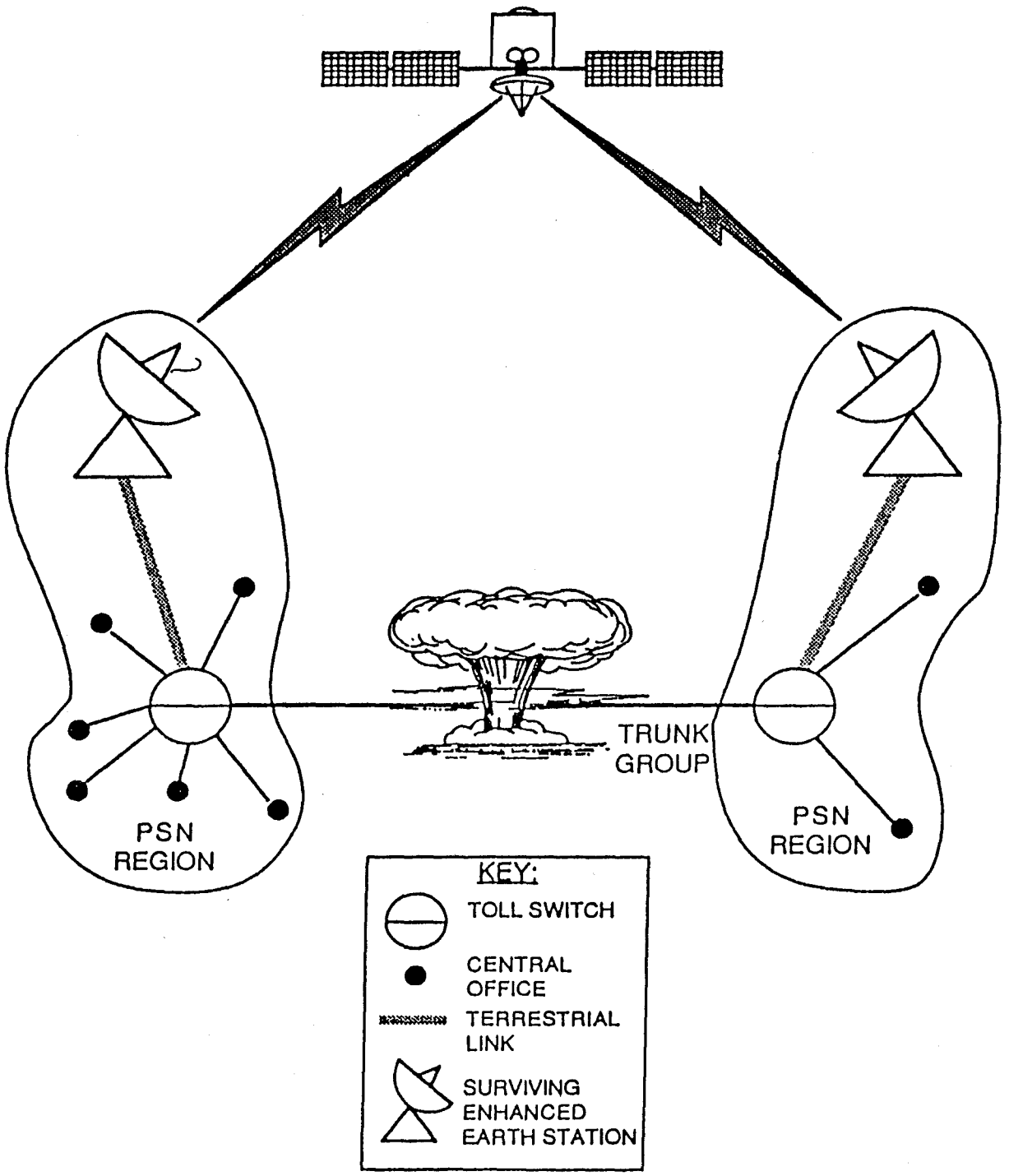



Figure 8. The commercial satellite interconnectivity (CSI) concept.

# 4. PREVENTIVE MEASURES

Preventive measures include techniques installed "a priori" and used to insure continuity of service by minimizing disruptions due to traffic congestion or equipment failures. There are a number of preventive measures already in use on today's networks to reduce traffic load in congested areas. Some of these congestion-reduction measures involve traffic flow controls while others involve alternate routing procedures. For example, telephone networks may restrict incoming calls to a congested area with "busy" tones. For data networks, the input data rate can be limited by signaling the input process to slow down or to stop accepting data until further notice. Congestion problems can also be reduced by routing traffic around congested nodes or by increasing the capacity of these nodes. These strategies are of interest here because many of the same concepts apply for restoring service under damaged network conditions.

In the following sections, some of the more important measures for preventing traffic overloads are discussed. These include reducing capacity requirements by restricting offered traffic, prioritizing traffic, and the design of network topologies to reduce their vulnerability to service disruptions. Network management concepts that have impact on traffic congestion are covered in detail.

## 4.1 Traffic Prioritizing

Traffic carried and network resources can be prioritized during stress situations. This may require specific regulatory or legislative action. Prioritizing users can greatly reduce the restoration capacity requirements. Prioritizing resources reduces the delay in restoring services.

Some of the priority systems in use or being established are given in the following paragraphs.

Telecommunications Service Priority (TSP) Systems. There is an ongoing activity to establish a TSP system that is both effective and can be approved by the Federal Communications Commission (FCC). It provides a regulatory, administrative, and operational system for authorizing and providing priority treatment of NSEP telecommunication services.

Restoration Priority System (RPS). There already exists a Restoration Priority System that is administrated under FCC 80.581 as follows:

- All Government requests for priorities are certified by the NCS and included in the service authorization. Each quarter NCS sends a computer printout of all Government restoration priorities (RPs) to the FCC for official certification. The FCC, in turn, sends copies of these printouts to the concerned carriers. All Government interstate RPs are forwarded to the Long Lines - Restoration Priority Coordinator who maintains a database of about 10,000 RP services. The BOCs administrate about 6,000 interstate RP services. The FCC sends individual BOC printouts to the AT&T Restoration Priority Coordinator who forwards them to the individual BOC RP coordinators.

- Non-Federal Government RPs are certified directly by the FCC using Form 915. Since there is a time lapse between the user request for an RP and the FCC certification, the requested service is usually ordered and in the engineering process before certification. The FCC sends the Form 915 certification directly to the common carrier sales office at which time a supplement must be issued. The organizations involved in this phase of RP Administration are the AT&T Restoration Priority Coordinator and Long Lines and BOC Coordinators.

Trunk Reservations. Section 606A of the Communications Act of 1934 allows the President, upon proclamation of threat or state of war, to authorize the seizure or exclusive usage of any facility upon just compensation to the owners. The difficulty in determining "just compensation" for individual toll trunks held out of service by the carriers is that these unit costs are not commonly available nor used in tariff. Furthermore, the cost and revenue characteristics of Intertoll Trunks are significantly different from subscriber-to-subscriber private lines.

## 4.2 Fault-Tolerant Networks

There are a number of ways to design networks that are less susceptible to stress conditions, whether they be overloads or damage. Some papers describe fault-tolerant networks (King, 1987) which basically introduce different fault-detection/service-restoration systems under the generic term of network management. Wu et al., (1988) addresses survivable network architectural issues for fiber optic networks. A number of topologies are considered and evaluated in terms of affordable survivability. For local network architectures, self-healing ring structures improve survivability.

Ring networks are also addressed by Ergle (1989) and Helmes (1989). One type of ring network uses time-division multiplexing and two fibers to connect

central offices to remote nodes. A loopback occurs at nodes adjacent to cable cuts. See Figure 9. Another type is the cable ring that contains many point-to-point fiber links. Each type has its own advantages and disadvantages. It is also possible to provide route diversity in the fiber network so that working and protection fibers are not in the same cable. If one fiber is cut the other can carry the traffic. Ring diversity switches (RDS) can be used in fiber optic rings. The RDS creates mirror-image high-speed digital signals and sends them in opposite directions on the ring. If a major service disruption occurs, at least one of the signals should arrive. These structures are designed primarily to enhance the survivability of local loops and wide-area networks. For the long-haul networks there are a number of topologies used such as trees, stars, loops, and partially or fully connected mesh configurations. Only the last one appears to have sufficient route diversity to provide any significant survivability. But this fully connected mesh topology is relatively expensive because of the number of links involved. It appears that some form of a structured configuration would be beneficial.

One example of a fault-tolerant network is the structured network described by Nesenbergs in the reference by Linfield et al., (1980). This structured concept is shown in Figure 10 for an arbitrary number of N nodes. The nodes are ordered in accordance with the number of terminals they serve. If $T_n$ is the number of terminals for the n-th node, then the ordering is

$$T_1 \geq T_2 \geq T_3 \geq \ldots \geq T_N \quad .$$

Thus, in this sense, $T_1$ is the largest node. $T_2$ is the next largest node, and so on. Finally, $T_N$ is the smallest. The nodes or switches are identified by $n = 1, 2, \ldots, N$. The individual number of terminals n at a node is $T_n$, $n = 1, 2, \ldots, N$. The link capacities between nodes n and m are $C_{nm}$, $N \neq m = 1, 2, \ldots, N$. The key question that must be answered is how the structured configuration link capacities $C_{nm}$ should be assigned to meet survivability objectives. Effective capacity assignment must be a function of the user terminal set, telecommunications traffic requirements, and other general design objectives.

Figure 11 compares the number of links necessary to implement this with those required in other more common network types. The structured configuration appears to offer reasonable survivability at the least cost.

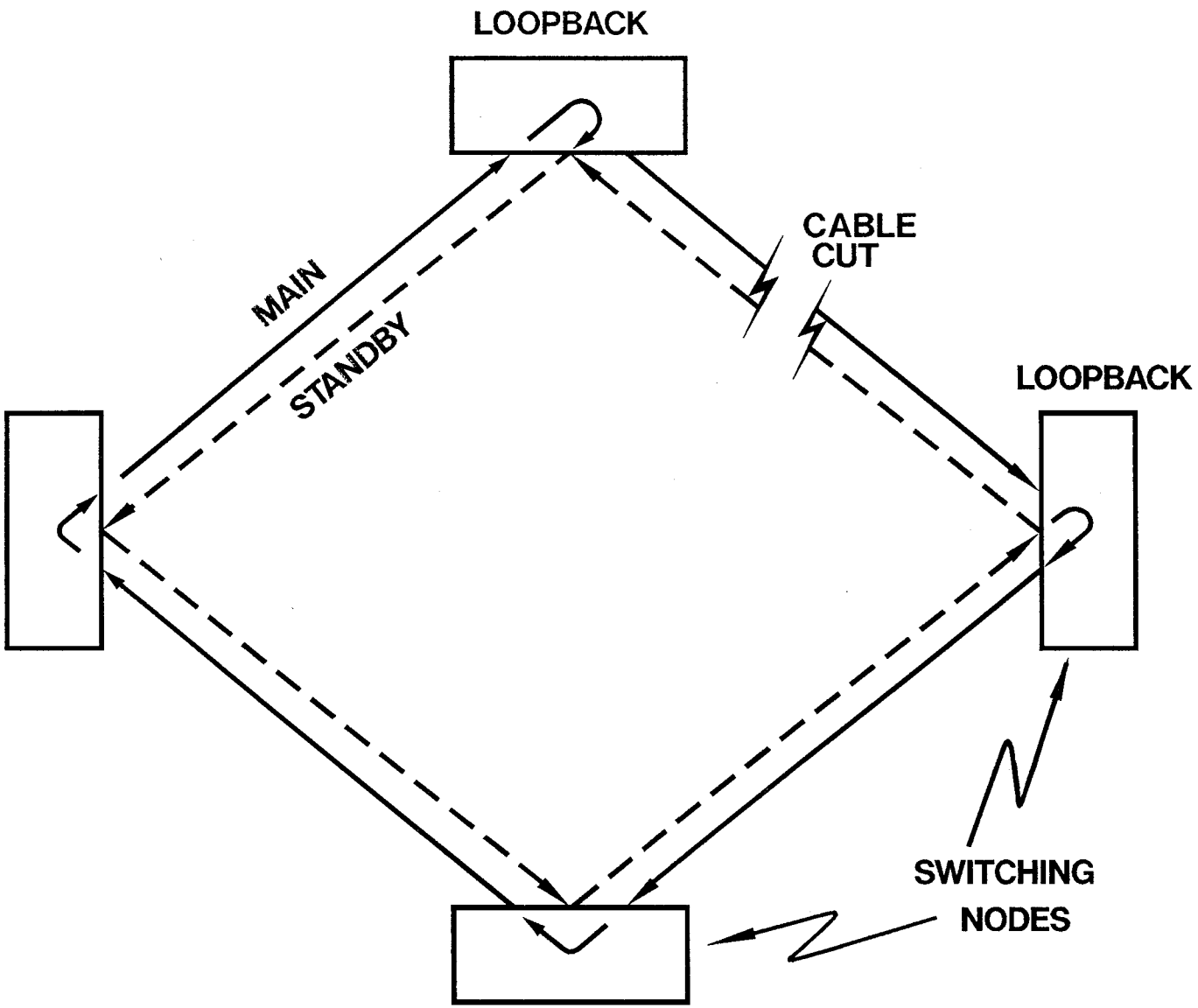



Figure 9. Fault tolerant network using two fiber rings.

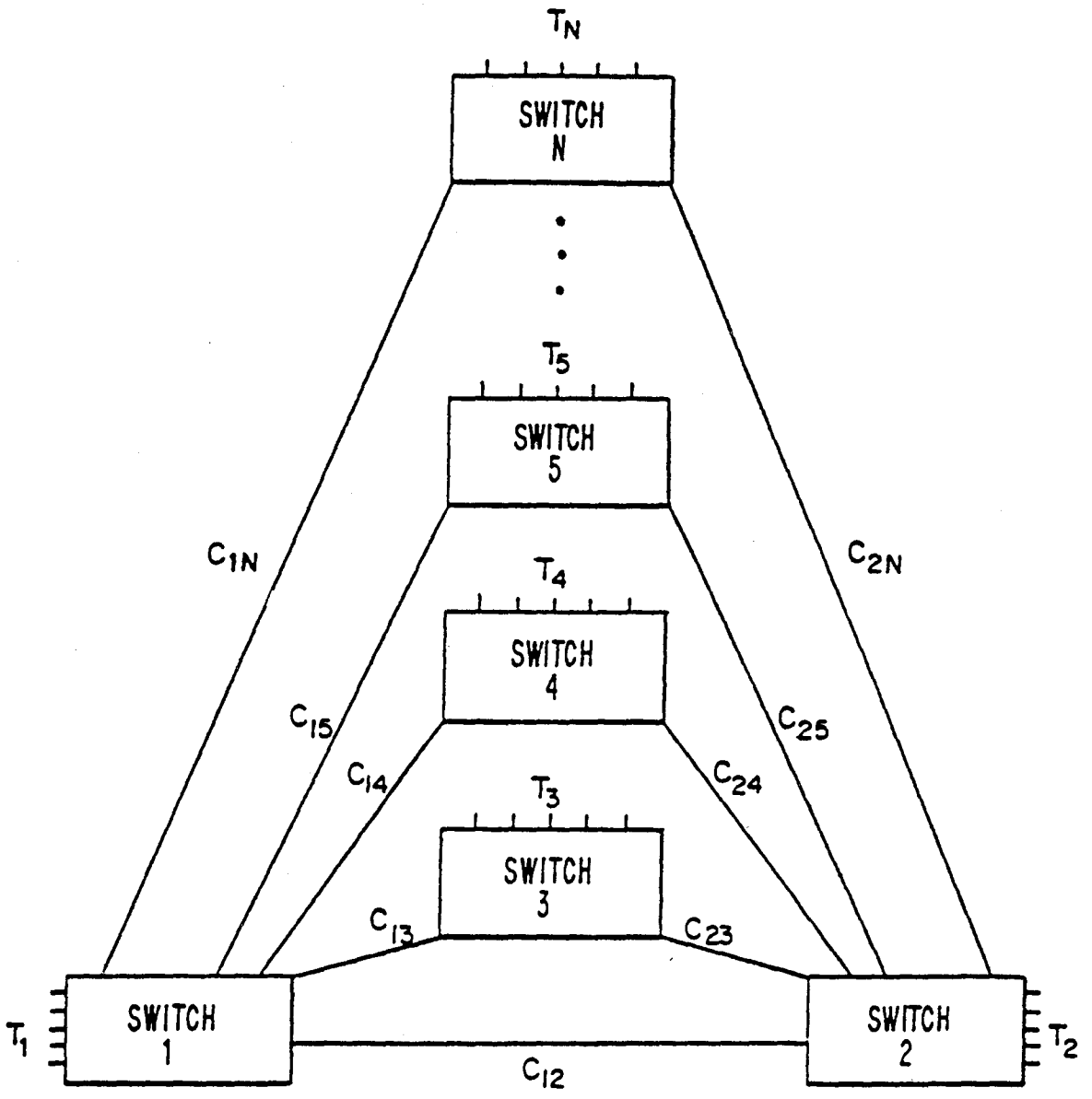



Figure 10. The general structured configuration of a fault-tolerant network.

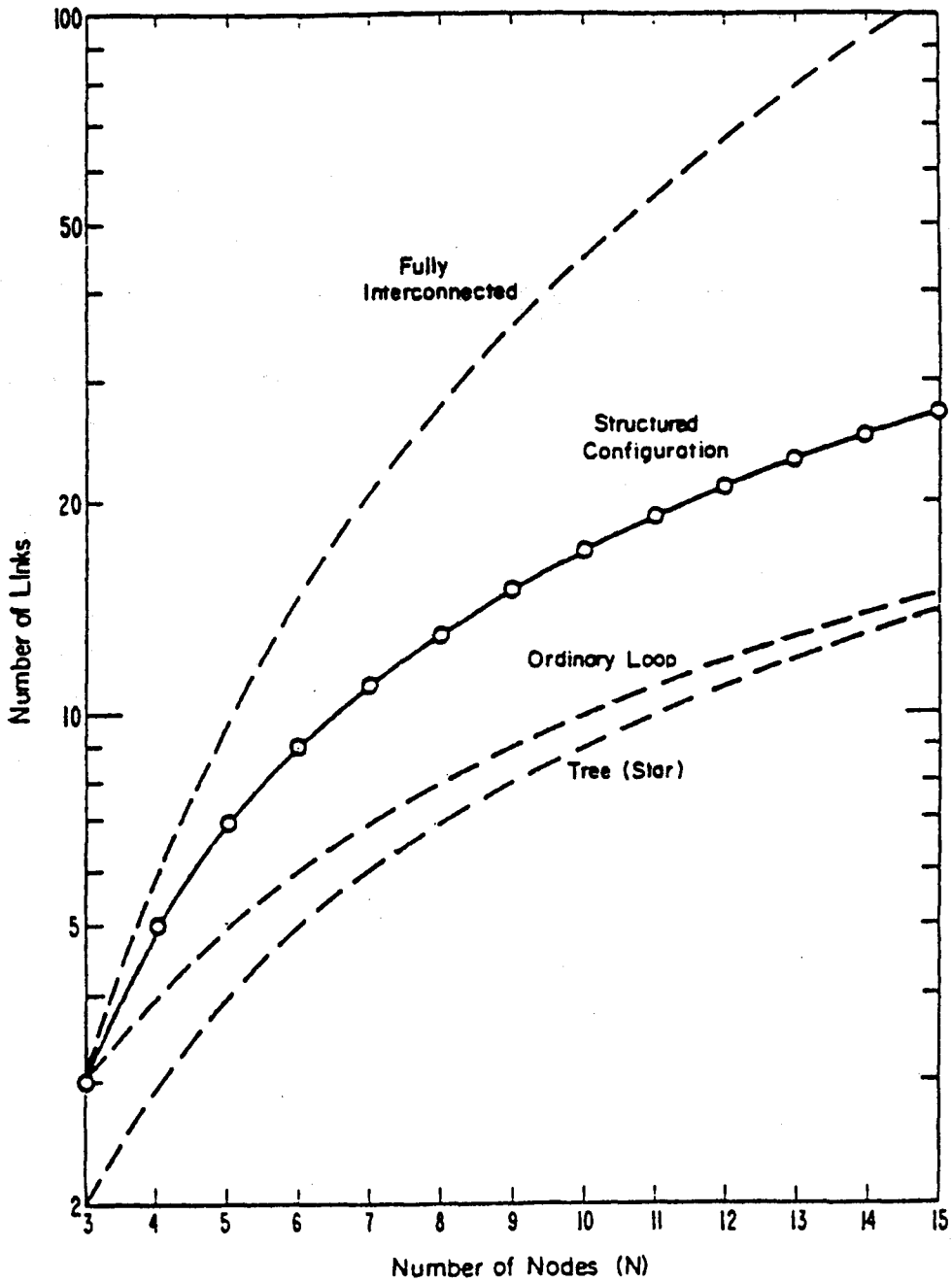



Figure 11. The number of links required by several common topologies.

## 4.3 Network Management

There are a number of network management concepts that have a direct impact on traffic congestion problems, trouble shooting, network configuration, flow control, and the like. According to Reedich (1987) a comprehensive network management and control system must support "the monitoring of network port and trunk link status; the detection and isolation of system faults and deteriorating conditions; automatic or manual alternatives of network configurations and parameters; the ability to diagnose and switch both analog and digital lines; the generation of traffic and event statistics as needed; and the ability to produce a variety of comprehensive management reports."

Others (e.g., King, 1987) use a three-level definition beginning with technical control, network control, and at the highest level network management. Still another view categorizes the network management functions in terms of time. The management functions may range from real-time (seconds and minutes) flow-control functions to long-term (weeks or months) strategic planning functions.

Network management for preventive and corrective actions tends to focus on the immediate problems affecting service provisioning. Two key roles of network management are: 1) fault identification procedures that include alarm monitoring and diagnostics and 2) service-restoration procedures that include fault isolation, bypassing faults or alternate routing, and switchover. Another related role is performance monitoring to analyze operating conditions and potential overloads in order to predict faults and configuration decisions. These are primarily preventive measures, so a secondary role of network management is statistical reporting and strategic planning. These then provide the longer term corrective measures like installing new facilities to add capacity. In a subsequent section, we discuss network management functions such as overload controls, alternate routing, facility selection, and network reconfiguration. All of these functions are directed toward preventing service disruptions.

### 4.3.1 Overload Controls

As the offered traffic load increases on any network, it ultimately reaches and may exceed the design load limit. When this design limit is reached the network becomes congested, equipment pools become exhausted,

delays occur, traffic is blocked and efficiency is drastically reduced. Such overloads occur during periods of extremely high usage (e.g., Mother's Day and Christmas) or when damage (e.g., cable cuts and switch outages) reduce the network traffic carrying capacity. As the offered load increases beyond the point of congestion, the carried traffic may actually be reduced below the engineered capacity unless specific control measures are introduced. These controls may be implemented manually or, more likely today, automatically. The controls are considered to be either protective or expansive. A protective control restricts traffic to a congested switch by sending congestion notifications to adjacent switches. An expansive control is a real-time routing algorithm that automatically reroutes traffic under overload conditions. Several alternative routing schemes are discussed in the following subsection.

### 4.3.2 Alternate Routing

Various methods for routing circuit-switched traffic are described by Hurley et al., (1987). A key method for alleviating traffic congestion is called alternate routing. With early systems, this was accomplished with manual patch cords. Later, automatic routing methods were used. In its simplest form an automatic scheme called direct routing was established progressively from dialed digits using step-by-step switches. Later, crossbar switches augmented with control units chose the best route based on the traffic loading on trunk groups. This was the first form of alternate routing.

Figure 12 distinguishes between these alternate and direct routing methods and also provides additional categories of alternate routing--namely hierarchical routing and adaptive routing. Hierarchical routing is based on a fixed definition for the toll switching connections between several classes of switching centers. A rigid set of routing rules determines the trunk group selected for each call. In 1984, AT&T introduced adaptive routing in the toll network whereby alternate routing tables are no longer rigid but change dynamically with time of day, season, or random traffic variations. Figure 12 indicates two kinds of adaptive routing - state dependent and time dependent. In the paragraphs below, we describe the three adaptive routing concepts that are currently in use or being seriously considered. These are Dynamic Nonhierarchical Routing (DNHR), used in AT&T's long-haul network, Dynamic

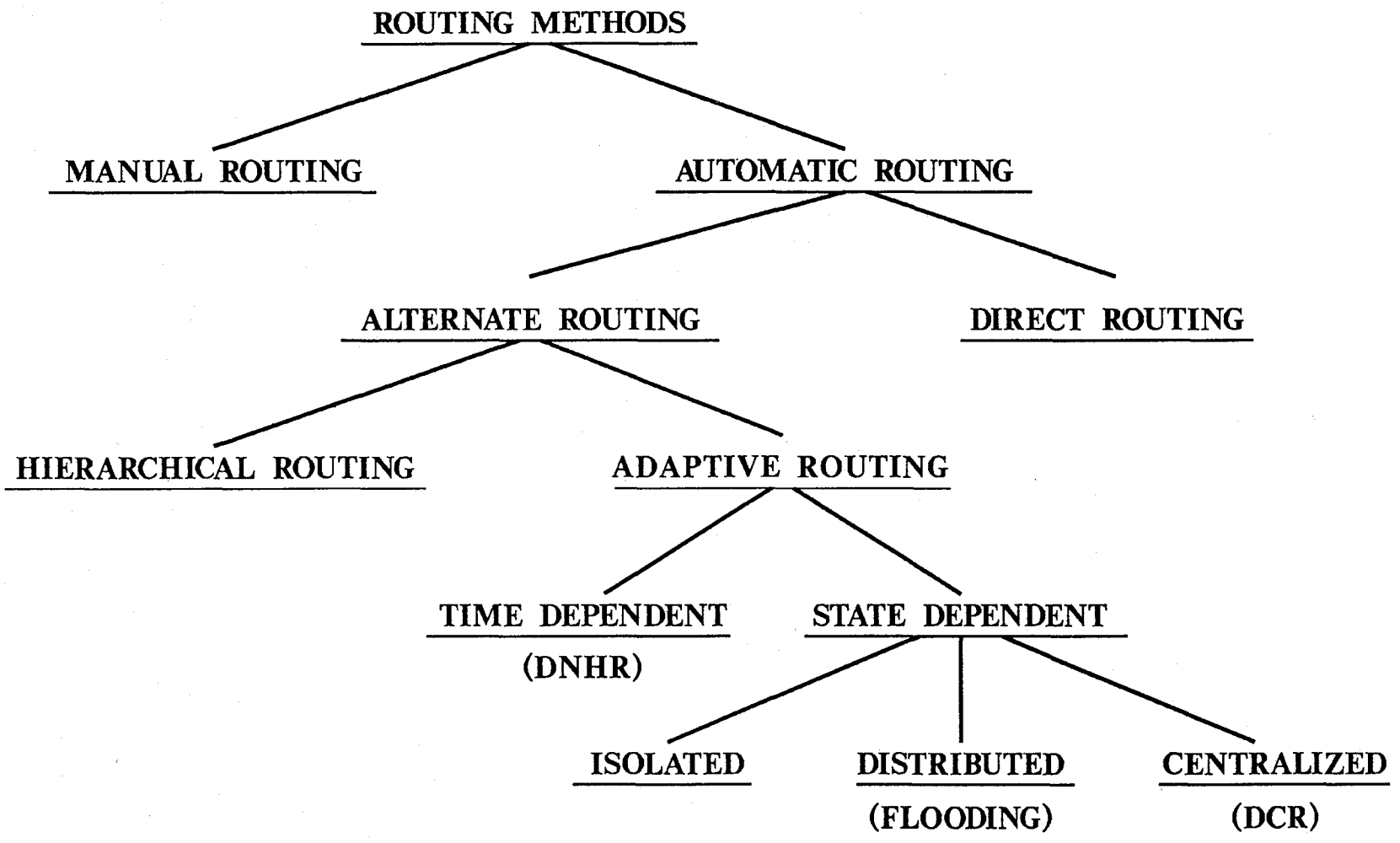



Figure 12. Routing alternatives.

Controlled Routing (DCR), being considered for use in Canada, and "flooding", a distributed routing method that has been identified for use on the Defense Switched Network (DSN).

Dynamic Nonhierarchical Routing (DNHR). The architecture of AT&T's long haul network is gradually being converted to this flexible system that permits fast, partially-automated rerouting of telephone traffic around trouble spots. The signaling network stores alternate paths, called "vias", for use if the best path is unavailable. These "vias" can be changed to reflect changes in traffic patterns.

Under DNHR, the switch systems will be classless and completely equivalent in their functions. Computer-controlled intelligence that has been built into the switching and trunking network is used. Predetermined routing patterns are changed as a function of measured and forecasted customer-calling patterns. Because DNHR makes efficient use of the network's existing capacity, it is expected that hundreds of millions of dollars will be saved by eliminating construction costs for new transmission facilities over the next 10 years.

Three kinds of traffic are handled by the DNHR network (see Figure 13):

1) Traffic that originates in different exchange access areas, but connects to DNHR switches--this traffic originates/terminates in exchange access networks 4 and 1.

2) Overflow traffic from the hierarchical network--this traffic is between exchange access areas 4 and 3.

3) Through-switched traffic loads from the hierarchical network--this traffic exists between exchange access networks 4 and 2.

The end result of the DNHR backbone structure is that it alleviates congestion at critical points in the network and provides better services at less cost. It is apparent than DNHR has application not only in preventing focused overloads but also when damage occurs on the network.

Dynamic Controlled Routing (DCR). This is a centralized concept whereby a centralized network processor recommends different new routes to participating exchanges in near-real time (minutes or less). This contrasts with DNHR that used nonreal time (hours) calculations to select routes. With DCR, the network is susceptible to the failure of the network processor because it must continually update routing recommendations. The DCR concept

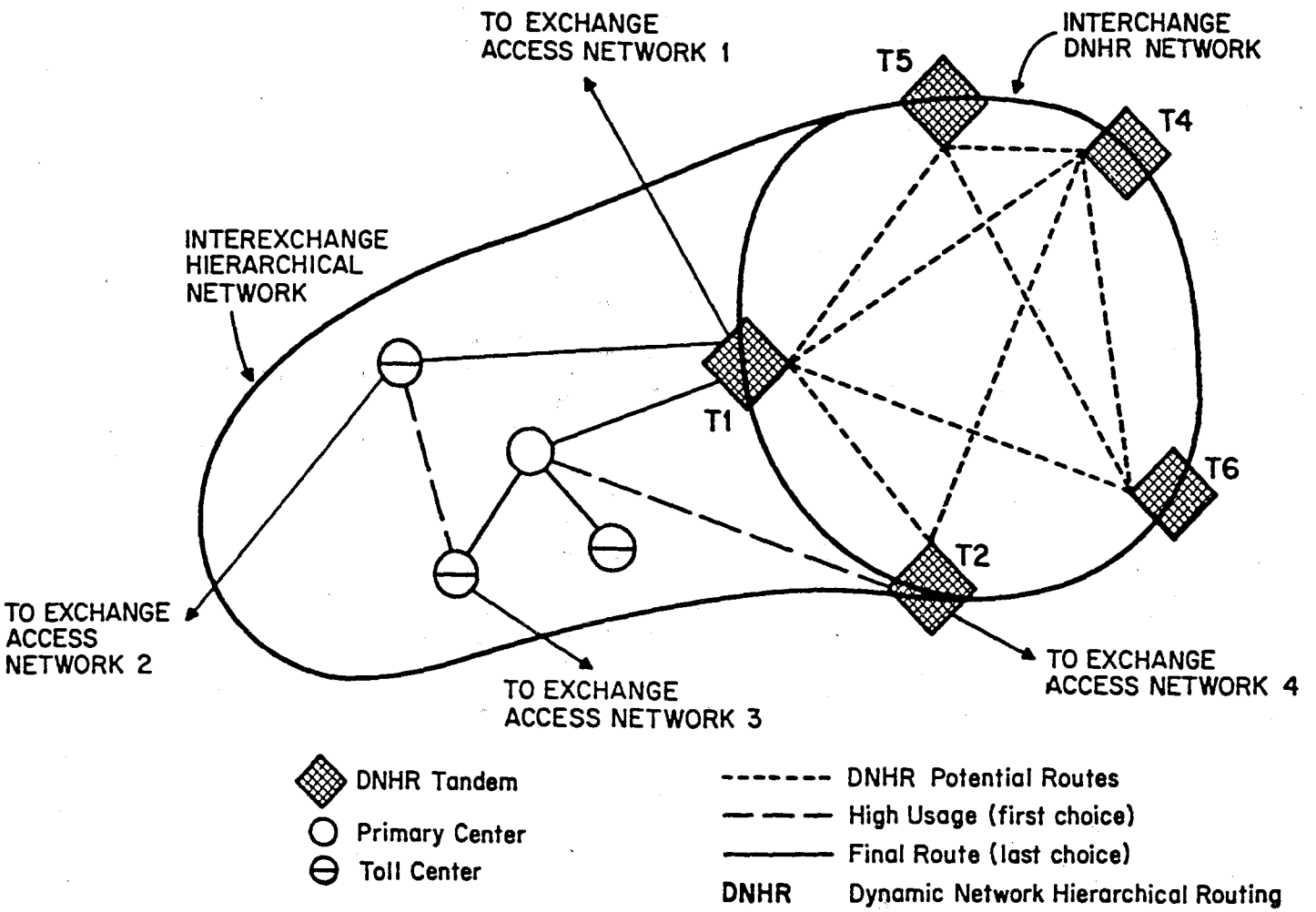



Figure 13. Dynamic nonhierarchical routing (DNHR).

is being considered for use on the Canadian public switched network and may be implemented in the near future.

Flooding. When network congestion information is sent over the communication network (e.g., in-band rather than over a separate signaling network), then it competes with the user traffic. One such adaptive routing algorithm is known as "flooding". With "flooding" the optimum route is determined on a per-call basis by seizing the first response from the network that ensues from an "all-points broadcast" or flooding on available routes to a particular destination. This has important applications on military networks such as DSN. The DSN also has a multiple level precedence preemption (MLPP) procedure that allows lower precedence calls to be terminated in order to complete higher precedence calls. The signaling system on the DSN (CCITT No. 7) provides the means to inform remote exchanges of network failures and alternate routes. This is accomplished by sending search messages on all possible routes (i.e., flooding the network) to all destinations. The optimum route can then be selected based on fewest links, traffic status, and preemptions.

### 4.4 Other Preventive Measures

There are many other measures that could be used and are used to reduce network congestion and improve performance or enhance survivability. Here we list a few of these other measures with only brief discussions.

Resource Selection. It may be feasible to select certain facilities in order to enhance network survivability and reduce restoral requirements. Examples include the following:

| Facility | Purpose |
|---|---|
| underground trunks and lines | these facility selections permit special calls to be routed via underground transmission links in certain geographic areas |
| no-satellite | prevents call detection and eliminates delay |
| end-to-end digital | may be required for encryption. |

Enhanced Features. Today's networks provide means to implement a number of features that can be used to reduce congestion during periods of overload. These features can be used on virtual private line networks (VPLN) imbedded in the public switched network. They include:

- o Call screening. This feature may be implemented during periods of stress. Certain categories of calls would be blocked. For example, calls into a focused overload area would be blocked at the source.

- o Authorization code. This is a form of prioritizing calls but applies to individuals rather than stations.

- o Internetworking or interconnectivity of different networks. This allows users to connect to other prearranged networks in case of failure of certain nodes or links.

Artificial Intelligence. There are several network management functions, such as diagnosing traffic overloads, that require the intervention of an expert. Increased automation will utilize software algorithms to perform diagnostics and expert systems to determine the nature of the overloads. Pattern recognition adaptive systems, and other artificial intelligence technologies may be used. See Hara et al., (1987).

## 5. CORRECTIVE MEASURES

Corrective measures are those methods used to restore service after disruptions have occurred due to unforeseen equipment failures or network damage. Corrective measures are taken after the disruption occurs and therefore involve some delays in service restoration.

### 5.1 Reconfiguration Techniques

There are several systems available today that allow network reconfiguration in essentially real time. Such systems provide another means of restoration - namely bypassing damaged or inoperative network elements.

Digital Access and Cross-Connect Systems (DACS). A basic digital access and cross-connect system (DACS), sometimes termed Digital Cross-Connect System (DSX) may have a wide range of capacities. One example provides up to 1524 cross-connect circuits among 3072 DS-0 (64 kb/s) channels carried on 128 T1 transmission facilities. A DS-1 channel carries 24 DS-0 channels at 1.544 Mb/s. The DS-1 signal may be transmitted via a T1 carrier line to the

DACS for rerouting as desired. Figure 14 shows the basic idea of how a DACS performs its access and cross-connect functions.

A new subrate data cross-connect feature, recently announced, will provide switching of subrate signals at 2.4 kb/s, 4.8 kb/s, and 9.6 kb/s within the DS-0 channel. At this time, however, only a few vendors offer a DACS-like capability and interworking between systems offered by different vendors' DACS is not yet possible.

One application of a DACS could be for dynamically switching bundled trunk facilities for either voice or data traffic on a near-real time basis.

Customer Controlled Reconfigurations (CCR). There are, of course, many different ways to control the network connectivity or topology and certain private network functions. Here we describe one method that allows the customer to control his private network's topology and certain features by accessing the network's control center.

The traditional approach of the local telephone companies (i.e., BOCs) has been to place private network control in the central office using centralized processing intelligence. More recently some carriers now allow the customer to control some portions of his network's database. This innovation permits customers to change dynamically the topology, user groups, and feature options as defined in the database.

One such scheme for controlling topology is shown in Figure 14. In this system, the CCR allows the user to reconfigure a network consisting of a number of DCSs connected by leased transmission circuits. Control is from a central computer. This is accomplished in the DACS at the DS-0 level by changing the software instructions to each DACS. Figure 15 is an example of the CCR used for control of three DACS systems.

## 5.2 Bypass Systems

There are a number of technological advances that will almost certainly influence the provisioning of services over the next decade or two. Here we can only describe a few of the more important new advances that could have bypass capabilities.

In the following paragraphs, we summarize several transmission technologies that have the potential to bypass the public facilities under stress conditions. These include microwave radio systems, cellular radio systems, satellites using very-small-aperture terminals (VSATS), and fiber

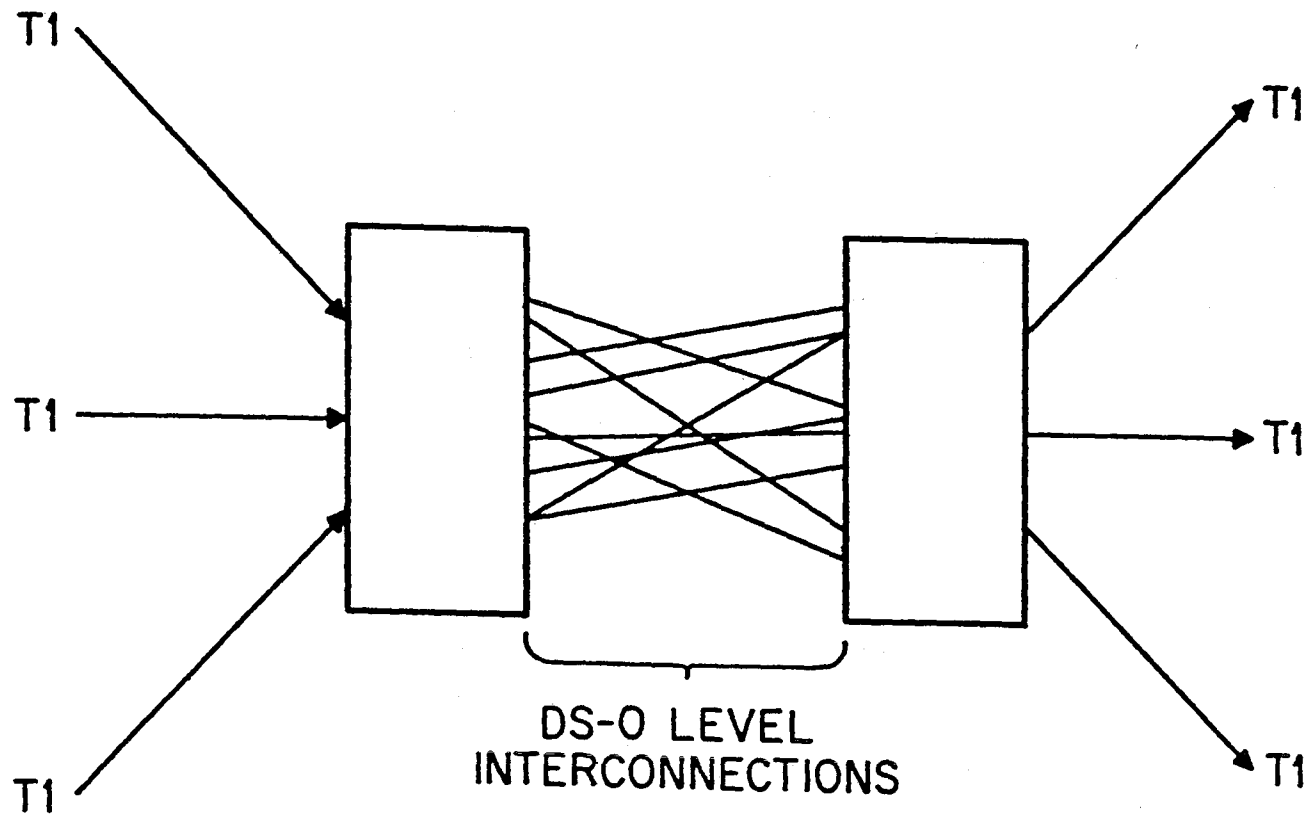



Figure 14. Digital access and cross-connect systems (DACS).

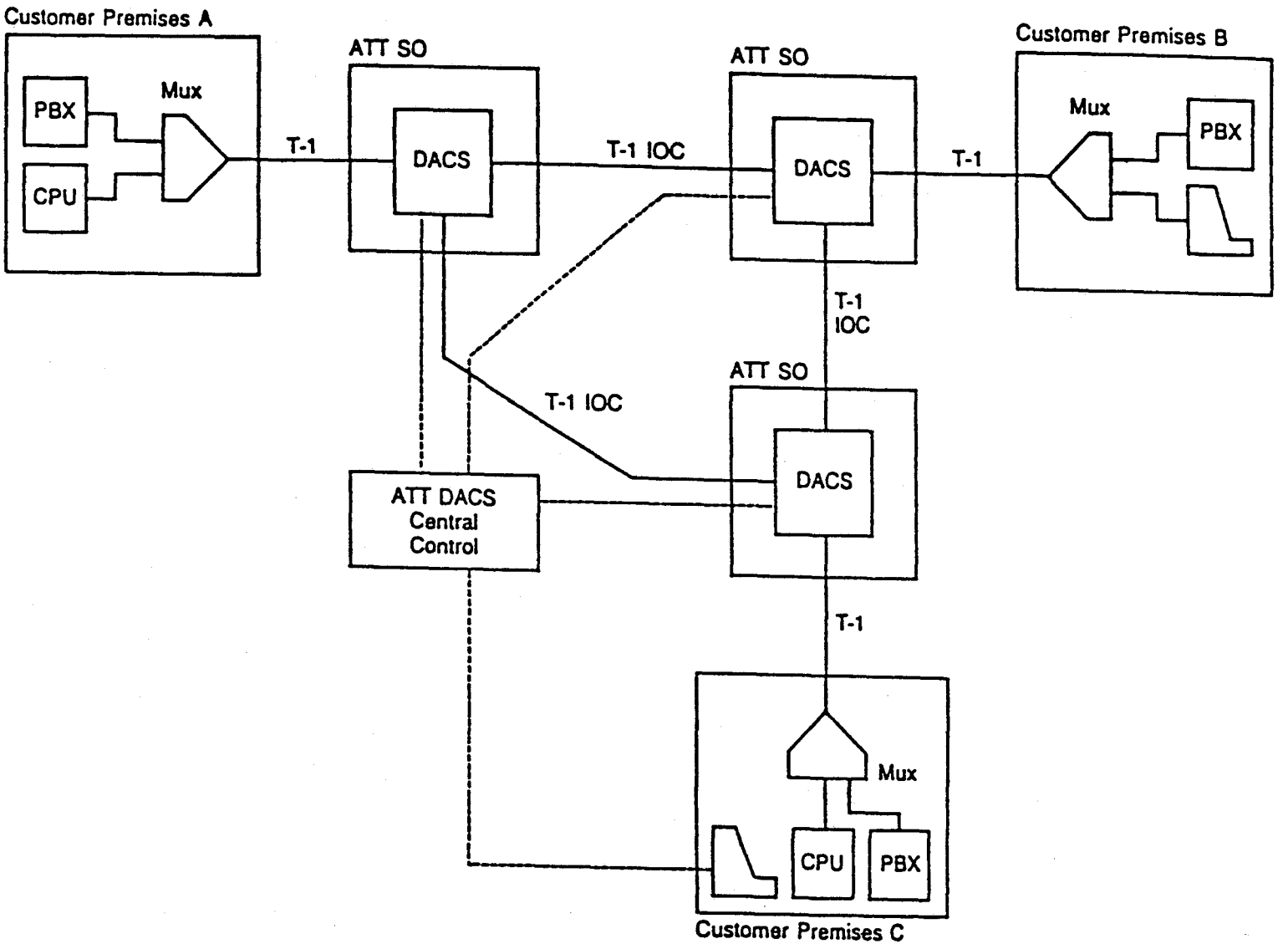



Figure 15. Customer-controlled reconfiguration used by AT&T.

optic systems. Some of these systems may be addressed in Phase II of the CSI program as noted earlier.

Microwave Radio Systems. Microwave radio systems in 1985 carried over 80% of domestic long-haul telephone traffic, and are the backbone of the long-distance telecommunications network. This percentage is probably much lower today due to the introduction of fiber transmission facilities.

The "bypass" trend, which allows a company to send transmissions over communication routes other than the traditional public telephone network, should substantially expand the market for digital microwave systems. Several companies sell microwave radio equipment that allows a customer to establish a direct digital link to an interchange carrier's point of presence. Although such a microwave link costs about $25,000, the payback period can be as short as two years. Microwave is a common option for facility bypass because few companies have the rights-of-way to install terrestrial cables. However, the implementation of microwave technology in large urban areas is already limited by spectrum congestion.

Microwave systems are often the easiest communications systems to install. Some configurations can literally be put into service overnight. Although FCC approval is required, the application process is relatively short and free of red tape. The application process can be initiated well before actually deciding on a specific vendor. The speed with which some microwave systems can be installed also eliminates the time and costs involved in laying cable, especially in remote geographical locations or in crowded metropolitan areas. Small portable microwave antennas permit the rapid deployment of a temporary communications link in case of natural disasters.

Figure 16 illustrates two key trends in digital microwave radio technology--increasing capacity and declining cost. Capacity per unit of bandwidth increased by almost a factor of 3 between 1975 and 1987, and an essentially linear extension of that trend is projected through the year 2000. Cost per voice channel is expected to decline throughout the 1990's.

Cellular Radio Systems. These systems divide service areas into "cells" with each cell having its own transmit/receive antenna operating on a different frequency from adjacent cells. Each antenna is linked to a mobile telephone switching office (MTSO) which connects to the local central office. Calls are handed off from cell to cell as a user traverses the service area. Some MTSOs cover small service areas which may be interconnected via satellite

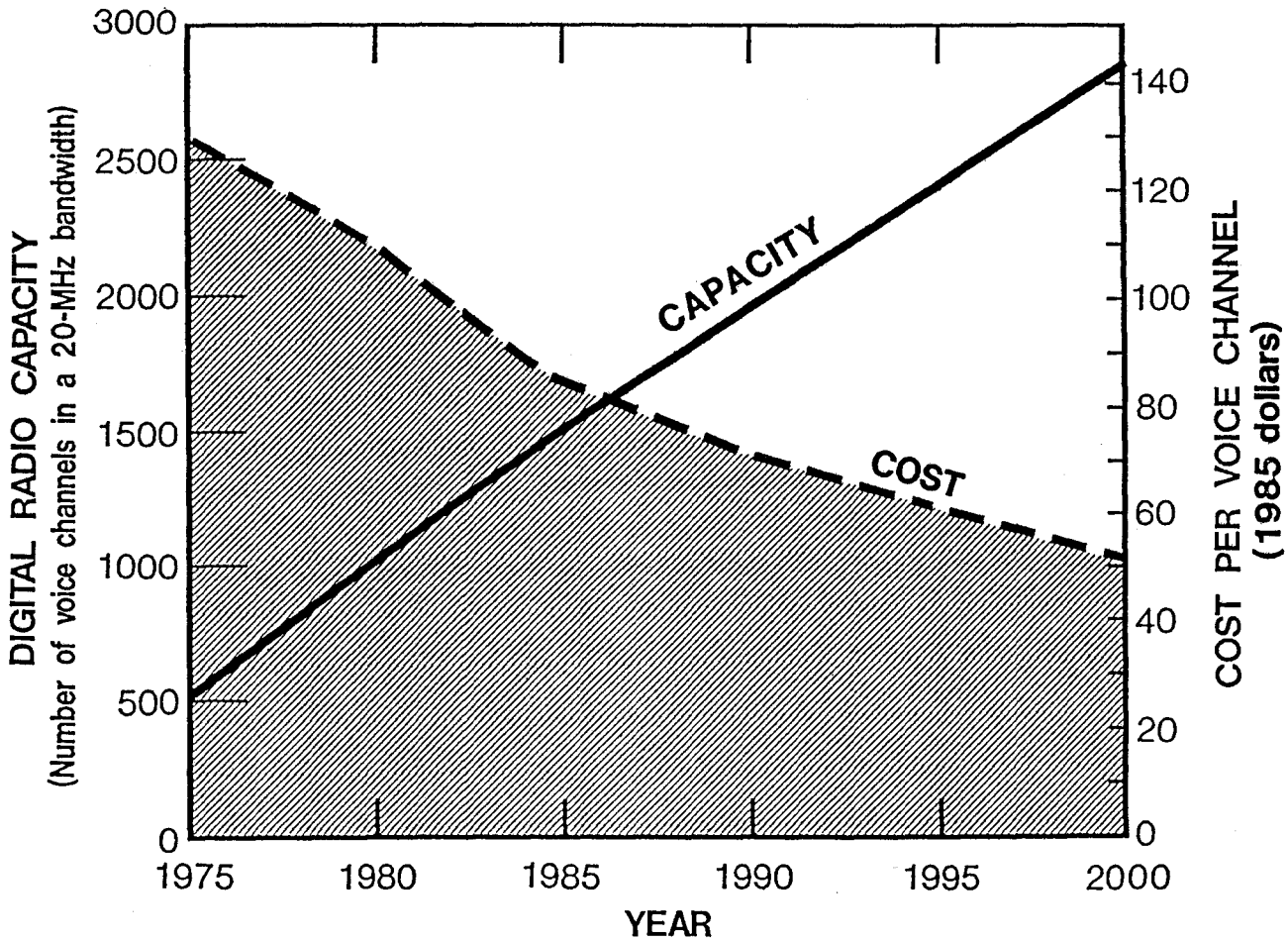



Figure 16. Trends in digital microwave technology.

links to other service areas. Such systems, if properly implemented, could be used under stress conditions to bypass damaged facilities.

Fiber Optic Transmission Systems. The past and projected milestones of fiber performance are depicted in Figure 17. See Kao and Basch (1988). Note that a bandwidth-distance product of 1000 GHz • km may be feasible in the 1990's. Currently, fiber systems are capable of handling bit rates of about 2 Gb/s. Future fiber transmission speeds may reach 10 Gb/s, which would provide transmission speeds far greater than their terminal signal processing speeds. Thus, bandwidth conservation may no longer be an important aspect of future overall information system design. In fact, such systems may purposely waste bandwidth if this simplifies the design and yields a more cost effective system.

Satellite Systems. Major technology advances are also being realized in satellite communication systems, which recently carried over 60% of the world's intercontinental telecommunication traffic. This percentage is coming down as transoceanic fiber systems are installed. A comparison of technical characteristics between INTELSAT I and INTELSAT V (1965 to 1980) revealed a 13-fold increase in the number of telephone circuits; and a 5-fold increase in expected satellite lifetime. This increase may continue but fiber also continues to be more competitive.

Very-small-aperture terminals (VSATs) operating in the Ku-band with antenna diameters on the order of 1 to 2 meters are capable of T1 transmission rates (1.544 Mb/s) to multiple users. Using time division multiple access (TDMA) or single channel per carrier (SCPC), this VSAT technology appears to be competitive with digital data services and the packet switched networks. See Chakraborty (1988).

As impressive as these statistics are, they are overshadowed by the planned introduction of a totally new kind of satellite technology in the 1990's. Conventional satellites essentially act as "bent-pipes" in the sky--receiving and amplifying an RF signal from one earth station and retransmitting it, without demodulation, to another. NASA has undertaken the development and demonstration of an Advanced Communications Technology Satellite, ACTS, that will provide on-board demodulation and switching of baseband signals. These signals will be selectively distributed to anyone of several dozen earth points, based on control signals relayed from the transmitting terminal. In effect, ACTS will put the switching capability of a

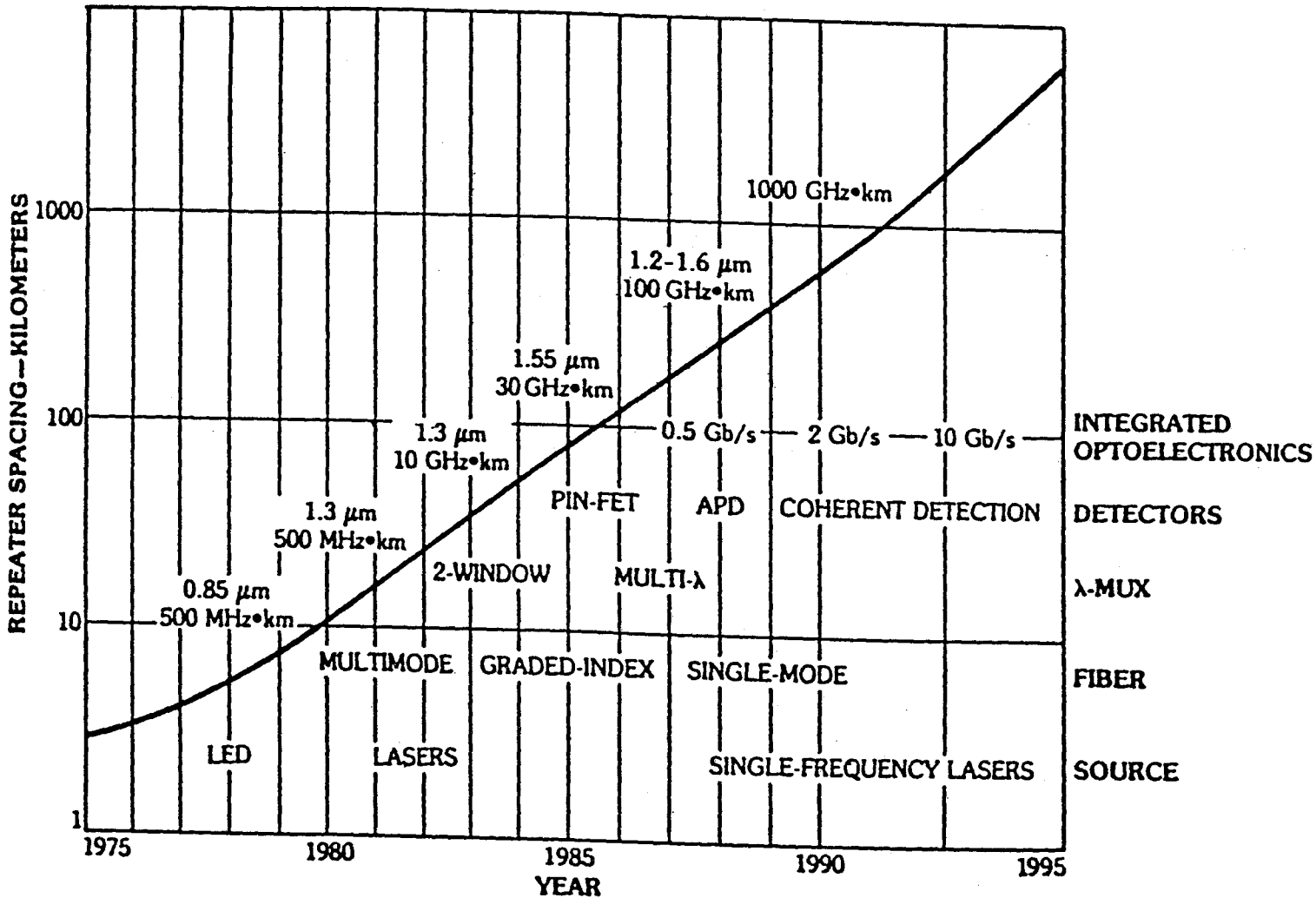



Figure 17. Past and projected milestones of fiber performance.

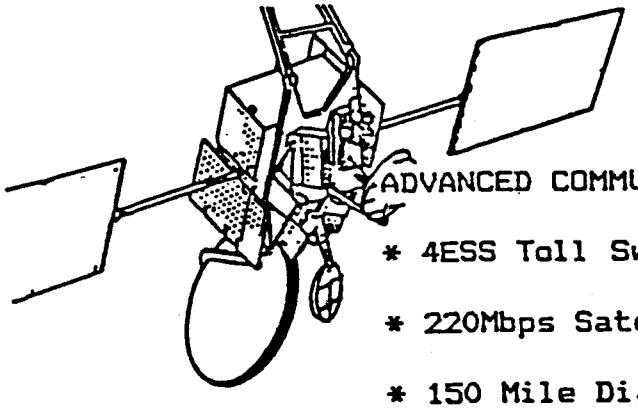
large toll switch in synchronous orbit--and make any fraction of its maximum 220-Mb/s capacity available to specific users after an access request. Phased-array antennas will enable switching of 150-mile-wide spot beams among any number of earth points on a microsecond basis, and will provide dramatic improvements in spectrum efficiency through frequency reuse. The development of Ka-band (30/20 GHz) technology will expand available bandwidth by a factor of 5, and will reduce the minimum earth station antenna size to 0.3 meters--a factor of 10 reduction in comparison with older C-band equipment. Circuit availability will be substantially improved through the use of Forward Error Correction (FEC) for on-board rain-fade compensation. Key features and planned coverage of the ACTS system are summarized in Figure 18.

ACTS has the unique capability to enhance not only the switching and control elements but also the transmission elements of terrestrial networks, both public and private. This is in contrast to the NETS program which primarily focuses on switching and control and the CNS and CSI programs that focus on transmission. (See Section 3.) For a more detailed description of ACTS, see Nesenbergs (1989).

Relative Costs. The relative costs for three competing long-haul transmission systems were evaluated some time ago and are compared in Figure 19. See Telephony (1984). These are averaged costs of geostationary satellite systems, point-to-point terrestrial microwave systems, and optical fiber systems. The figure shows relative circuit costs per month in 1984 dollars. These data are five years old, so the relative costs may still apply but the actual costs may vary widely. The recent surge in implementing fiber optic circuits in the United States is due to the fact that fiber optic costs are significantly lower than shown here.

### 5.3 Transportable Restoration System

Recent tests of portable telecommunications systems are described by Boensch et al., (1989). The purpose of these tests was to demonstrate one method for restoring telecommunication services rapidly to an area that becomes isolated from the public switched telephone network (PSTN) due to a natural disaster or other emergency. A commercially available C-band satellite earth station, a transportable cellular telecommunications system, and a digital microwave system were deployed to a Department of Energy plant in Florida following a simulated disaster. These tests verified the



ADVANCED COMMUNICATIONS TECHNOLOGY SATELLITE

* 4ESS Toll Switch in the Sky
* 220Mbps Satellite Switched-TDMA Trunks
* 150 Mile Diameter Scanning Spot Beams
* 30/20 GHz Technology
* On-board FEC Rain-fade Compensation
* LASER Communication

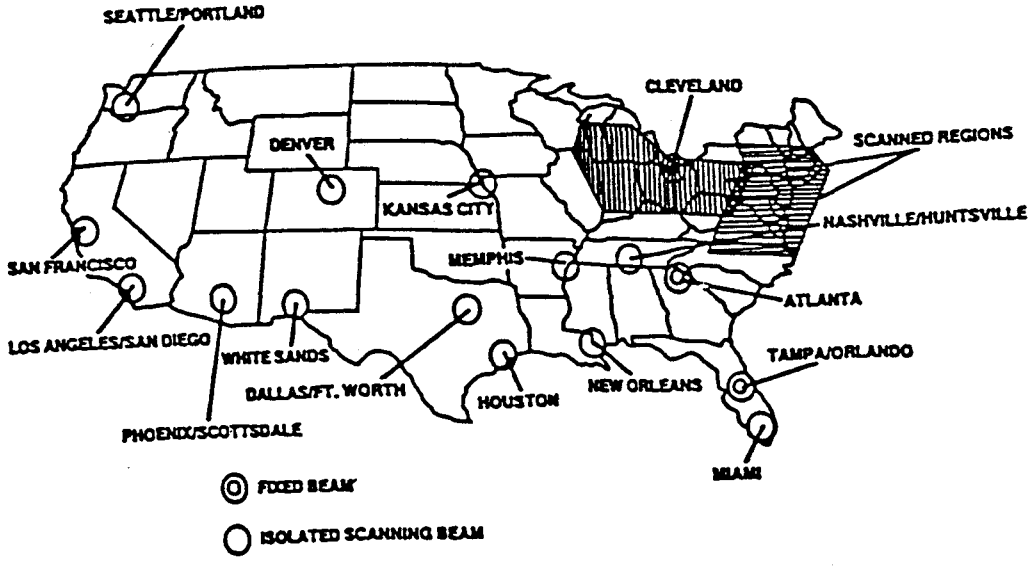



Figure 18. Key features of the ACTS technology.

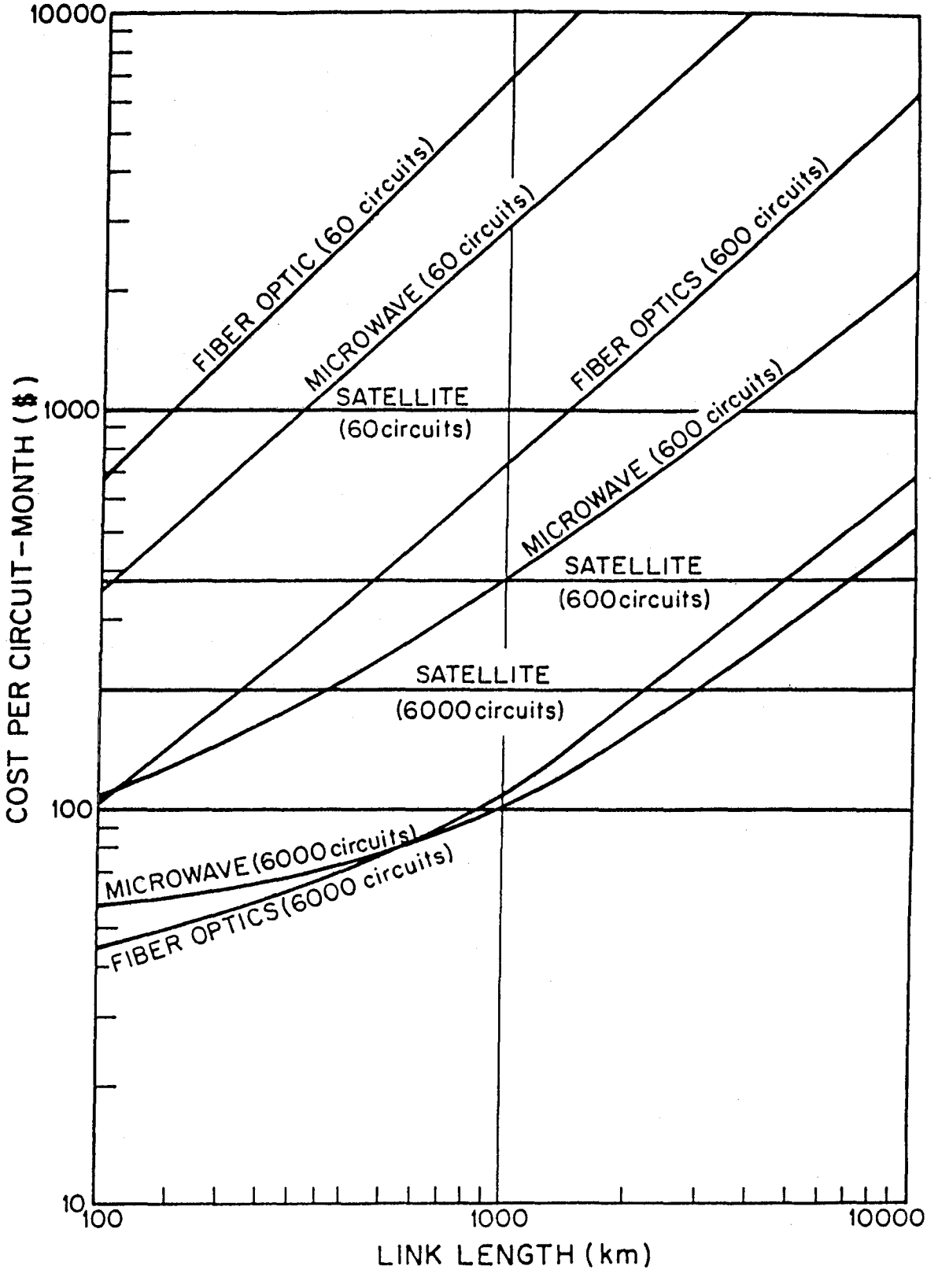



Figure 19. Circuit costs per month as a function of distance and parametric in transmission media (1984 dollars).

capabilities and voice quality of the system. Once deployed the system can be operational within a few hours.

There are other methods for restoring critical system elements using all portable equipment including switching systems, microwave terminals, and VSAT terminals.

## 5.4 Interconnecting Networks

Interconnecting Networks. International standards organizations have been developing recommendations for interconnecting networks for many years. One important recommendation is based on the Open Systems Interconnection (OSI) reference model. See Folts (1982). This OSI reference model contains a layered structure that divides system interconnections into seven functional layers. Each layer provides a set of well defined services to the layer above by adding value to services provided by the layers below. The ultimate objective is to standardize network protocols for all networks and for a network of networks. With such an "open" system, users may ultimately access a variety of services from circuit-switched and packet-switched voice and data networks, and from private, public, local, metropolitan, and wide-area networks. Many of the standard interfaces have been defined and descriptions are published by the CCITT (1989) of the International Telecommunications Union.

Network restoration also may involve interconnections between public and private networks, including interconnections between networks. These interconnections may occur at different levels as depicted, for example, in Figures 20 and 21. These multilevel diagrams of public and private networks are different from the more conventional block diagrams. They are used here because they provide a more graphic insight into a network's physical architecture. For example, with this structured approach it is possible to depict more physical details and to illustrate how the public and private domains interact at different levels, how connectivity is established, and where responsibilities for providing and maintaining service resides. The four structural levels illustrated in Figures 20 and 21 were described in Section 2.2. These levels are unrelated to the OSI model. This multilevel, two domain approach to presenting network architectures is another useful way to view interconnectivity on a physical basis. Interface boundaries, transmission facilities, alternate links, and protocol conversions are

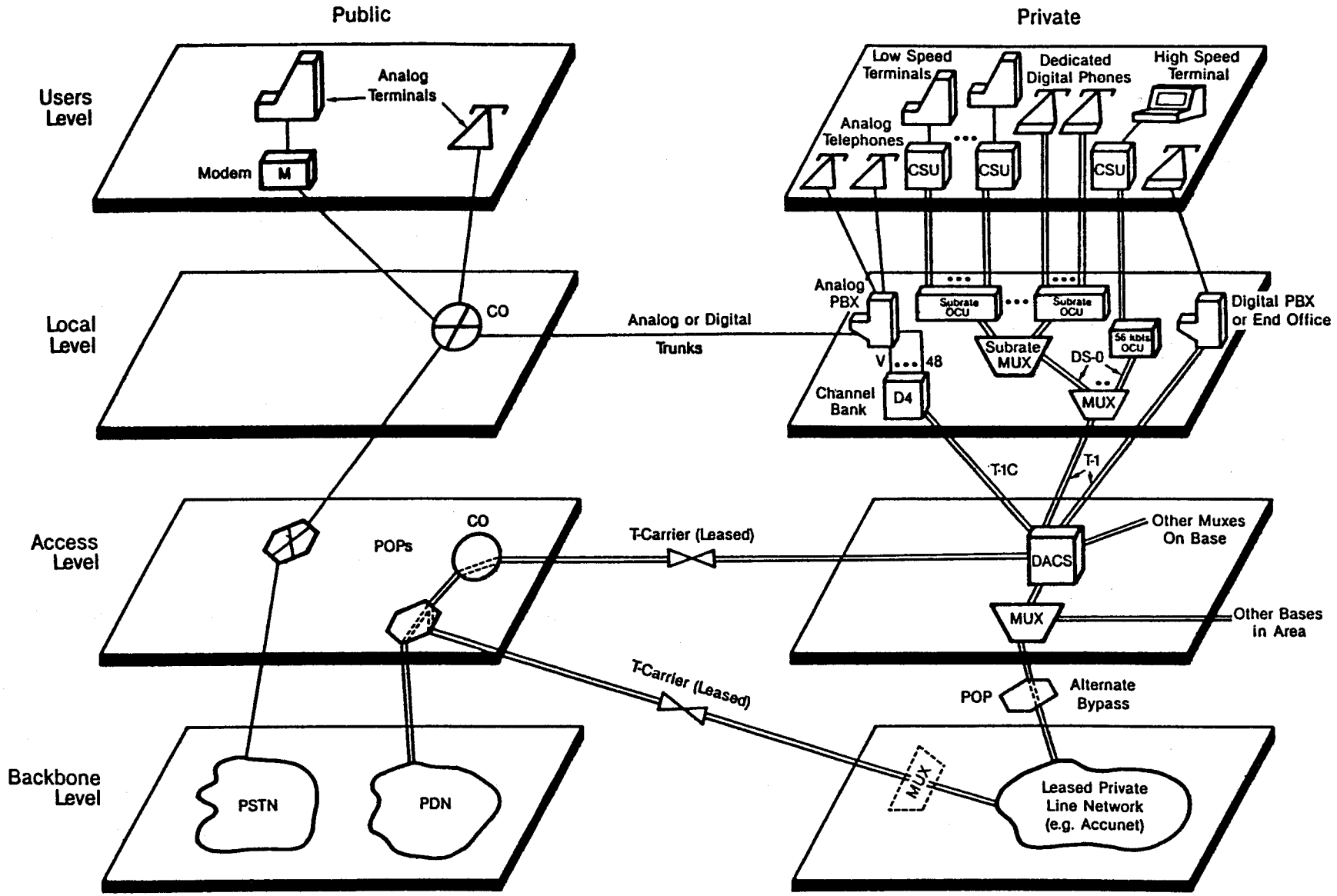



Figure 20. Interconnecting public and private networks with T-carrier.

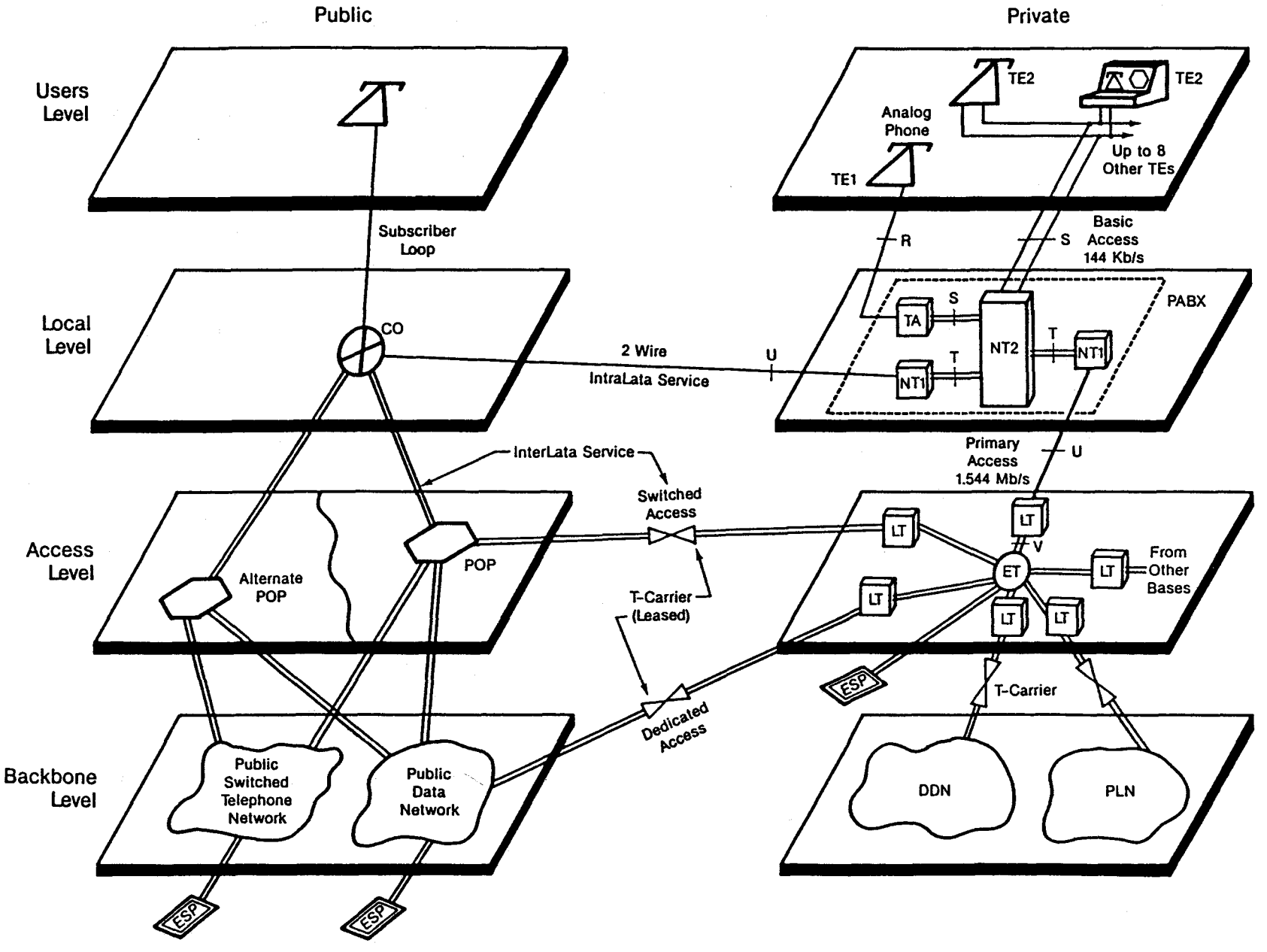



Figure 21. Interconnecting public and private networks using private ISDN.

immediately apparent. Figures 20 and 21 demonstrate the concept and are described below.

Public/Private Interconnections. Figure 20 is just one example of a possible T-carrier facility for interconnecting public and private facilities. Both analog and digital terminals are depicted at the user level. Analog or digital trunks provide voice telephone service through the nearest local exchange carrier (LEC) from the PBX. Digital circuits are multiplexed locally at the T-1 or T-1C level. Then, at the access level, many T-1 or T-1C circuits are cross-connected for local and long-haul distribution.

Access to the T-carrier network may be by private lines that are leased from the LEC or by some form of LEC bypass circuits connecting directly to the point of presence (POP) of the leasing carrier. Both of these access arrangements are shown in Figure 20.

End users can bypass the leased-line connections during stress conditions using a variety of means, including microwave, satellite, fiber optics, and cable, usually using T-carrier equipment. Fiber and cable, however, may not be cost-effective because of the right-of-way costs and restrictions. Local fiber deployment seems very slow. Many of the interface standards and protocols have yet to be determined.

Accessing Private ISDN. Figure 21 illustrates one method for providing ISDN interfaces between the public and private sectors. This particular configuration provides narrowband ISDN features and functions using private facilities owned and operated by a private organization such as a large university campus. This is accomplished using a PABX that provides NT1 and NT2 functions. (See Section 2.1.) Several such PABXs may be employed to provide ISDN interfaces within major building complexes on the campus. These switches are connected to the exchange terminal (ET) via the 2-wire U interfaces and may also be connected to the public switching central office (CO) in the same manner. Other connections may also be provided by using T-carrier directly to commercial carrier POP or to Public Data Network (PDN) access points. The three connections to the public network permit subscribers public access, but can also serve as restoration links or alternate routes during periods of stress.

## 5.5 Other Corrective Measures

There are a number of restoration techniques known today in addition to those already discussed. There are also companies that specialize in coping with disasters by providing alternate services to subscribers. One such company, Comdisco Disaster Recovery Service (CDRS), offers customers network recovery services using VSAT technology. (See Harrison, 1989.) This service plus rerouting, interconnecting networks, VSAT technology, and microwave links have all been used to restore services after disasters. See Harrison (1989), Zorpette (1989), Moberg (1989), and Morley (1987). Voice messaging has also been used to refer callers to unaffected mailboxes (Harrison, 1989). Some other alternatives are the following.

Metropolitan Area Networks (MANs). A MAN is generally considered a public network offering voice and data service and possibly video over fiber or microwave facilities. These networks are suitable for alternate access to carriers and for switching to alternate data backup centers.

Self-Healing Networks. Grover (1987) describes a self healing network that uses wide-bandwidth digital cross-connect systems to reroute traffic automatically in essentially real time when links fail. The concept provides distributed control with no recourse to centralized control or data bases. Automatic restoration of trunks after loss of physical transmission facilities is accomplished by geographical rerouting of the high-capacity circuits using DS-3 (45 Mb/s) machines.

# 6. ISSUES SUMMARY

As this study progressed, it became apparent that there are many important areas yet to be addressed concerning ways and means to ensure continuity of service to essential government entities. This is particularly true for the corrective actions taken after disaster strikes. Some of the more important issues are listed below.

Performance. It is important that certain critical user-oriented performance measures (blocking probability, error rates, throughput delay) be quantified in order to assess network adequacy after restoration. Questions like what is really good enough and what is not for the restoration process must be addressed since the answers will largely determine the kind of restoration needed and the cost. Specific critical service features and functions should be specified along with the grades of service and types of service desired by critical users.

Capacity. The traffic carrying capacity of network architectures must take into account the rerouting procedures. This along with traffic prioritizing determines how survivable the service will be. Simulation may be necessary to quantify the capacity figures.

Detection. The fault detection part of network management is essential to the restoration process. The survivability of the detection system itself must also be considered. How and where fault information is processed (centralized or distributed) is an issue to be resolved.

Standards. Interconnecting networks, whether they be public and private, satellite and terrestrial, LANs or MANs, involves some form of standard interface with appropriate compatible protocols. All the restoration aspects of network management involve standards, including performance monitoring, fault detection, and rerouting. Network interoperability and management standards development is a continuous process. Fault detection and restoration requirements should be incorporated during this standardization process.

Regulation. It may be necessary in some restoration concepts to review the statutes and possibly revise them in order to meet requirements. For example, it may require enabling legislation to permit priority traffic to displace public traffic or to limit use of public facilities during periods of stress. Reservation schemes can be envisioned whereby certain facilities can be withheld for specific prioritized users but with added costs for that privilege.

Signaling. The advantages of common channel signaling networks are well known. However, such systems are often vulnerable to stress. This and other hidden networks may affect the entire system operation. The vulnerability and impact of all of these other hidden networks should be evaluated.

Cost/Benefit Analysis. Planning for disaster requires an assessment of restoration alternatives, their costs, and the tradeoff between these costs and the loss of revenue due to the loss of communication facilities. This so-called cost/benefit analysis is required so the telecommunications manager can develop restoration procedures following a disaster. There are a number of planning issues that must be addressed, including strategic, economic, and technical issues.

## 7. REFERENCES

Boensch, C. J., and R. J. Sogegian (1989), Portable telecommunications for national security emergency preparedness, Signal, July, pp. 51-55.

CCITT (1985), Integrated services digital network, Recommendations of the Series I, Red Book, III, Fascicle III.5, VIIIth Plenary Assembly, Malaga-Torremolinos, 8-19 October 1984.

CCITT (1989), Recommendations of the IXth Plenary Assembly, Blue Books, Melbourne, 14-25 November 1988.

Chakraborty, C. (1988), VSAT communications networks - an overview, IEEE Communications Magazine 26, No. 5, May.

Ergle, W. (1989), A network survival game plan, Telephony, August.

Folts (1982), Information processing systems--open systems interconnection, Draft International Standard 7498.

Grover, W. D. (1987), The self healing network, Globecom, Tokyo, November, p. 28.2.1.

Hara, J. E., C. T. Keyes, R. C. Windiker (1987), Network management of the evolving public switched network, International Switching Symposium, Phoenix, AZ.

Harrison, B. (1989), Planning for disaster, TPT Magazine, September, pp. 23-29.

Helmes, T. (1989), Crash proof fiber rings, Telephony, August, pp. 22-23.

Hurley, B. R., C. J. R. Seidl, and W. F. Sewill (1987), A survey of dynamic routing methods for circuit-switched traffic, IEEE Communications Magazine 25, September, pp. 13-21.

ISO (1982), Information processing systems--open system interconnection reference model, Draft International Standard 7498.

Kao, C., and E. E. Basch (1988), Introduction to Fiber Optics, Optical Fiber Transmission (Howard Sams and Company).

King, L. (1987), The need for fault-tolerant networks, Telecommunications (International), March, pp. 38-40.

Linfield, R. F., M. Nesenbergs, and P. M. McManamon (1980), Command post/signal center bus distribution system concept design, NTIA Report 80-36.

Macurdy, W. B. (1973), Network management in the United States, Proc. 7th International Teletraffic Congress, Stockholm, Sweden, Paper 621, June.

Moberg, K. (1989), A plan called MAP, Telecommunication Reseller 2, No. 8, August/September, pp. 1-4.

Morley, N. (1987), Disaster in Dallas, Telecommunications, May, pp. 114-117.

NCS (1988), Commercial SATCOM interconnectivity: system description, National Communications System, Washington, DC (for official use only).

Nesenbergs, M. (1989), Stand-alone terrestrial and satellite networks for nationwide interoperation of broadband networks, NTIA Report 89-253.

Nesenbergs, M., and P. M. McManamon (1983), An introduction to the technology of intra- and interexchange area telephone networks, NTIA Report 83-118.

NRC (1987), Nationwide Emergency Telecommunications Services for National Security Telecommunications (National Academy Press, Washington, DC).

NRC (1989), Growing Vulnerability of the Public Switched Networks: Implications for National Security Emergency Preparedness (National Academy Press, Washington, DC).

Reedich, J. (1987), The role of network management in evolving T1 voice/data networks, IEEE International Conference on Communications, v. 3, p. 36.4.1.

Telephony (1984), Long haul transmission: a cost comparison, December 3, pp. 130-142.

Western Electric Company (1982), Defense switched network access area concept development, Final Technical Report, submitted to U.S. Army's Communications Systems Agency, Ft. Monmouth, NJ, Contract No. DAA-307-81-C-0725.

Wu, T. H., D. J. Kolar, and R. H. Caudwill (1988), Survivable network architectures for broadband fiber optic networks: model and performance comparison, IEEE J. Lightwave Technology 6, pp. 1698-1709.

Zorpette, G. (1989), Keeping the phone lines open, IEEE Spectrum, June, pp. 32-36.

FORM **NTIA-29**
(4-80)

U.S. DEPARTMENT OF COMMERCE
NAT'L. TELECOMMUNICATIONS AND INFORMATION ADMINISTRATION

# BIBLIOGRAPHIC DATA SHEET

| | 1. PUBLICATION NO. | 2. Gov't Accession No. | 3. Recipient's Accession No. |
|---|---|---|---|
| | | | |

4. TITLE AND SUBTITLE

Congestion-Reduction and Service-Restoration Strategies for Telecommunication Networks

5. Publication Date

6. Performing Organization Code

NTIA/ITS.N

7. AUTHOR(S)

Robert F. Linfield

9. Project/Task/Work Unit No.

8. PERFORMING ORGANIZATION NAME AND ADDRESS

National Telecommunications and Information Admin.
Institute for Telecommunication Sciences
325 Broadway
Boulder, CO 80303-3328

10. Contract/Grant No.

11. Sponsoring Organization Name and Address

National Communications System
Office of the Manager
Washington, DC 20305-2010

12. Type of Report and Period Covered

13.

14. SUPPLEMENTARY NOTES

15. ABSTRACT *(A 200-word or less factual summary of most significant information. If document includes a significant bibliography or literature survey, mention it here.)*

This report covers the first task of a three-task effort designed to explore the potential of using advanced satellite system technologies to enhance the rapid restoration of telecommunication services that may be disrupted due to traffic congestion or natural or man-made disasters. The purpose of this first task is to survey the various strategies currently used to alleviate stress. The telecommunication networks included are long-distance common carriers, local exchange carriers, and private networks. Both preventive and corrective measures are covered. Preventive measures include prioritizing traffic using fault-tolerant systems, and implementing alternate routing procedures. Corrective measures include network reconfiguration, engaging bypass systems, using transportable equipment and interconnecting systems.

16. Key Words *(Alphabetical order, separated by semicolons)*

alternate routing; disaster recovery; fault detection; network reconfiguration; restoration; telecommunications

| 17. AVAILABILITY STATEMENT | 18. Security Class. *(This report)* | 20. Number of pages |
|---|---|---|
| ☒ UNLIMITED. | Unclassified | 62 |
| ☐ FOR OFFICIAL DISTRIBUTION. | 19. Security Class. *(This page)* | 21. Price: |
| | Unclassified | |

☆ U.S. GOVERNMENT PRINTING OFFICE: 1990—773-002/11031