Wells

KSC-DL-3572
Revision A

KENNEDY SPACE CENTER

NETWORK HANDBOOK

March 31, 1995

ENGINEERING DEVELOPMENT DIRECTORATE

National Aeronautics and
Space Administration

John F. Kennedy Space Center

KSC FORM 16-12 (REV. 7/92)

RECORD OF REVISION/CHANGES

REV LTR	CHANGE NO.	DESCRIPTION	DATE
		Basic Issue	June 10, 1993
A		General Revisions	March 31, 1995

PREFACE

This revision of the KSC Network Handbook was prepared and issued to fulfill the Engineering Development Directorate responsibility — to develop and maintain a KSC Network Handbook — as defined in Attachment A of KMI 2520.4, "KSC Institutional Network Communications Development, Operations and Management."

This document applies to all government and contractor organizational elements that are responsible for, or require access to, KSC Institutional Networks (KIN's) for computer data communications. It is not applicable to KSC Operational Networks [e.g., Launch Processing System (LPS)] which are mission critical systems.

This document provides the single information manual about all KIN's and the KSC Network Environment (KNE). It provides comprehensive information about the procedures for obtaining network services, the network architecture and physical layout, organizational responsibilities and policies, and network standards and installation specifications. It is KSC policy to develop a more unified approach for a centerwide network communications architecture that provides integrated, interoperable, and cost-effective service for all KSC users. It is hoped that the information in this document will facilitate cooperative interaction among the many network groups to accomplish this end.

This document was organized so that information of interest to the biggest audience (and the least technical) is in the first section. Subsequent sections will be of interest to a smaller audience desiring more in-depth information. When information is covered in other documentation, the reader will be given a brief description of that information and directed to the other document.

- Section I - Helps the reader to get connected and provides basic useful information
- Section II - Orients the reader to the centerwide network picture
- Section III - Tells the reader about the services and resources available on the network
- Section IV - Tells about networking organizations, their responsibilities and interfaces
- Section V - Institutional network security policies and practices
- Section VI - Technical information about network transmission media and standards
- Section VII - An overview of network protocols
- Section VIII - Applicable government and industry standards and specifications

The appendices provide the reader with an acronym list, definitions, physical network illustrations, and samples of service request forms.

As the need for revision of this document is recognized and justified by changes in services, configuration, procedures, or policies, KSC organizations are requested to forward changes to:

Raymond Pecaut
DL-CMD-N
Kennedy Space Center, FL 32899

Copies of this document may be obtained by requesting it, by number and title, from:

Engineering Documentation Center
Headquarters, RM 3436 (Mail Code: EDC)
Kennedy Space Center, FL 32899
407-867-3265

TABLE OF CONTENTS

TABLE OF CONTENTS (cont)

TABLE OF CONTENTS (cont)

TABLE OF CONTENTS (cont)

TABLE OF CONTENTS (cont)

LIST OF ILLUSTRATIONS

LIST OF ILLUSTRATIONS (cont)

REFERENCES

The KSC and NASA management issuances and technical documentation shown below are listed by basic number without regard to revisions. The latest revision or change to each cited document will be applicable.

NMI 2410.7 "Assuring the Security and Integrity of NASA Automated Information Resources"

NMI 2520.1 "Communications System Acquisition and Management"

NHB 2410.9 "NASA Automated Information Security Handbook"

KMI 2410.2 "Information Resources Management"

KMI 2410.4 "Assuring Security and Integrity of KSC Data Processing"

KMI 2520.4 "KSC Institutional Network Communications Development, Operations, and Management"

79K33182 "Premises Distribution System Specifications"

79K33909 "FDDI/Switched Ethernet Concentrators and Management Package, Specification for"

KSC-TS-DL-002 R1 "Payload Operations Network Plan"

Payload Operations Network User's Guide (CS-GSD-21, Network and Communications Section)

SECTION I

USER INFORMATION

1.1 INTRODUCTION

This section provides answers to the questions most asked by KSC network users and provides some common sense do's-and-don'ts that every network user should know and follow.

Also provided is a comprehensive list of KSC institutional networks and services by physical location (building where the user works). There are numerous help desks and response centers available, due to the three major contracts at KSC. Users may obtain new service, repair existing service, or obtain information concerning other networks by calling the appropriate phone number.

1.2 NETWORK CONNECTIONS - ADMINISTRATIVE AUTHORITIES

Three administrative authorities control network connections available at KSC and NASA facilities at Cape Canaveral Air Station (CCAS).

a. **LAUNCH COMPLEX 39.** The authority for the Launch Complex 39 area is the Shuttle Operations Data Network (SODN). To obtain connections, send an SODN Support Request - New Service, (KSC Form 29-784), attached to either a Support Request (SR), (KSC Form 19-15), or an Engineering Support Request (ESR), (KSC Form 21-319) or the Domain Name Service (DNS) (KSC Form 29-786), to the LSOC Comm Work Control, Mail Code LSO-095, 867-2151.

b. **PAYLOADS-RELATED INDUSTRIAL AREA AND CCAS.** The Payload Operations Network (PON) is the administrative authority for the Operations and Checkout (O&C) Building, the Payload Support Building (M7-505), LETF (M7-505A), MMSE, SAEF-2, VPF, SSPF, PHSF, PSTF-R, EML, M7-698, EDL, M7-502, M7-503 and NASA-leased facilities at CCAS (E&O, AE, AO, AM, L, Dispensary, Apollo warehouse, S and AF). To obtain connections, send a Customer Support Request [CSR (KSC Form 31-134)], to Mail Code F428. Any questions about the form or to obtain one, call the Help Desk at 867-1709.

c. **KSC INDUSTRIAL AREA.** The Kennedy Data Network (KDN) is the administrative authority for the rest of the KSC Industrial Area. For KDN connections, send an Avoid Verbal Orders (AVO), (KSC Form 1-14)

or equivalent, requesting a connection to KDN, Mail Code BOC-074. Call 867-3127 for further information.

Sample forms for requesting network connections are located in Appendix E.

1.3 NETWORK ASSISTANCE

Users experiencing trouble with computers can obtain help from various sources. Each of the three administrative authorities provide call-in help centers to answer software problems. Because it is often unclear to users whether they are experiencing a software or hardware problem, the help desk personnel will make this determination. When a problem is encountered that the center does not handle, it will direct the user to the proper organization.

Main administrative authority assistance (trouble calls) lines:

- For SODN help: call the IPS Operations Help Desk at 861-HELP.
- For PON help: call the Help Desk at 867-1709.
- For KDN help: call the Care Center at 867-2332.
- For KSDN help: SPC Customers call the Help Desk at 861-HELP.
  Non-SPC Customers call the Care Center at 867-2332.

If training is needed, each help center can provide further information. Training can also be obtained through your training officer or the Computer Training Center at 867-3245.

Along with the major networks, KSC has a variety of other computer networks and services available. Table 1 provides a breakdown of these networks by facility. For a detailed description of each network and service, refer to Section II, Kennedy Space Center Network Environment, and Section III, Resources Available to Network Users.

NOTE: The help desks are open only during normal operating hours (first shift). Problems encountered after hours need to be addressed the following business day. Users can also reference Appendix D, Network User Help Guide, for more contacts.

NOTE: The authors recognize that new networks and services are being created at KSC and that this table may not include them. Please send updates to this list to the Engineering Development Directorate (DE), Networks Section, DL-CMD-N, Attn: Ray Pecaut.

Table 1. Network Contacts by KSC Facilities

Facility	Network/Service	Help Desk Contact	Phone
All Facilities	AppleTalk Network Support	I-NET ESC	867-4847
	Wide Area Network Interface	Wide Area Networks	867-7278
	Shuttle Operations Data Network (SODN)	IPS Operations Help Desk	861-HELP
	Kennedy Switched Data Network (KSDN) - SPC Customers	IPS Operations Help Desk	861-HELP
	KSDN - Non-SPC Customers	BOC Care Center	867-2332
	Program Support Communications Network	I-NET/Prisms	867-7726
Headquarters	CAD/CAE Network	KSC CAD Support	867-3234
	Kennedy Data Network (KDN)	BOC Care Center	867-2332
	Payload Operations Network (PON)	PON Help Desk	867-1709
	DE-Integrated Engineering Support Group (IECS)	IECS Support Group	867-2334
O&C	CAD/CAE Network	KSC CAD Support	867-3234
	Payload Operations Network	PON Help Desk	867-1709
	Payload Data Management System	PON Help Desk	867-1709
	Payload Processing Network	PON Help Desk	867-1709
	DE-Integrated Engineering Computer System (IECS)	IECS Support Group	867-2334

Table 1. Network Contacts by KSC Facilities (cont)

Facility	Network/Service	Help Desk Contact	Phone
EDL	CAD/CAE Network	KSC CAD Support	867-3234
	Kennedy Data Network (KDN)	BOC Care Center	867-2332
	Payload Operations Network	PON Help Desk	867-1709
	DE-Integrated Engineering Computer System (IECS)	IECS Support Group	867-2334
CIF	CAD/CAE Network	KSC CAD Support	867-3234
	Kennedy Data Network	BOC Care Center	867-2332
	Shuttle Operations Data Network (SODN)	IPS Operations Help Desk	861-HELP
SSPF	PON	PON Help Desk	867-1709
LETF	DE-Integrated Engineering Computer System (IECS)	IECS Support Desk	867-2334
CDSC	Shuttle Operations Data Network (SODN)	IPS Operations Help Desk	861-HELP
	Kennedy Data Network (KDN)	BOC Care Center	867-2332
BOB, BOC SUPPLY	Kennedy Data Network (KDN)	BOC Care Center	867-2332
Security	Kennedy Data Network (KDN)	BOC Care Center	867-2332
Occup. Health	Kennedy Data Network (KDN)	BOC Care Center	867-2332
Base Support Bldg. & Trailers	Kennedy Data Network (KDN)	BOC Care Center	867-2332

Table 1. Network Contacts by KSC Facilities (cont)

Facility	Network/Service	Help Desk Contact	Phone
VAB	Shuttle Operations Data Network (SODN)	IPS Operations Help Desk	861-HELP
	Shuttle Processing Data Management System (SPDMS)	IPS Operations Help Desk	861-HELP
LCC	Shuttle Operations Data Network (SODN)	IPS Operations Help Desk	861-HELP
	Kennedy Data Network (KDN)	BOC Care Center	867-2332
	Central Data Subsystem Operational Network	Help Desk, CDS Control Room	861-0707
	LPS Operational Network (LON)	Help Desk	861-0707
	SPDMS	IPS Operations Help Desk	861-HELP
OPF	Shuttle Operations Data Network (SODN)	IPS Operations Help Desk	861-HELP
	SPDMS	IPS Operations Help Desk	861-HELP
OSB	Shuttle Operations Data Network (SODN)	IPS Operations Help Desk	861-HELP
	SPDMS	IPS Operations Help Desk	861-HELP

Table 1. Network Contacts by KSC Facilities (cont)

Facility	Network/Service	Help Desk Contact	Phone
PCC	Shuttle Operations Data Network (SODN)	IPS Operations Help Desk	861-HELP
	SPDMS	IPS Operations Help Desk	861-HELP
	LPS Software Development Network (LSDN)	Help Desk	861-7368
	LPS Operational Network (LON)	Operations Help Desk	861-0707
PSTF-R	PON	PON Help Desk	867-1700
LC-39 Modular Complexes A-J	Shuttle Operations Data Network (SODN)	IPS Operations Help Desk	861-HELP
	SPDMS	IPS Operations Help Desk	861-HELP
	Kennedy Data Network (KDN)	BOC Care Center	867-2332
	LSDN	Help Desk	867-7368
LC-39 Pad A and Pad B	SPDMS	IPS Operations Help Desk	861-HELP
	Shuttle Operations Data Network (SODN)	IPS Operations Help Desk	861-HELP

See Appendix D, Network User Help Guide, for further network contacts.

1.4 PERSONAL COMPUTER UPGRADES

Acquisition of computer hardware and software is the responsibility of the user's local organization, not the network. A purchase request signed by supervision is

normally needed to acquire new supplies. However, help is available for determining what software or hardware upgrades to purchase.

Call the network's help line for directions to someone who can recommend a standard configuration that should meet one's needs. Or, call the Technical Learning Center (TLC). This group is constantly evaluating new products and can recommend products to meet most needs. The TLC can also demonstrate many products or loan a software product for a short period of time for the user's evaluation.

1.5 NETWORK USER TIPS

1.5.1 Security

The user is responsible for protecting the automated information resources contained in the computer, according to NMI 2410.7, "Assuring the Security and Integrity of NASA Automated Information Resources," and KMI 2410.4, "Assuring Security and Integrity of KSC Data Processing." This includes the user's network access. A password to log onto the computer and/or network should be used. When choosing a password, don't use one easily guessed, like "secret" or a family name.

For more detailed information on network security, see Section V.

1.5.2 Incident Reporting

If it appears that some unauthorized person has logged onto a user's computer, the user should immediately stop working on the computer and report the incident to the Help Desk or the computer security official for the appropriate system. To obtain a list of computer security officials and phones numbers, contact the KSC Automated Information Security Manager, HM-INF, 867-7293.

Help desks should be able to provide security assistance. After hours security help can be obtained from the NASA Automated Systems/Incident Response Capability (NASIRC), 800-7-NASIRC (Hotline/Helpdesk [M-F/7:30 - 5:30 EST]).

800-SKY-PAGE/PIN#: 6460866 (24 HR Nationwide Skypager)
301-306-1010 (24 HR FAX)

nasirc@nasa.gov (24 HR Internet e-mail server address)

1.5.3 Safe Computing

Safe computing requires taking precautions and avoiding high risk activities to prevent viruses. The easiest way to contract a computer virus is from "freeware" obtained from a computer bulletin board or a friend's diskette. Contaminated software can infect not only the user's computer, but the entire network. The TLC, located in HQS, Room 2145, provides a disinfectant service to scan for and remove these viruses. Consult NHB 2410.9, NASA Automated Information Security Handbook, for more details.

1.5.4 Do-It-Yourself Networking

This is absolutely forbidden without coordination with the Network Managers (see 4.3.1). Networks have to be configured properly and administered by trained operations and maintenance personnel. If equipment is not configured properly, it can cause problems for other users on the network. (The offending party is usually not affected; instead, some innocent users three rooms away develop communication problems.) Also, the equipment you attach may not only bring down communications on your network, but adversely effect communications on the network backbone [e.g., the Broadband Communications Distribution System (BCDS)] as well. Wait, and let the proper personnel make the changes.

SECTION II

KENNEDY SPACE CENTER NETWORK ENVIRONMENT (KNE)

2.1 KNE ELEMENTS

The Kennedy Space Center Network Environment (KNE) consists of five major elements. The first three elements are the Kennedy Institutional Networks (KIN's) (See figure 2-1, Kennedy Space Center Network Environment):

- The Kennedy Data Network (KDN), operated by the Base Operations Contractor (BOC).
- The Payload Operations Network (PON), operated by the Payload Ground Operations Contractor (PGOC).
- The Shuttle Operations Data Network (SODN), operated by the Shuttle Processing Contractor (SPC).

The fourth KNE element is the KSC Metropolitan Area Network (KMAN), the central link between the KIN's. KMAN also links with the KSC Wide Area Network (KWAN) Interface, the fifth element of the KNE. The KWAN Interface provides access to other NASA Centers and facilities through the Program Support Communications Network Interface (PSCNI) and the NASA Science Internet (NSI).

The following sections present the network user with a description of the KIN's, the KMAN, the Kennedy Switched Data Network (KSDN), the AppleTalk Network, Local Area Networks (LAN's), and the KWAN Interface.

2.2 KENNEDY DATA NETWORK (KDN)

Note: The KDN is an institutional network and is not intended for use in support of any critical mission operations.

The Kennedy Data Network consists of multiple LAN segments transported to a major hubbing system via assigned Broadband Cable Distribution System (BCDS) channels, fiber optic links, KSDN Bridged Network links, and T-carrier links. The major hubbing system, known as the Admin Hub (ADMHUB), consists of a multi-protocol, multi-interface routing system. The ADMHUB routes traffic between the backbone links that join LAN's within KDN. KDN utilizes the KWAN interface to

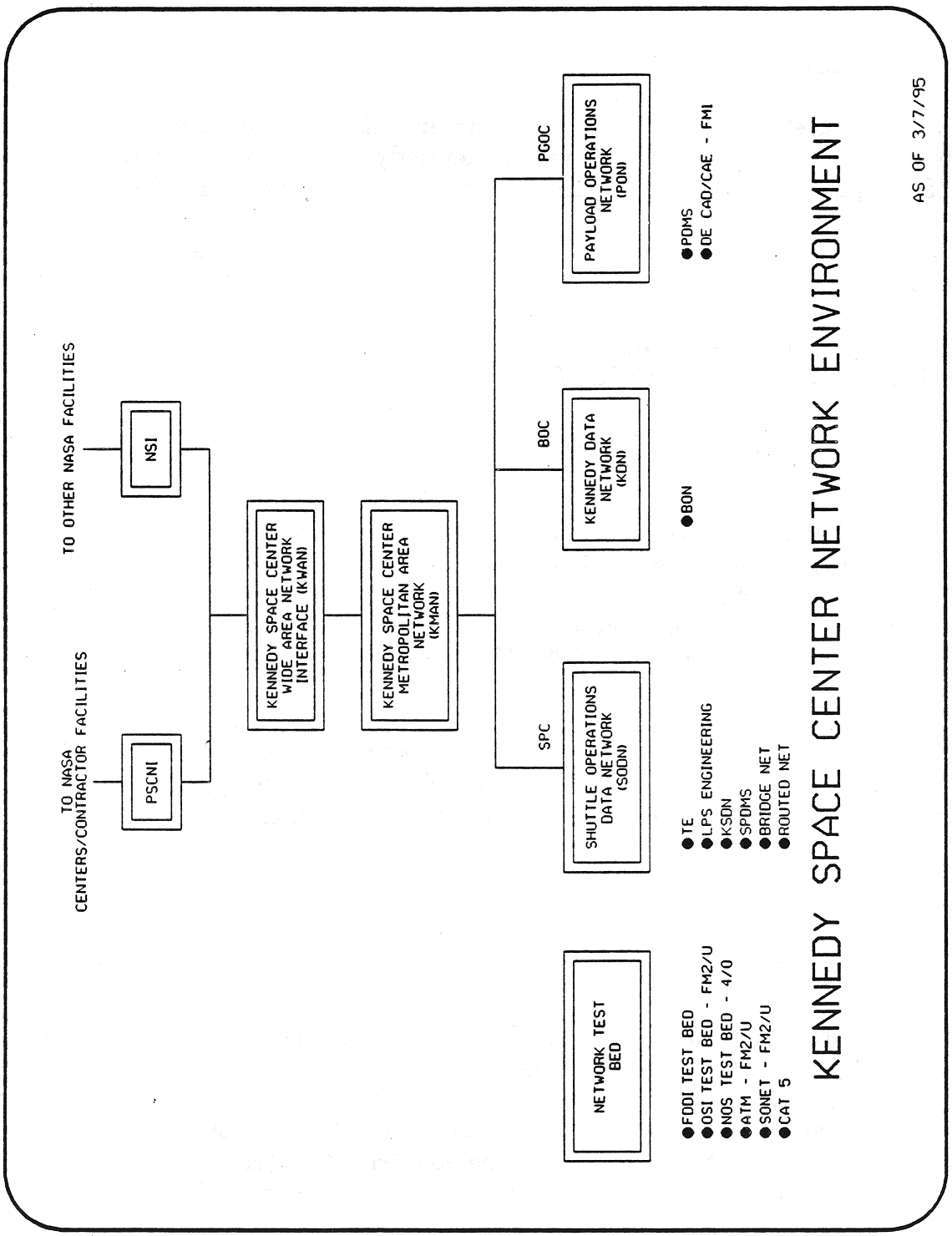


Figure 2-1. KSC Network Environment

SECTION II

KENNEDY SPACE CENTER NETWORK ENVIRONMENT (KNE)

2.1 KNE ELEMENTS

The Kennedy Space Center Network Environment (KNE) consists of five major elements. The first three elements are the Kennedy Institutional Networks (KIN's) (See figure 2-1, Kennedy Space Center Network Environment):

- The Kennedy Data Network (KDN), operated by the Base Operations Contractor (BOC).
- The Payload Operations Network (PON), operated by the Payload Ground Operations Contractor (PGOC).
- The Shuttle Operations Data Network (SODN), operated by the Shuttle Processing Contractor (SPC).

The fourth KNE element is the KSC Metropolitan Area Network (KMAN), the central link between the KIN's. KMAN also links with the KSC Wide Area Network (KWAN) Interface, the fifth element of the KNE. The KWAN Interface provides access to other NASA Centers and facilities through the Program Support Communications Network Interface (PSCNI) and the NASA Science Internet (NSI).

The following sections present the network user with a description of the KIN's, the KMAN, the Kennedy Switched Data Network (KSDN), the AppleTalk Network, Local Area Networks (LAN's), and the KWAN Interface.

2.2 KENNEDY DATA NETWORK (KDN)

Note: The KDN is an institutional network and is not intended for use in support of any critical mission operations.

The Kennedy Data Network consists of multiple LAN segments transported to a major hubbing system via assigned Broadband Cable Distribution System (BCDS) channels, fiber optic links, KSDN Bridged Network links, and T-carrier links. The major hubbing system, known as the Admin Hub (ADMHUB), consists of a multi-protocol, multi-interface routing system. The ADMHUB routes traffic between the backbone links that join LAN's within KDN. KDN utilizes the KWAN interface to

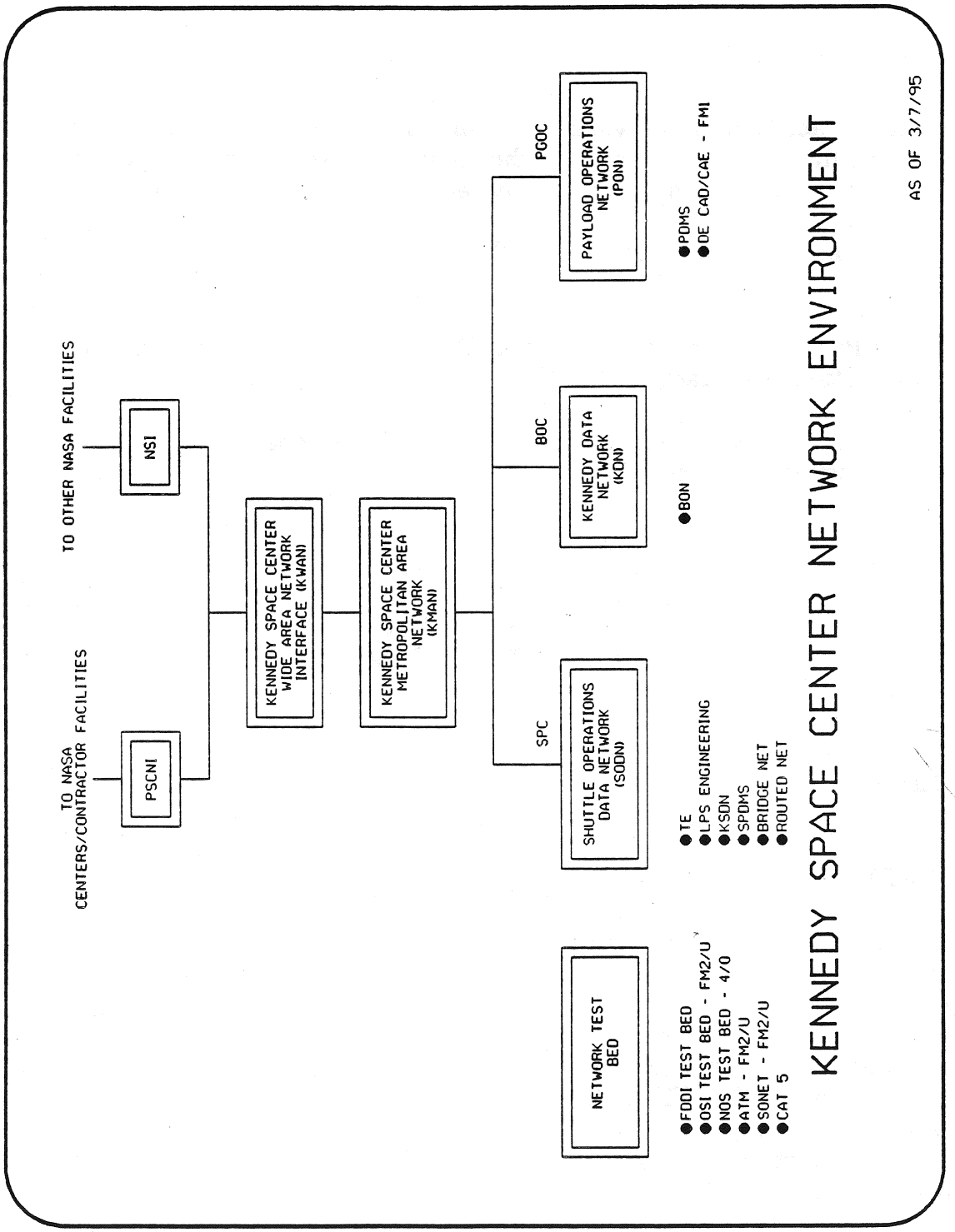


Figure 2-1. KSC Network Environment

link with NSI and PSCNI through the BCDS channels known as the KSC Metropolitan Area Network (KMAN) Interface and the KSC Wide Area Network (KWAN) Interface.

This Network topology supports numerous nodes (See figure 2-2, Kennedy Data Network Environment). Major ones include:

- The Base Operations Network (BON), used by the Base Operations Contractor and NASA. This network utilizes SPX/IPX to communicate between user workstations and file servers, and TCP/IP for terminal services and file transfer services between the workstations and host systems. Connectivity is also provided to the Amdahl mainframe for Automated Information Management (AIM) applications, and the Honeywell mainframes supporting the Kennedy Inventory Management System (KIMS).

- The CAD/CAE network, used for computer drawings at KSC. This network utilizes TCP/IP to communicate between the CAD/CAE workstation and the host.

- The Document Imaging network, used to process documents like Material Safety Data Sheets (MSDS) at KSC. This network utilizes SPX/IPX to communicate between workstations, file and object servers.

The KDN also provides sustaining engineering, operation and maintenance for Kennedy Electronic Mail system (KMail) and the Domain Name System (DNS).

The Network Control Center (NCC) for the KDN is located in the CIF, Rm. 151. The NCC is responsible for Operation and Maintenance (O&M) of the KDN associated clients/servers, routers, bridges, gateways and hubs. In addition, network performance, utilization, and responsiveness is monitored to provide real time response to network abnormalities. The NCC phone number is 867-2182.

Sample forms for requesting network connections are located in Appendix E.

2.3 PAYLOAD OPERATIONS NETWORK (PON)

Note: The PON is an institutional network and is not intended for use in support of any critical mission operations.

The Payload Operations Network provides administrative support for the processing of Space Shuttle and Expendable Vehicle payloads at the Kennedy Space Center and NASA facilities at CCAS.

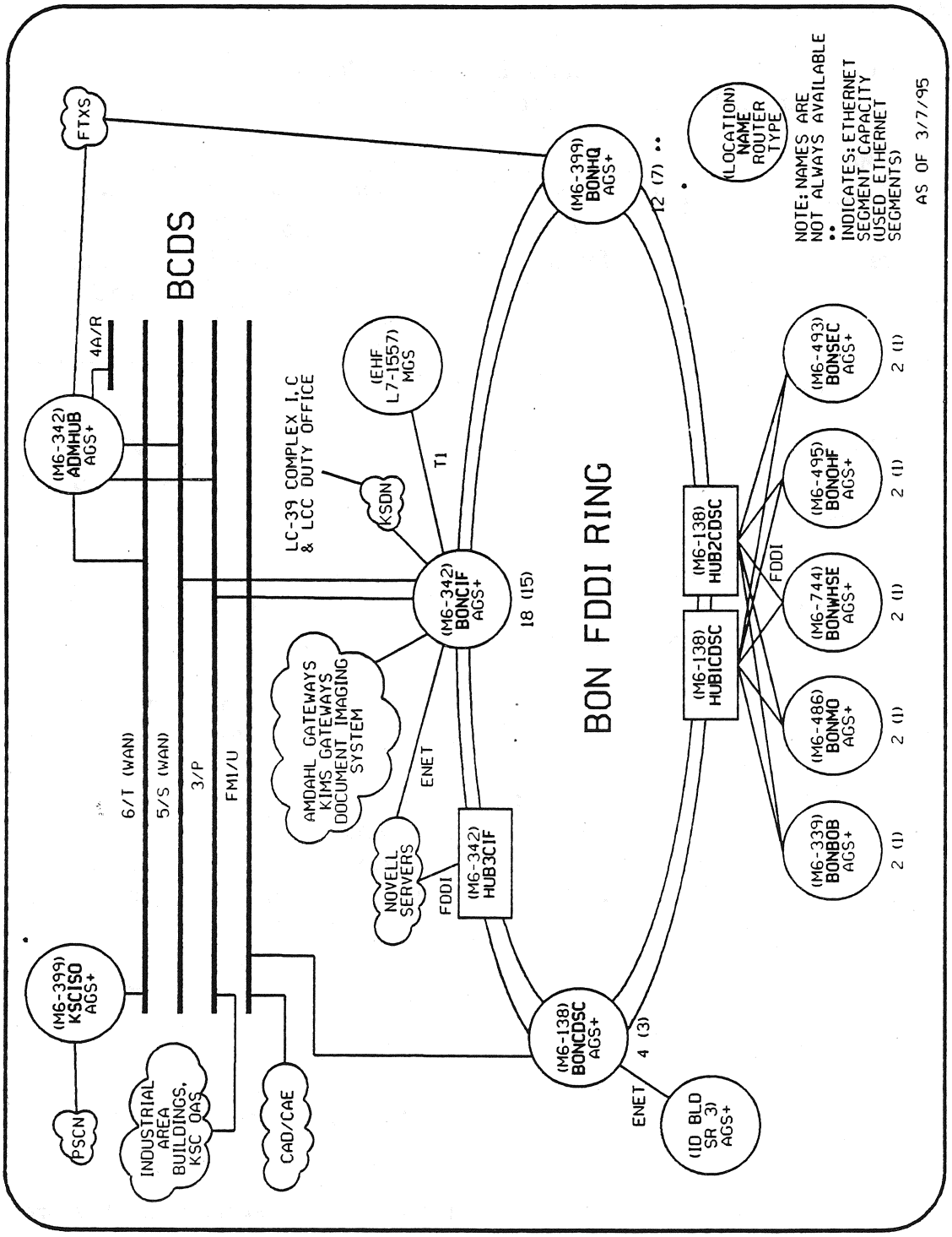


Figure 2-2. Kennedy Data Network (KDN) Environment

2.3.1 PON Infrastructure

The PON provides network connectivity to about 30 facilities located in the KSC Industrial Area, NASA facilities at CCAS, and local off-site contractor facilities. (See figure 2-3, Payload Operations Network.) The PON interconnects over 50 local ethernet segments, which support about 2,000 NASA and PGOC users. The PON uses broadband and fiber-optic technologies to interconnect the local ethernet segments into a unified computer communications network. The PON has wide area network connectivity to the NASA Science Internet (NSI) and the Program Support Communications Network Internet (PSCNI).

PON's physical and data link layer protocols are in conformance with IEEE 802.3 specification, adopted as an accepted Open Systems Interconnection (OSI) standard. The PON is in compliance with the data link layers of the OSI model.

The network and transport layer protocols used on the PON include:

- TCP/IP
- Intergraph XNS
- DECnet Phase IV
- Appletalk Phase 2
- Microsoft NetBEUI

The X.25 protocol suite is used to provide access to the PSCN NASA Packet Switched System (NPSS). The network servers on the PON use the IP and NetBEUI protocol suites.

The PON currently supports many protocols at the network and transport layer which are not in compliance with OSI. The OSI migration strategy is to migrate to an approved short term protocol as called for by the Intercenter Council for Computer Networking (ICCN). Initially, IP will be implemented in place of these proprietary protocols. The network servers can simultaneously support multiple network protocols (NetBEUI, IP and OSI) stacks. This capability will allow the PON to implement OSI protocols in an orderly fashion. User functionality will not be impacted by the transition from IP to OSI.

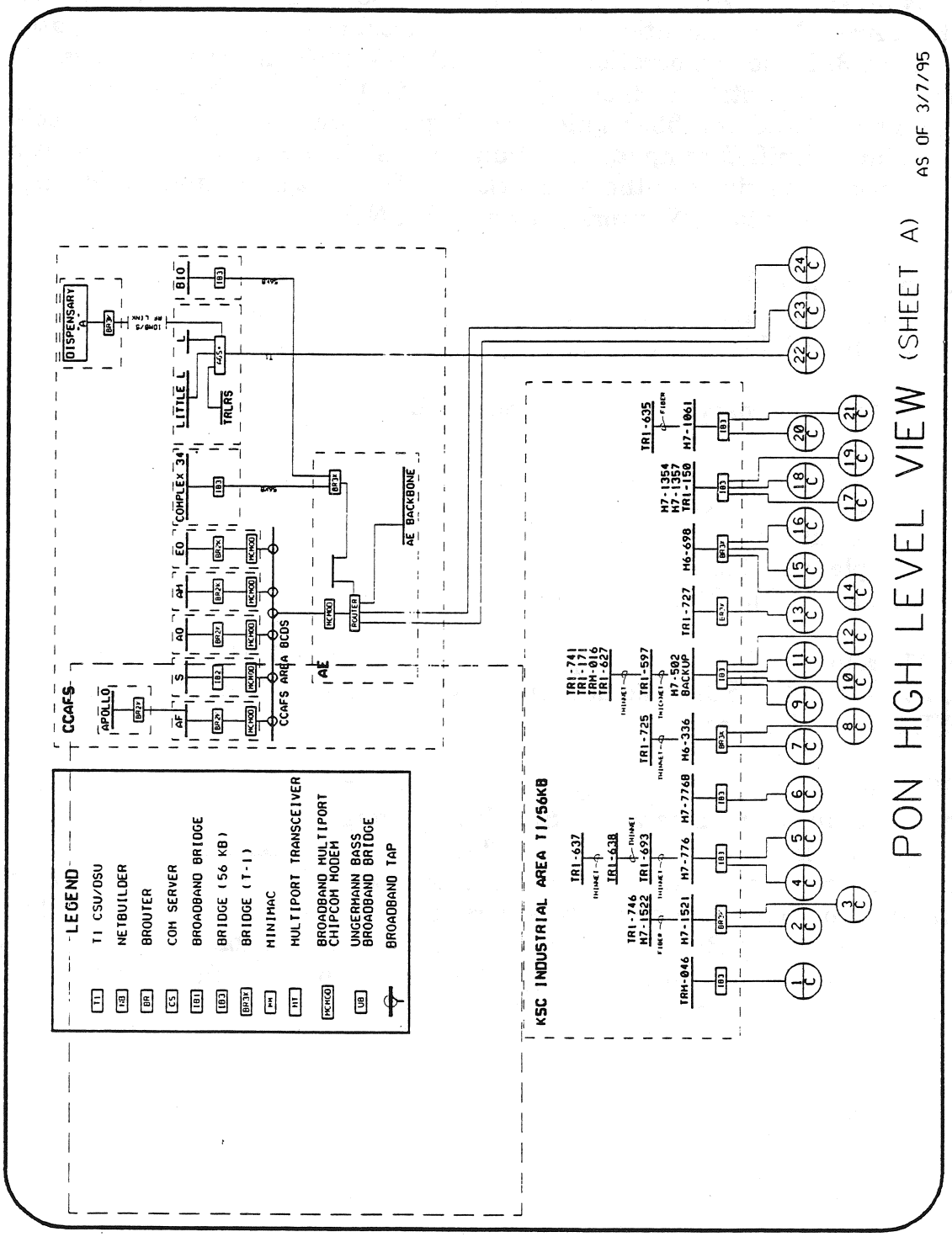


Figure 2-3. Payload Operations Network (Sheet 1 of 4)

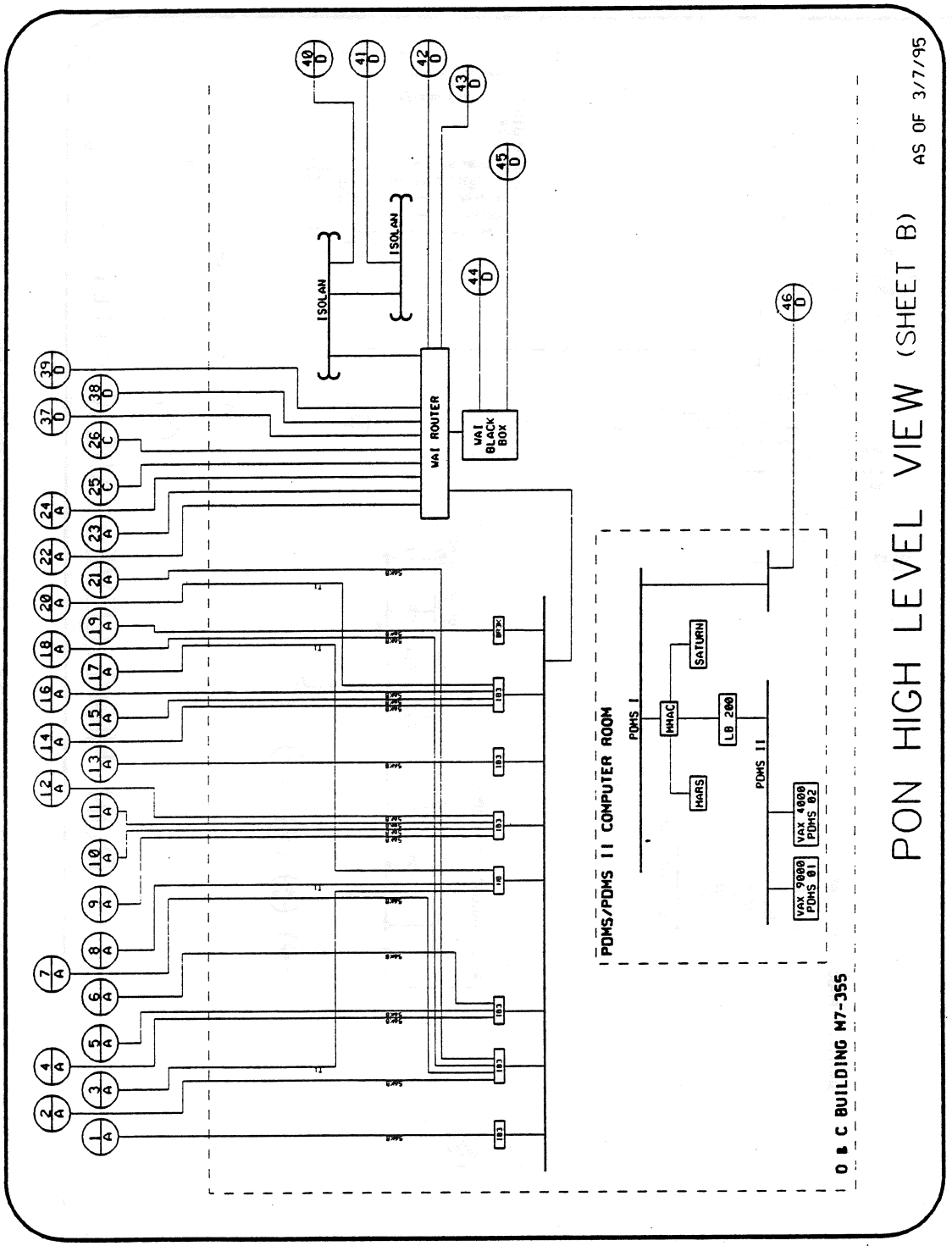


Figure 2-3. Payload Operations Network (Sheet 2 of 4)

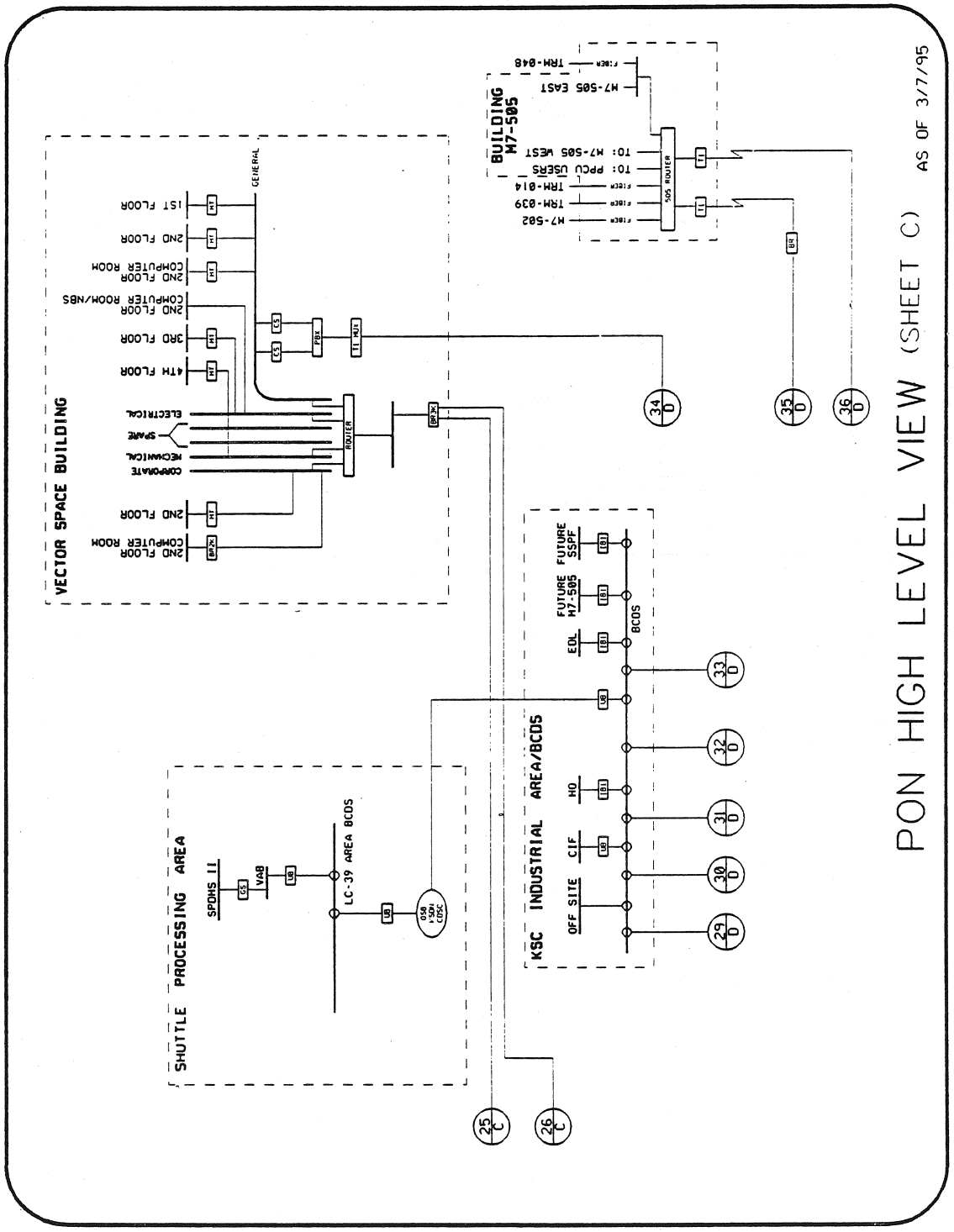


Figure 2-3. Payload Operations Network (Sheet 3 of 4)

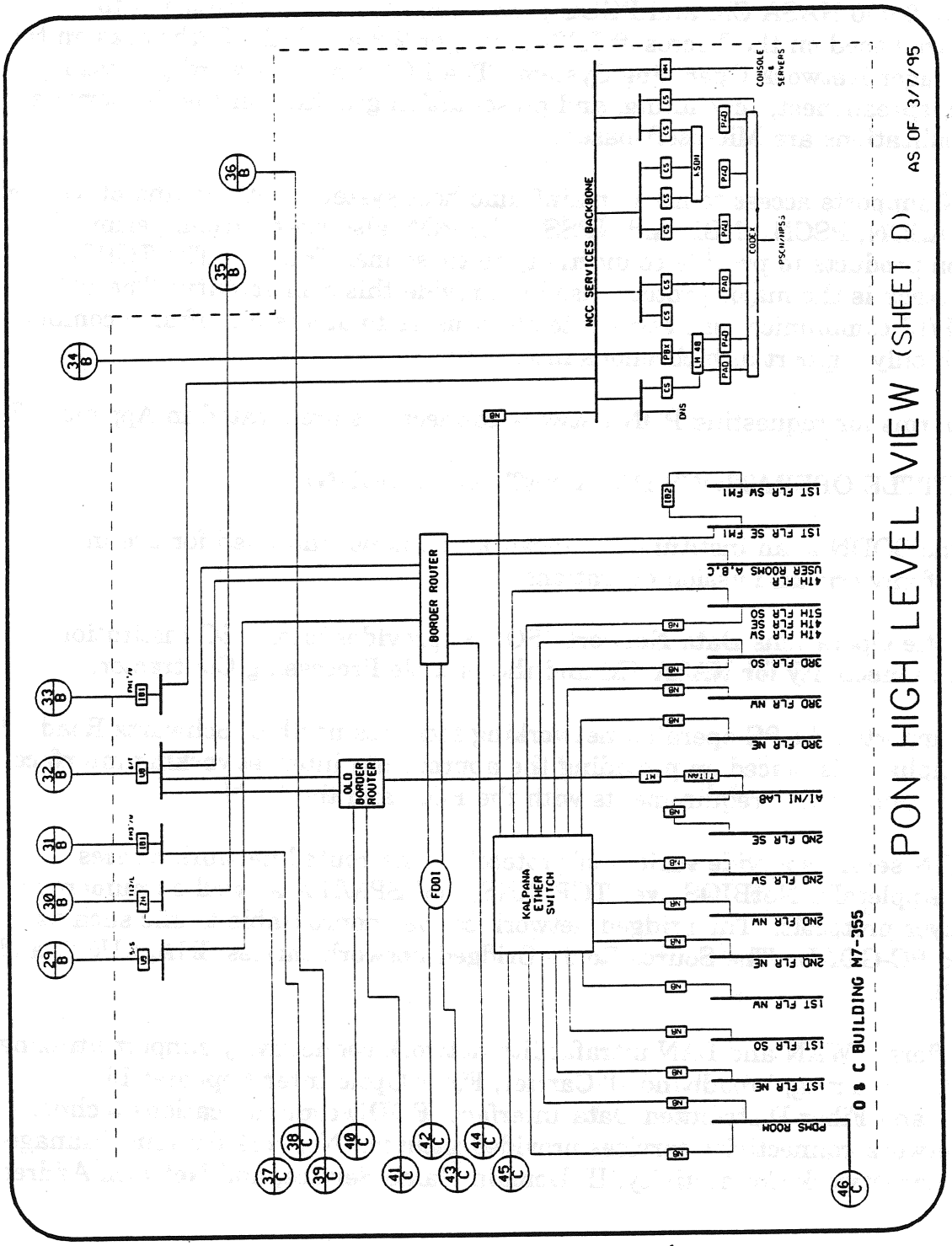


Figure 2-3. Payload Operations Network (Sheet 4 of 4)

2.3.2 PON Applications

The PON provides print, file, application, terminal emulation, and electronic mail services to 2,000 NASA CM and PGOC personnel. The PON's print and file services are based on the Microsoft LAN Manager 2.2 and DEC Pathworks on the LAN Manager Network Operating System. The PON provides word processing, database, spreadsheet, scheduling, and presentation graphics on the file servers. These applications are Microsoft-based.

The PON supports access to many mainframe host systems both on and off center through KSDN, PSCNI, NSI, and NPSS. The PON also uses various terminal emulation products to provide connectivity to these mainframes. The TCP/IP protocol stack is the major protocol used to provide this connectivity. The PON uses TCP/IP communications servers to allow users to access mainframe computers which only support asynchronous interfaces.

Sample forms for requesting PON network connections are located in Appendix E.

2.4 SHUTTLE OPERATIONS DATA NETWORK (SODN)

Note: The SODN is an institutional network and is not intended for use in support of any critical mission operations.

The Shuttle Operations Data Network (SODN) provides local KSC institutional network connectivity for NASA TM and the Shuttle Processing Contractor.

SODN supports all SPC-operated networking facilities north of Schwartz Road. A major emphasis is placed on providing the appropriate internetworking interfaces to satisfy connectivity requirements with the PON and the KDN.

The SODN services a wide variety of protocols. The routed network carries TCP/IP, Appletalk, NetBIOS over TCP, XNS, and SPX/IPX as well as numerous upper layer protocols. The bridged network carries nonroutable traffic such as LAT and PC-GOAL. The Source-Route Bridged network carries SNA, LU6.2, and NetBIOS.

SODN offers a WAN and LAN intrafacility network connectivity support utilizing ethernet, token-ring, broadband, T-Carrier, Fiber Optic Inter Repeater Link (FOIRL), and Fiber Distributed Data Interface (FDDI) communications technologies. Network connectivity services provided include: Network Systems Management, Internetwork Connectivity, IP Domain Name Service, and Network Address

Management. Network Systems Management is conducted from the SODN Network Control Center in the Communications Distribution and Switching Center (CDSC) facility with state-of-the-art monitoring and troubleshooting equipment. SODN's primary backbone transport medium is the FDDI Transmission System (FTXS) connecting primary SODN LC-39 Area facilities (VABR, PCC, OSB, LCC, LC-39 Modular Complex D and Complex C, Pads 39A and 39B, and Lockheed Logistics Facility) to SODN Industrial Area Installations (CDSC, CIF, and HMF) and other KSC institutional networks and services. (See figure 2-4, SODN Physical Layout). Connectivity between primary SODN sites and other SODN served facilities will be accomplished via point-to-point FOIRL, Fiber Optics Token-Ring and T1 synchronous links as well as the LC-39 Broadband Communications Distributed System.

While a high speed backbone is critical to SODN's distribution, premises wiring is the key to local distribution. By prewiring a carefully chosen media for each work area, nearly all communications needs can be met in an organized and maintainable fashion. This system will allow quick responses to moves and changes.

SODN also integrates the internetwork connectivity requirements of the Shuttle Processing Data Management System (SPDMS), Engineering Data Access and Management System (EDAMS), and Shuttle Processing Contractor networks including Rockwell International, Martin Marietta, Rocketdyne, Grumman Technical Services, Inc., and Bionetics Corp. Other facilities and institutional networks will be integrated with SODN by the proposed TM Network Plan.

The SODN gains connectivity to offsite networks, through the NASA Science Internet (NSI) and the Program Support Communications Network Internet (PSCNI) via the KSC ISO router and the Industrial Area BCDS channel 6/T.

The Information Processing System (IPS) Operations System/Network Control Center is the central point for SODN customer technical assistance. This help desk can assist with questions about outages and loss of network connectivity trouble reports. Information concerning SODN support and service installation and deletion is available in the SODN Customer Interface Guide.

SODN is operational 24 hours a day, 7 days a week, except for scheduled outages. However, the SODN operations and maintenance control center is manned only from 7:15 am to 12 midnight, Monday through Friday. In general the SODN is not supported by an Uninterruptible Power Supply (UPS) and is susceptible to power fluctuations and outages.

Samples for requesting network connections are located in Appendix E.

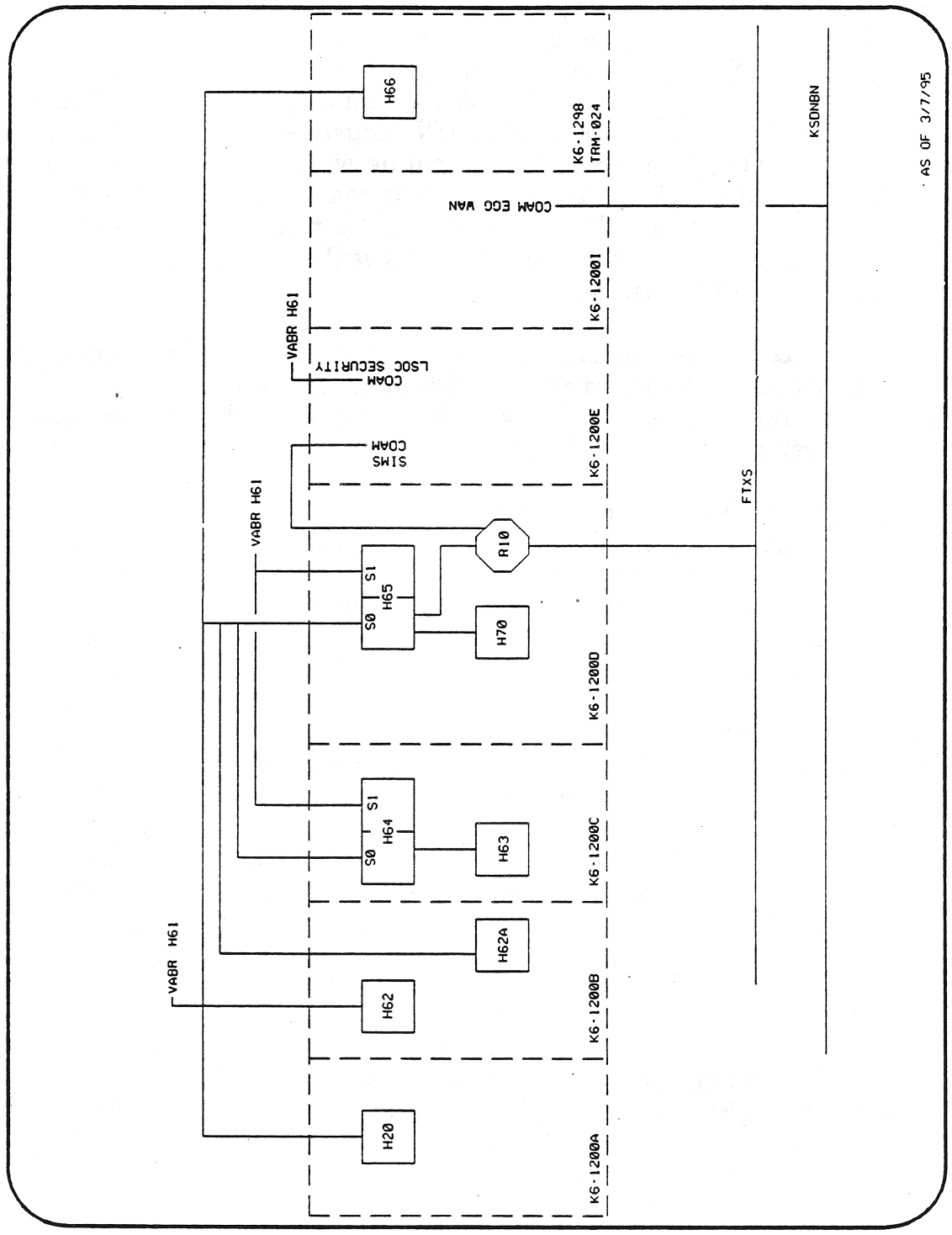


Figure 2-4. SODN Physical Layout (Sheet 1 of 8)

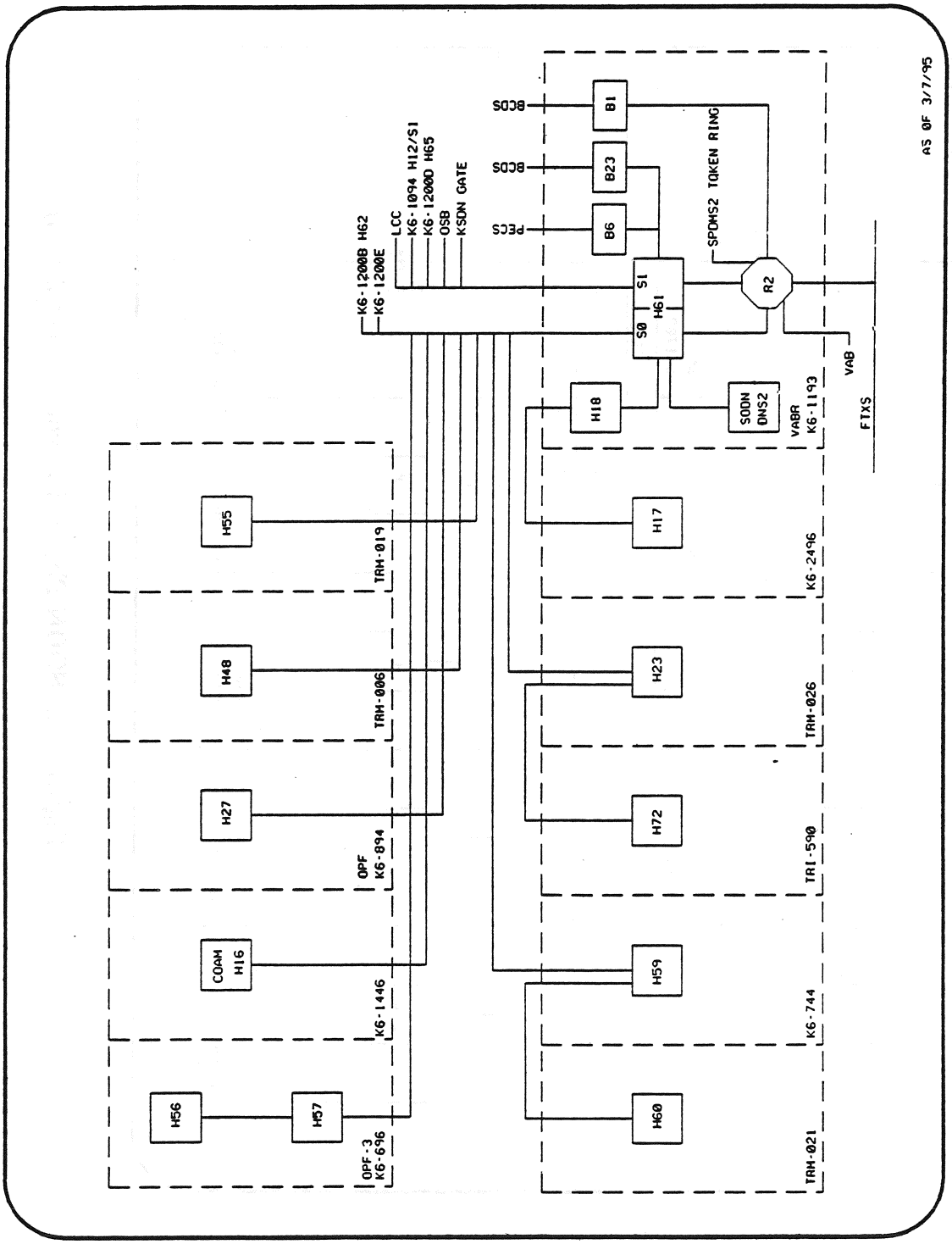


Figure 2-4. SODN Physical Layout (Sheet 2 of 8)

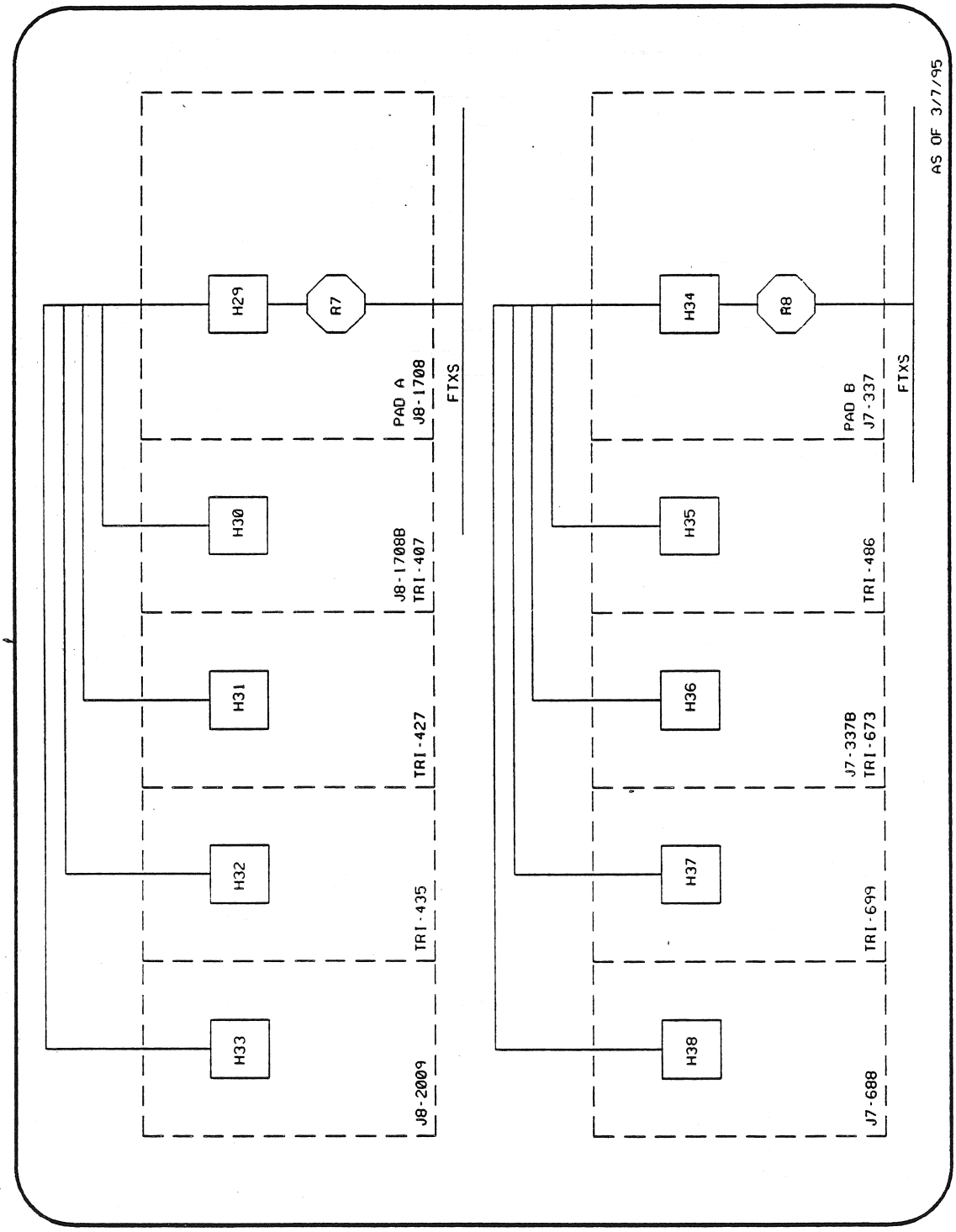


Figure 2-4. SODN Physical Layout (Sheet 3 of 8)

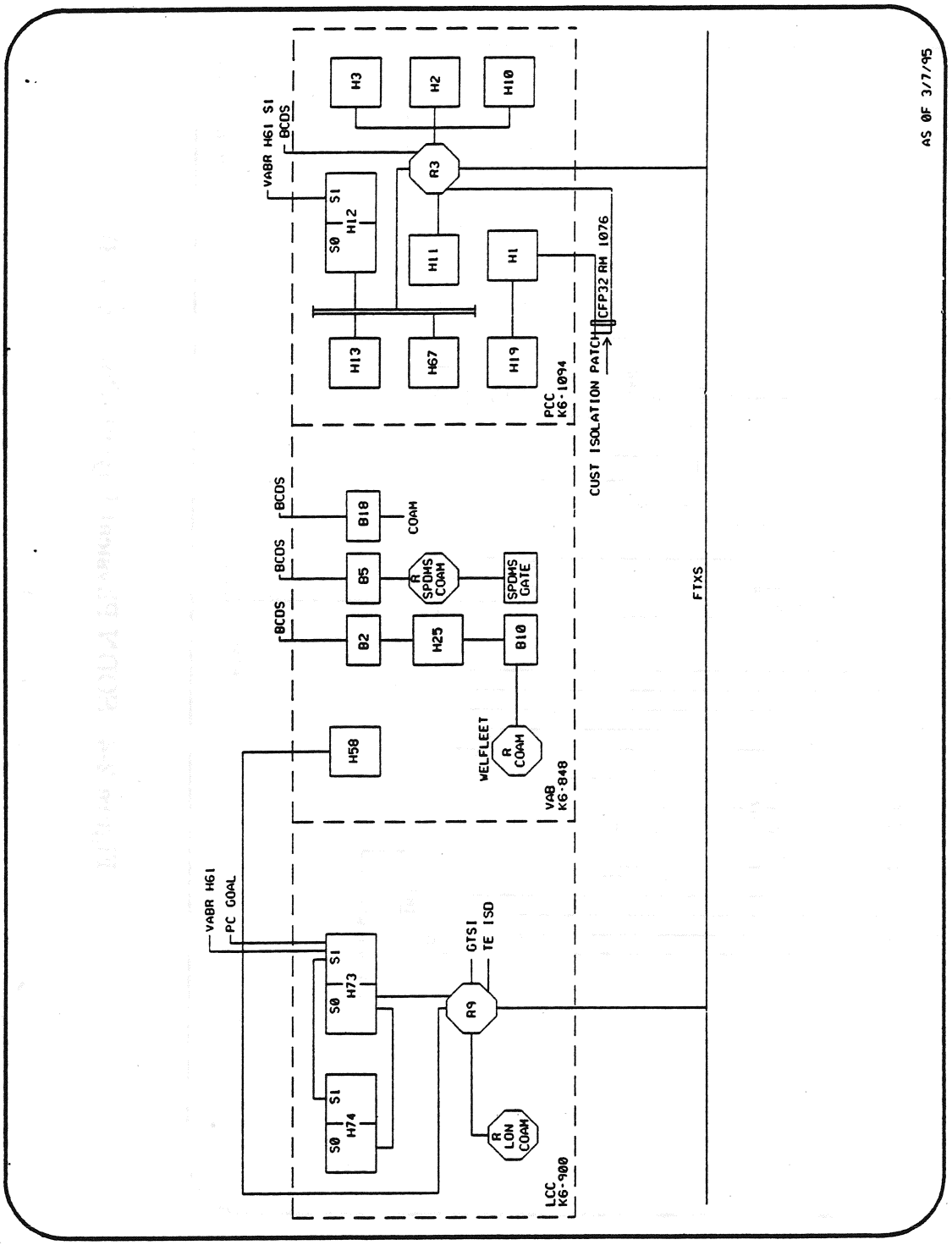


Figure 2-4. SODN Physical Layout (Sheet 4 of 8)

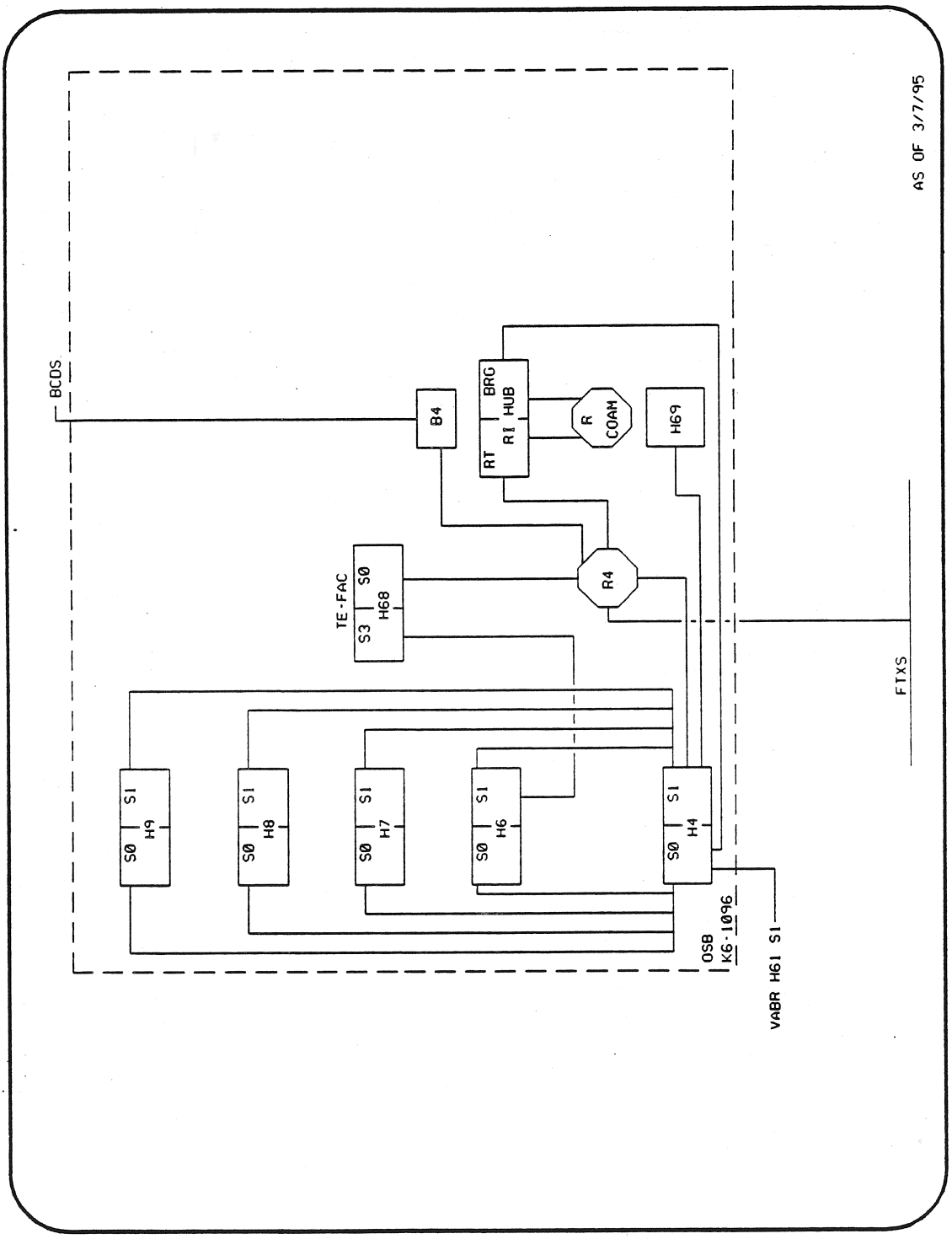


Figure 2-4. SODN Physical Layout (Sheet 5 of 8)

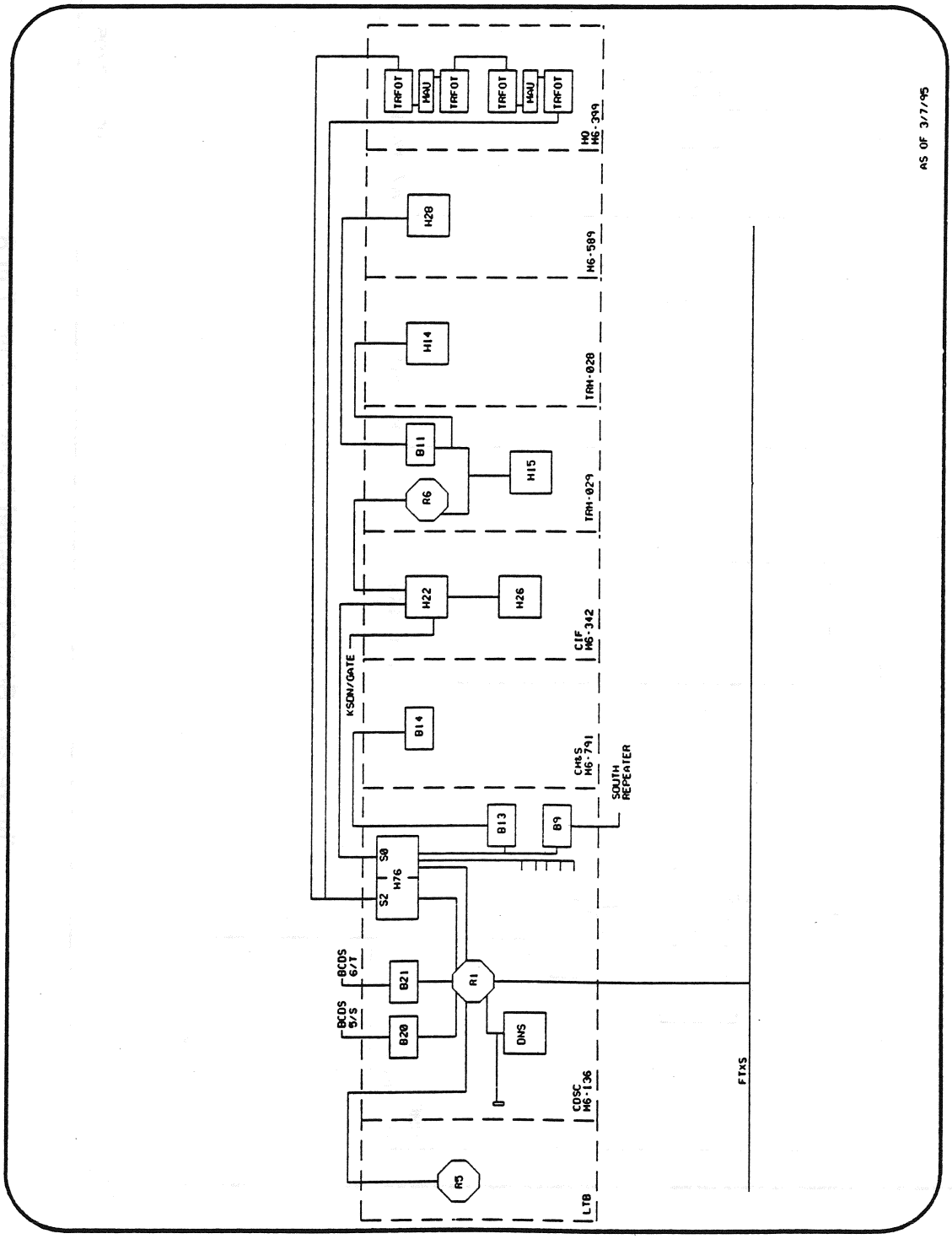


Figure 2-4. SODN Physical Layout (Sheet 6 of 8)

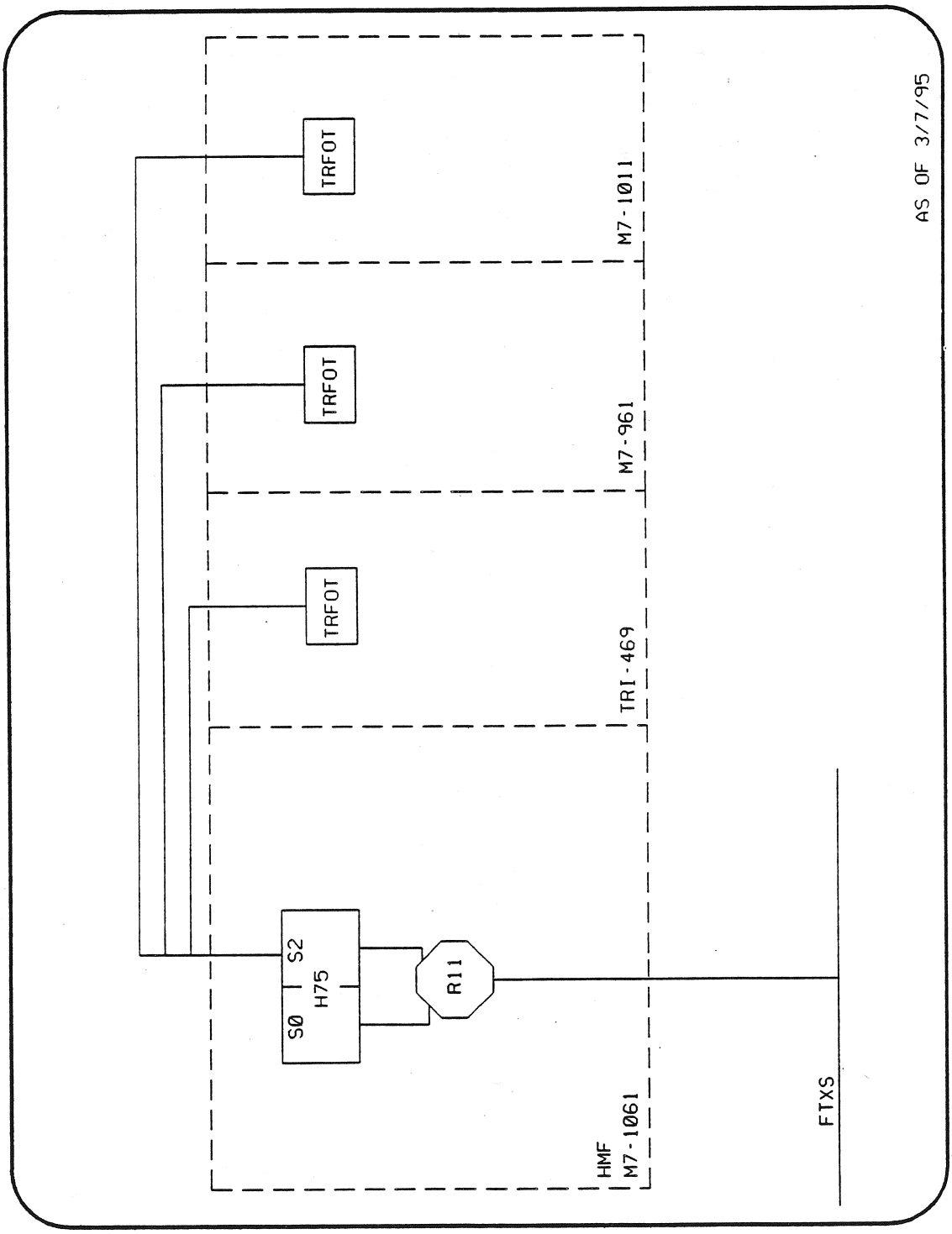


Figure 2-4. SODN Physical Layout (Sheet 7 of 8)

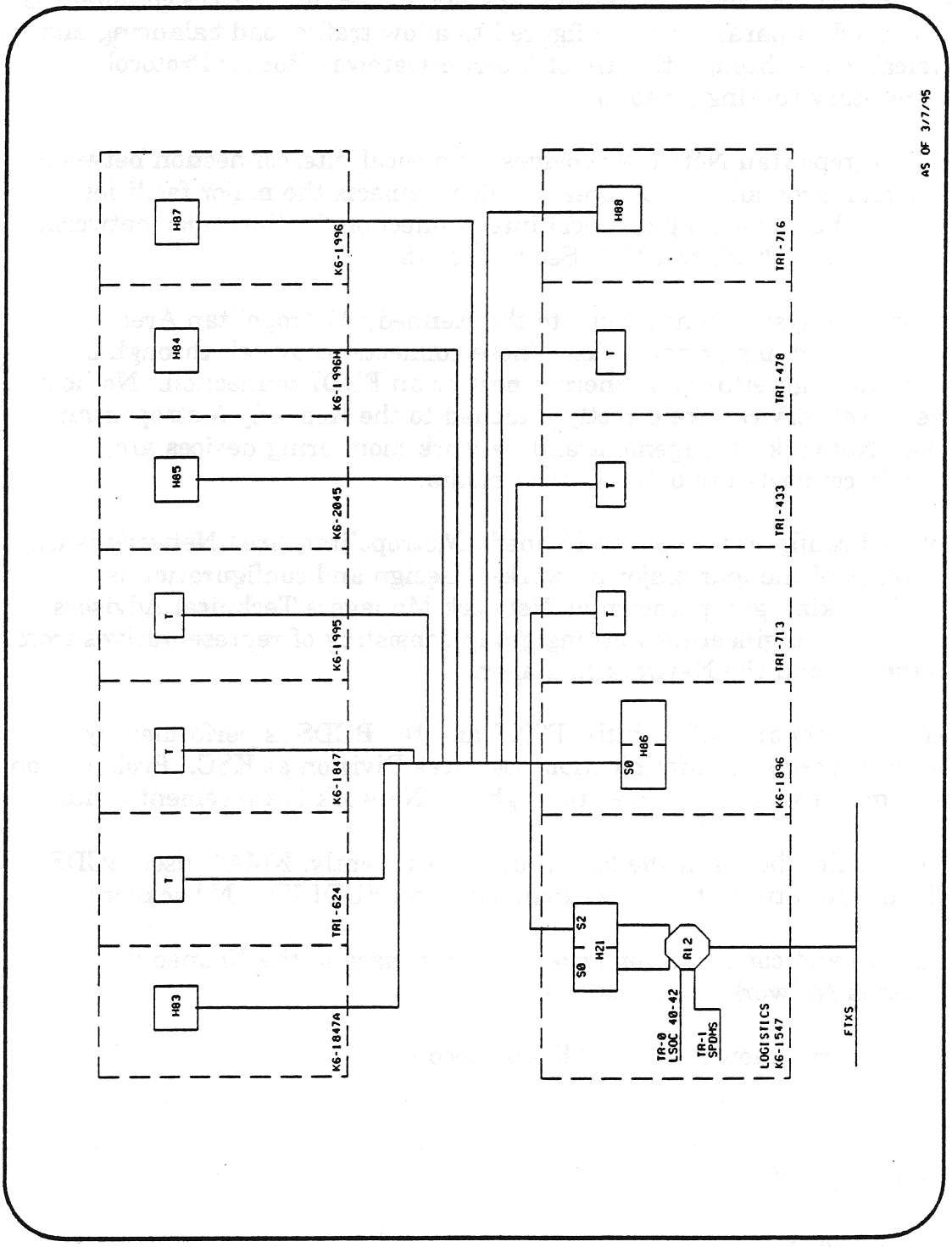


Figure 2-4. SODN Physical Layout (Sheet 8 of 8)

2.5 KENNEDY METROPOLITAN AREA NETWORK (KMAN)

The Kennedy Metropolitan Area Network is a logical network consisting of two physical networks, the Fiber Transmission System (FTXS) and BCDS channel 5/S. These systems used in parallel are configured to allow traffic load balancing and prohibit physical loops through the use of Interior Gateway Router Protocol (IGRP), a proprietary routing protocol.

The Kennedy Metropolitan Network provides a physical interconnection between the KSC Industrial area and LC-39 area. It also connects the major facilities within each area, thus providing a logical interconnection for the major networks at KSC: SODN, KDN, PON, and DE. See figure 2-5.

There are multiple physical connections to the Kennedy Metropolitan Area Network by each of the major networks. These connections are all through a KSCISO router through either an ethernet port or an FDDI connection. No host level or server level services are directly attached to the Kennedy Metropolitan Area Network. Network Management and network monitoring devices are, however, directly connected to both physical media.

Management and configuration of the Kennedy Metropolitan Area Network is the joint responsibility of the four major networks. Design and configuration is facilitated by a working group known as Network Managers Technical Advisors Group (NMTAG), an engineering working group consisting of representatives from the major networks and the Network Managers.

Operation and maintenance of both the FTXS and the BCDS is performed by Lockheed Space Systems, Communications Services Division at KSC. Problems on either of these media will be reported through the Network Management centers.

The KMAN is the link between the Hub routers. Currently, KMAN uses BCDS Channel 5/S. In the future, it will be expanded to an FDDI KMAN backbone.

Network interface and configuration criteria for interface to the Kennedy Metropolitan Area Network are as follows:

The following lists are allowable ROUTED protocols:

- IP Suite
- Novell SPX/IPX
- DECNET Ph IV

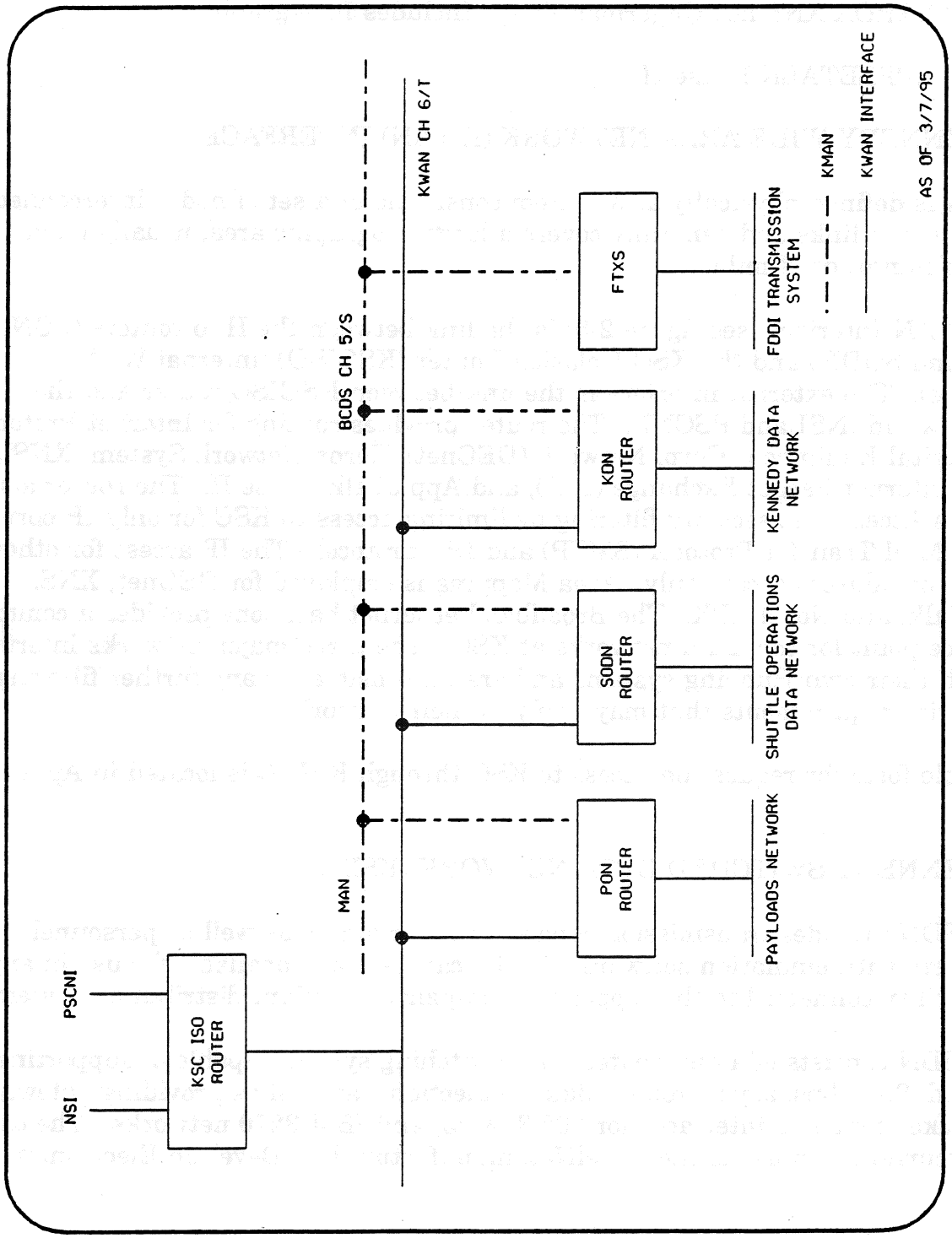


Figure 2-5. NASA/KSC NSI/PSCNI Wide Area and Metropolitan Area Networks

- OSI ES/IS CLNP
- SNA (more info to follow)
- XEROX XNS not Ungerman Bass. (Includes Intergraph)
- APPLETALK Phase II

2.6 KENNEDY WIDE AREA NETWORK (KWAN) INTERFACE

A WAN is defined physically as a system consisting of a set of nodes interconnected by a set of links and generally covers a large geographic area, usually on an order of hundreds of miles.

The KWAN Interface (see figure 2-5) is the link between the Hub routers (PON, KDN, and SODN) and the KSC Isolation Router (KSCISO) (internal WAN interface). The external interface is the link between KSCISO router and the outside world (NSI and PSCNI). The router provides routing for Internet Protocol (IP), Digital Equipment Corp. Network (DECnet), Xerox Network System (XNS), Novell Internet Packet Exchange (IPX), and AppleTalk Phase II. The router also provides Access List security filtering by limiting access to KSC for only IP port 25 Simple Mail Transfer Protocol (SMTP) and IPX protocol. The IP access for other ports is by address access only. Area Mapping is employed for DECnet, XNS, AppleTalk, and Novell IPX. The Broadband ethernet backbone provides a common interface point for the main networks at KSC. The three major networks interface through their own Hubbing systems and are responsible for any further filtering or security requirements that may apply to their network.

A sample form for requesting access to KSC through KWAN is located in Appendix E.

2.7 KENNEDY SWITCHED DATA NETWORK (KSDN)

The KSDN provides transmission capability to terminals as well as personnel computers with emulation software. KSDN can be made available for use in any KSC facility connected to the copper twisted-pair cable plant distribution system.

The KSDN consists of a distributed data switching system capable of supporting switched, 9600 bps, asynchronous data connections, as well as providing gateways and packet switched interfaces for 802.3, X.25, and IBM 3270 networks. The data switch currently in use is the DevelNet, manufactured by Develcon Electronics, Ltd.

The system was initially installed in the Fall of 1985. The architecture of the system is a distributed, multi-node configuration with high speed T1 links between the respective nodes. The primary use of the system is the transfer of administrative type data. This system offers a low cost solution for supporting a large number of users, and provides port contention to host computers allowing maximum utilization of the host's resources. The system is currently supporting fourteen such connections. Upgrade enhancements from Develcon have included a very comprehensive access control system for system administration. Within the LC-39 area, nodes are located at the VABR, VAB, boxcar complex (BCC), LCC, PCC, OPF 1, 2, and 3, LLF, and the OSB. KSDN has 250 Async ports to SPDMS. KSDN provides switched Async connectivity to SPDMS for 7171 protocol converters.

The KSDN interfaces with Data Transmission Equipment (DTE) or Data Communications Equipment (DCE) utilizing RS-232-C interface, or four-wire compatible, digital, limited distance data sets. The KSDN has the capability to accept incoming telephone calls from the KSC switched telephone network (this capability is not activated as a general access basis due to security and management policies), and provides the capability for initiating calls to the KSC switched telephone network from the KSDN. The KSDN is highly flexible in design so that configuration changes can be accomplished with minimal effort.

The KSDN uses high speed interconnecting communications facilities between nodes to reduce underground cable plant utilization. The design incorporates automatically switched, redundant central processing units, logic memory, and power supplies. The KSDN provides software alterable configuration parameters, diagnostics, and statistical data for traffic analysis.

KSDN is manned two shifts, five days a week (Monday through Friday) and for other scheduled support. The IPS Operations System Network Control Center is the central point of contact for SPC customer's technical assistance. The KDN Care Center is the point of contact for non-SPC customer's technical assistance. These help desks can assist with questions about outages and loss of connectivity trouble reports.

2.8 LOCAL AREA NETWORK (LAN)/NETWORK OPERATING SYSTEMS (NOS's)

A LAN is defined physically as a configuration of transmission facilities connected in such a manner to provide communications within a limited geographical area.

A LAN is also defined as a physical segment or series of segments connected through the use of media access devices; i.e., bridges, repeaters, remote bridges, etc. A boundary is reached when a device capable of higher level addressing is

encountered; i.e., router, gateway, etc. Logically, a LAN is a group of workstations physically connected to a transmission path boundaried by the same network address.

In general terms, a Network Operating System (NOS) consists of an applications software shell that augments the function of a user-node workstation sufficiently to handle a LAN data communications interface. For example, within a client/server environment, the NOS shell on a client workstation takes the form of a "redirector," whereas on a server it handles file-sharing capabilities. In a peer-to-peer environment, the workstation NOS not only handles the file-sharing capabilities but it also executes the redirector program.

Network Operating Systems (NOS's) have evolved from the centralized mainframe computing environments to a personal computer (PC) based distributed system. All NOS's have several common characteristics:

- Initiate a network communications path
- Emulate the resident file servers file and data structure
- Send and receive errorless data across the network
- Terminate communications gracefully

Today's NOS's are generally divided into two different categories:

- Client-server technology

- Peer-to-Peer technology

Client-server technology is based on a relatively simple but efficient way of running applications. It provides the security of a mainframe environment while letting large numbers take advantage of the simplicity of the personal computing environment. Client-server architecture splits an application into two parts and assigns the processing of each part to the resource best suited to handle it. The front-end client component presents and manipulates data on the local workstation. The back-end component of the application stores, retrieves, processes, and secures data; i.e., the file server is used for file distribution to many clients and the workstation for processing the actual file information. Some newer applications such as Structured Query Language (SQL) servers utilize the file servers' higher computing power to perform data manipulation on the server end before sending data back to the client PC. This cuts down on network traffic and helps slower client machines process data faster. This technology makes the server a centralized data source for all parties since communication must take place through this server.

Peer-to-Peer NOS's support most of the functions of client-server NOS's plus more. Peer-to-Peer workstations allow individual workstations to talk directly. They can share data and print services directly over the network and not be linked to a centralized source. Although this seems to allow more freedom, in operation it makes security and centralized data collection more difficult.

The area of NOS's also include other types of operating systems such as UNIX and its many types of remote machine communications: UNIX-to-UNIX Copy (UUCP), Remote Procedure Call (RPC), Telnet, and File Transfer Protocol (FTP). Another network operating system to gain popularity recently is the Network File System (NFS). This application allows many different types of machines and file systems to share data; i.e., a PC can store a file on a UNIX host. NFS "mounts" a drive on the initiating machine as if it were a local native drive and file system.

KSC has a variety of LANs and networking NOS's. Two of the more predominant ones are Novell's Netware and Microsoft's MS NT Advanced Server. The different KSC Institutional Networks use different LAN systems and services. These include:

KDN: Novell Netware, MSNT Advanced Server, AppleTalk
PON: LAN Manager, AppleTalk
SODN: LAN Manager, IBM LAN Server, Microsoft Network (MS-NET), ALIS, Novell Netware, and Apple "Ethertalk/Appletalk" LAN OS.

With user needs and computing requirements growing all the time, networking and NOS's need to keep changing and improving with them. Wide area connectivity across routed, bridged, and high speed serial links is becoming a major priority of users and a requirement of NOS vendors. Network management and fault tolerance are also of prime importance.

2.9 APPLETALK NETWORKS

AppleTalk is an established protocol used extensively throughout the Kennedy Space Center networking environment. (See figure 2-6, KSC Network Physical Layout - Industrial Area.) Currently, the majority of these networks are located in the KSC Industrial Area. A large number of network services are currently supported by these networks, including printing, file transfer/sharing, E-mail, and electronic conferencing. The AppleTalk networks support a significant number of programs and projects, including the Shuttle, Payloads, Space Station, advanced programs, and a significant number of the KSC mission support contractors. Wide Area AppleTalk network services are currently supported between most of the PSCNI sites, but are not currently supported across the NSI network. The service is currently scheduled for termination in August 1995 to meet the requirements of the FIPS 146 and NASA ICCN WAN policy.

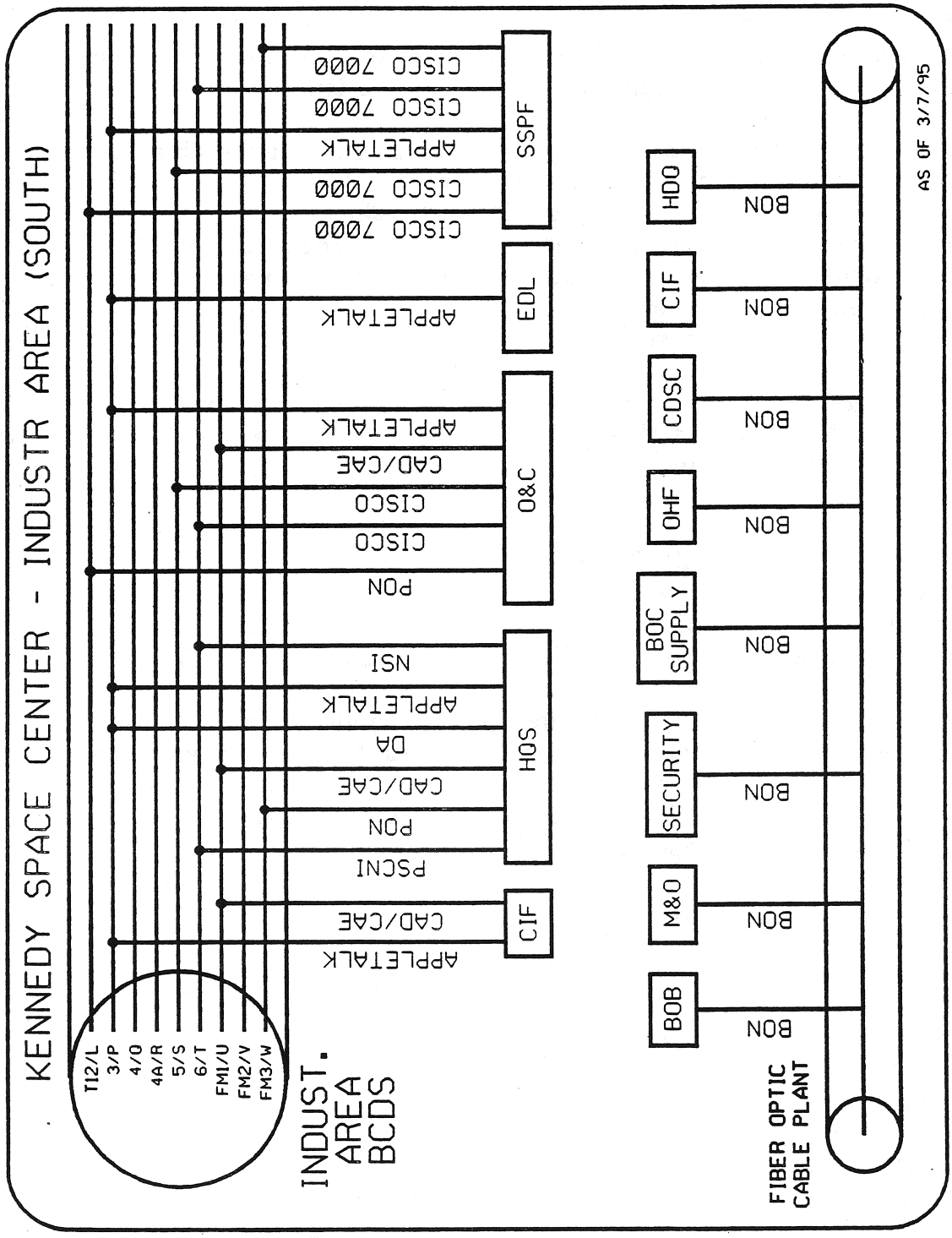


Figure 2-6. KSC Network Physical Layout - Industrial Area

There is no central point of contact for the AppleTalk networks, as they are supported by most of the existing networking organizations at KSC as a subset of the existing networks. Information concerning AppleTalk network support and service installation is available from the local networking organization care centers or help desks (see section 1.3). Support hours vary between networking organizations - this information can also be obtained from the previously listed networking organizations.

An extensive transitional effort is underway on the AppleTalk networks to provide an enhanced infrastructure for a migration to POSIT, FIPS 146.2 and other standard networking architectures. From a physical networking standpoint, this includes an elimination of all LocalTalk cabling systems (2-wire unshielded cable in a ring or star configuration with a maximum throughput of 220 kbytes/sec) and an upgrade to an Ethernet-based system. Additionally, work is underway in all of the networking organizations to migrate the services provided by the AppleTalk protocol to services provided by OSI and other approved Wide Area Network protocols without diminishing the level or quality of the existing network services.

2.10 EXTERNAL NETWORKS

The KNE has a number of external network connections to KSC contractor facilities outside of the physical boundaries of KSC. Examples are:

- Harris Core Facility, Rockledge
- Lockheed Design Engineering, Titusville (LST-2)

These networks are connected to the KNE through external interfaces in much the same way as the KNE interfaces with the Wide Area Networks. However, they are typically extended local area networks located at a site remote from KSC, and are much smaller in scope than the major networks. These may be LAN's that are set up to support a single KSC project or contract. Their scope is limited, and KSC is the principle interface for their LAN and they share KSC services. Typically, these remote LAN's are locally managed. They must conform to the same external interface policy as the Wide Area Networks.

SECTION III

RESOURCES AVAILABLE TO NETWORK USERS

3.1 INTRODUCTION

This section provides the user with information on the direct and automated services that are an integral part of the KSC Network Environment. In order to increase the scope of the capabilities available to KNE users, the Center provides on-line services and accessibility to Wide Area Networks and various mail services through gateways.

3.2 DIRECT SUPPORT

KSC is divided into three major networks: KDN, PON, and SODN. Wide area network connectivity to PSCNI and NSI is provided by DE through DL-CMD-N. One of the four organizations will provide the assistance needed to fulfill your network requirements. Assistance includes:

- Consulting with the user
- Developing requirements
- Developing a preliminary design
- Developing guidelines for a statement of work
- Estimating the cost for implementation
- Planning for future expansion

Each network group will also be responsible for providing the following user support:

- Network design and engineering
- Costing and acquisition of materials
- Installation and maintenance
- Problem determination reporting and resolution
- Performance monitoring and reporting
- Sustaining engineering

To determine which group will provide support to your requirement, consult Section I, User Information.

3.2.1 Distribution of Information

Distribution of information is one of the primary functions of the Internet Network Working Group (INWG). However, there are a number of other sources of information available to the user. These include:

- This Handbook
- Network Help Desk (see section 1.3)
- Electronic mail distribution lists
- Courses and seminars on topics in high demand offered on Center to interested participants

Users who may wish to be on an appropriate distribution list should contact the INWG for more information. See Section 4.4.

3.3 AUTOMATED SUPPORT

This section presents the user with an array of electronic services and networks offered by the institutional network authorities, NASA, and various contractors at KSC.

Computer systems and services include:

- Kennedy Mail System (KMail)
- Shuttle Engineering Computer Application System (SECAS)
- Launch Processing System Software Development Network (LSDN)
- Technical and Management Information System (TMIS)
- Shuttle Processing Data Management System (SPDMS)
- Space Shuttle Program Network (SSPN)
- Bionetics Work Order Tracking Network (BWOTN)
- Launch Processing System (LPS) Office Network
- LPS Operational Network (LON)
- Central Data System (CDS) Operational Network
- Kennedy Inventory Management System (KIMS)
- KSC Domain Name Service (DNS)
- Base Operations Network (BON)
- Payload Data Management System (PDMS)
- CAD/CAE Network
- Network Documentation System (NDS)
- DE Integrated Engineering Computer System (IECS)

Wide Area Network services include:

- Program Support Communications Network (PSCN)
- NASA Packet Switched System (NPSS)
- PSCN Internet (PSCNI)
- NASANet
- NASA Science Internet (NSI)
- Network News
- 45th Space Wing Network

3.3.1 KMail Service

KMail (short for Kennedy Mail System) is a centerwide electronic mail system that utilizes the KDN, PON, and SODN to link the different E-Mail systems at KSC together. (See figure 3-1, KMail Service.) Since there are no KMail "accounts," there is no mail system that users log onto to read mail. KMail names are used to keep track of the actual location and E-Mail system for particular users. The KMail name is the user's E-Mail locator.

KMail communicates with a variety of E-Mail systems through the use of gateways which translate mail messages into UNIX Mail (Simple Mail Transfer Protocol-SMTP). Each of the systems (i.e., IBM PROFS, All-In-One, MS Mail, ALIS, Futurus Team, etc.) sends a message through KMail (whose "native tongue" is UNIX Mail) which checks to see what user the mail is intended for, and routes the message out to that user's mail system.

A new KMail system has been implemented and operational as of June 30, 1994. The new KMail system encompasses a mail gateway (PP) and a X.500 directory service host (X500).

The KMail name has also been changed. A typical name is <first name>.<last name>-#. For example, the KMail for John Smith is: john.smith-1. The number is used to ensure name uniqueness across KSC (this is the Relative Distinguished Name, or RDN). If there is more than one John Smith, then the next John Smith will be john.smith-2.

Unlike the old KMail system, a name not recognized by the new mail gateway will not be rejected immediately. If PP does not recognize the e-mail addressee, it will ask X500 to perform a search of the real identity of the intended mail recipient. If a unique match is found, X500 will return the person's real KMail address to PP for delivery. If multiple matches are found, the matched list is returned to PP, and PP will return the rejected mail and the matched list to the sender for further mail recipient clarification.

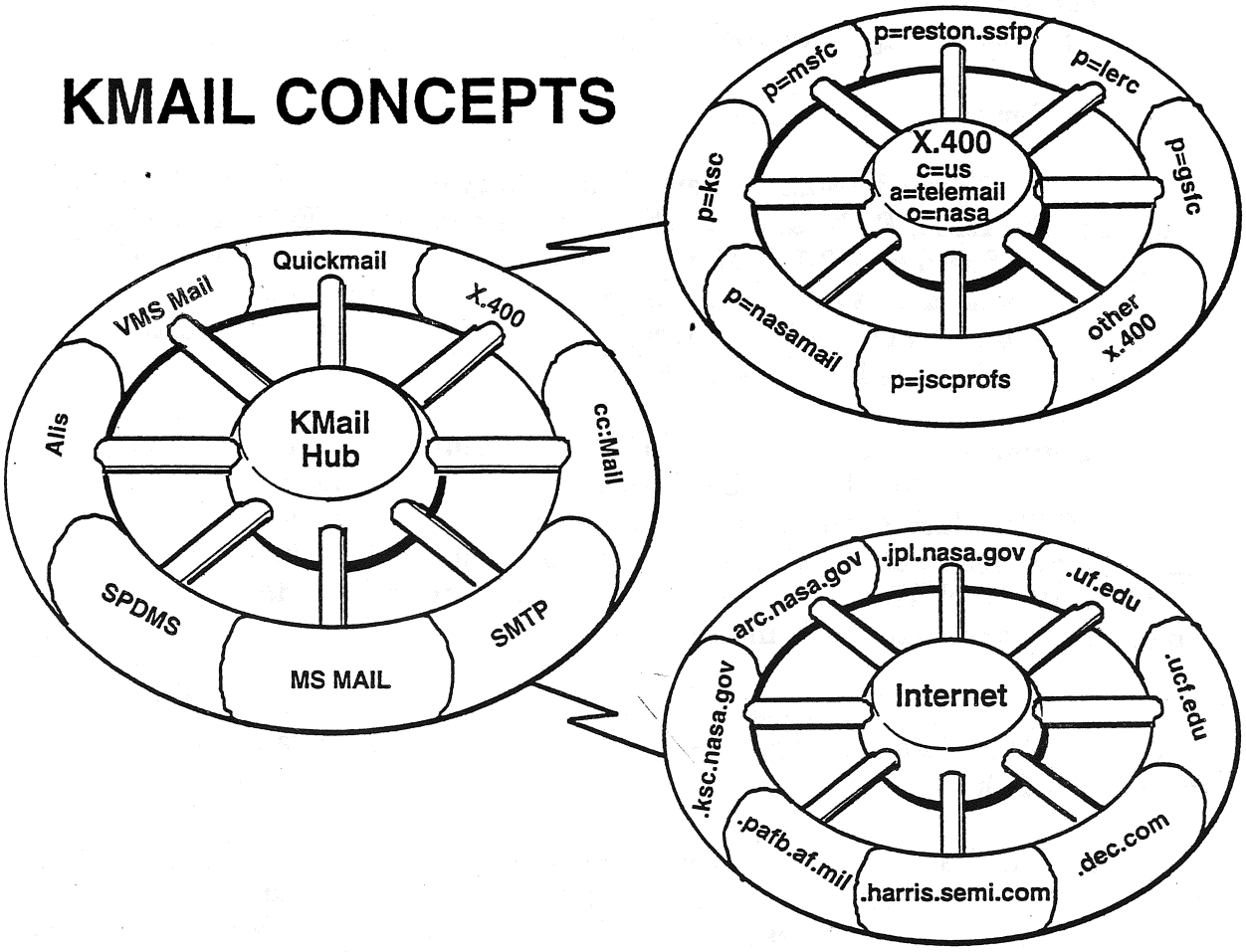


Figure 3-1. KMail Service (Sheet 1 of 2)

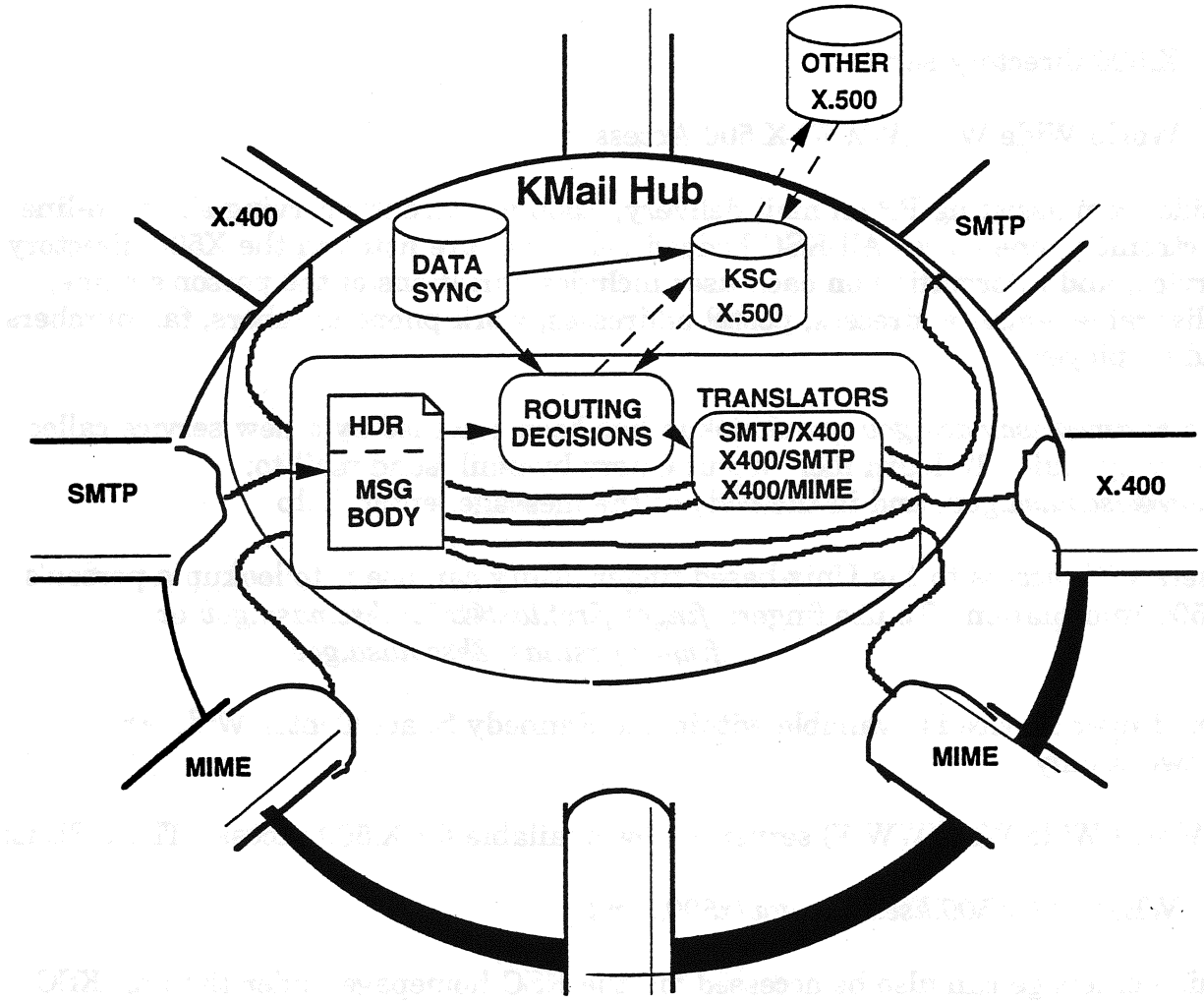


Figure 3-1. KMail Service (Sheet 2 of 2)

For example, an e-mail addressed to: *linda.myers@ksc.nasa.gov* will cause PP to pass *linda.myers* to X500 for a unique match. In this case, X500 will return *linda.myers-1@ksc* as the true KMail address to PP for mail delivery.

The new KMail system provides the following enhancements:

1. Allow a KMail message to be delivered up to 4 different e-mail addresses.

2. Attempt to deliver mail with a variety of name formats.

3. A new KMail address is assigned.

4. E-mail services are standardized across NASA centers and facilities.

5. X.500 directory service.

6. World Wide Web (WWW) X.500 Access

Aside from assisting PP on mail delivery, X500 is currently serving as an on-line electronic phone book. All KSC badged personnel are listed in the X500 directory service, and information on each user includes variations of the person's name, deliverable e-mail addresses, postal addresses, work phone numbers, fax numbers and employer.

The *kname@ksc.nasa.gov* name lookup has been replaced by a new service called Query-by-mail. To learn more about Query-by-mail, send mail to: *query@ksc.nasa.gov*, and in the body of the message, enter: help

Users with access to the Unix-based finger utility can use it to lookup a person's X.500 information. To use finger: *finger first.last@x500.ksc.nasa.gov* or
finger first.last@ksc.nasa.gov

This finger service is available within the Kennedy Space Center Wide-Area Network only.

A World Wide Web (WWW) server is now available for X.500 access. The URL is:

WHP: // *X500.ksc.nasa.govtx500.ntml*

This homepage can also be accessed via the KSC homepage under the link KSC X.500 locator service.

Further plans call for extensions to the current X.500 directory services such as yellow pages, blue pages, and distribution list management; and digital signature management.

3.3.2 Shuttle Engineering Computer Application System (SECAS)

The Shuttle Engineering Computer Application System (SECAS) is a network-based file server system designed to support LC-39 SPC test operation engineering. It functionally replaces the earlier mini/mainframe VAX based PECS (Process Engineering Computer System).

The SECAS system is based on the IBM OS/2 Operating System and utilizes NetBIOS and SNA network protocols on the SPDMS Token Ring Network. Workstations are configured, with OS/2, LAN Manager and token ring adapters which are generally implemented on PS-2 model PC's. A 3270 Terminal Emulator application is also provided for access to the host (mainframe) SPDMS II computer complex.

The SECAS server provides a central location for commonly used application software products, including: word processor, spreadsheet, flowcharter, project management and drawing/presentation tools. The server also provides for user unique and common (departmental) general file storage and functions as a print server.

3.3.3 Shuttle Processing Data Management System (SPDMS)

The SPDMS is the hardware/software platform hosting an integrated work control system which provides engineering, scheduling, and work processing/control support for Shuttle processing from landing to launch. Additionally, office and publishing services are provided within the SPDMS platform to support NASA TM and SPC contractor personnel's operational requirements necessary to complete processing tasks. The SPDMS workstations are OS/2 based and the SPDMS standard network operating system is IBM LAN Server 2.0 and 3.0.

Requests for access to SPDMS are handled by resource coordinators who are individuals assigned throughout the SPDMS application user community. Individuals at KSC can obtain connectivity by completing a SPDMS II ID Support Request, obtainable through the Information Processing System (IPS) Operations System/Network Control Center at 861-HELP (4357). For off-center access to SPDMS, Ken Taylor, LSO-131, 861-5405, is the primary contact. The NASA organization responsible is TE-ISD.

See Appendix E for a sample of the SPDMS ID Support Request form. This form provides the information required prior to granting a SPDMS userid. An Ac-

knowledgement of Understanding (AOU) form is also required to be completed and signed by the requestor. This form establishes acknowledgement by the requestor of responsibilities associated with proper user of SPDMS and government computing resources.

Depending on which intercenter network is used for access to SPDMS from off-center, additional userid and/or access authorization is required. The form to request a Security Access Control System (SACS) is also required. A SACS userid is needed when accessing SPDMS from the PSCN NPSS network. Currently, access to SPDMS from the PSCNI requires access control lists within KSC controlled network routers to be updated to permit access to the SPDMS network gateway. The form to submit these requests is currently being developed and said sample is not available for inclusion in this Handbook version.

SPDMS provides local system interfaces to the BOC AMDAHL, LSDN, EDAMS, PECS, and the SSPO SNA network.

3.3.4 Space Shuttle Program Network (SSPN)

This network currently is separate from any Rockwell networks and is linked to other SSPN offices via PSCNI services. This network is included here as a reference to other Florida Operations Network activities. The primary systems supported on this network are the Xerox 6085 workstations supporting Flight Readiness Reviews (FRR's) and the Office Automation System (OAS), consisting of IBM PC workstations and Novell file servers. JSC Resident office Level III personnel use the network for their support role here at KSC as well and have PC's, Macintosh and Xerox workstations.

The SSPN consists of Ethernet segments in Complex C, OSB, LCC, HQS, and O&C interconnected utilizing SODN and other KNE resources. The JSC Resident Office, NASA Level III, on the 6th floor of the OSB is connected to the network via the bridge on the second floor using a twisted pair Ethernet connection linking together the two universal wiring concentrators on each floor. Off center Wide Area Networking connectivity is supported via the KNE and PSCNI (see section 3.3.1.6).

Future plans for this network include upgrading the bandwidth and communications speed between buildings on site and integrating with the KIN's where possible. Plans are also underway for this network to support the Shuttle Drawing System (SDS). SDS is an image distribution system with a database of all shuttle drawings. Access to these drawings could be made available to SSPN users.

3.3.5 Bionetics Work Order Tracking Network (BWOTN)

The BWOTN supports the Bionetics photographic support contract with the U.S. Air Force at CCAS and KSC. Presently, the BWOTN is linked from the KSC HQS building to Bldg. 44401 (CCAS). The network runs on the Payload Operations Network (PON).

Future plans call for the 44401 circuit to be upgraded to a T1 carrier system and to migrate it to the 45th Space Wing Network linking with Patrick Air Force Base and the down range sites of Antigua and Ascension Island.

3.3.6 Launch Processing System (LPS) Office Network

The TE-LPS Office Network provides support for TE-LPS support personnel at KSC. It is composed of ALIS servers and PC ALIS users. PC's using the Excelan 3.5 LANWork Place for DOS can access the network, as well as PC's using the Syntax Total Net, SUN, HP 700, and IBM RS-6000 workstations.

The TE-LPS Network provides communications with the CDS network, ALIS, KMail, and other KSC sources. Network access to CDS is required and limited to the LCC segment only.

3.3.7 LPS Operational Network (LON)

The LPS Operational Network (LON) is the incorporated set of operational networks used to support Shuttle launch efforts. LON provides a unified network management for Shuttle operational networks. It is composed of existing CCMS-I and CDS networks, and their external Shuttle interfaces to LSDN, SPDMS, RNET and SODN. The CDS Operational Network (see 3.3.8) is that segment of the LON that is used to provide network access to the CDS hosts and the Special Interface Subsystems; the Real Time Interface (RTIF) and Video Simulation Interface (VSI). The operational usage of the Shuttle Data Stream (PCGOAL) is on the LON Global Bus and the feed to SODN is from the LON Global Bus.

LON has a single network access point to KSC networks via SODN and is viewed as a single "host" responsible for its internal security. It provides level 3 security protection for systems connected to LON by providing limited access to LON. Network access is blocked with routers from the open networks. Hardware and software electronic "smart card" gateways are provided to allow Telnet access to LON systems. The smart card gateways eliminated the need for encryption of passwords on the open networks. LON network management is done with a master network manager and two remote status and display stations. All network events are reported to and cleared by the CDS Control Room.

The main areas served by LON are the LCC Control Rooms 1-4 (inside the PAC's areas), the Engineering Support Area (ESA) and the Data Review Room (DRR), CDS, RPS and CCS. Existing LSDN and SPDMS stations in these areas are managed and maintained by their respective agencies. See figure 3-2.

3.3.8 Central Data Subsystem (CDS) Operational Network

The CDS Operational Network is a subset of LON. CDS is used to build Firing Room software loads and record real time test and launch data. It provides near real time data retrievals for launch and test support for the Ground Support Equipment (GSE), Hardware Interface Modules (HIM's), and provides Orbiter simulation support to Checkout, Control and Monitor Subsystem (CCMS) part of the LPS. The network is used to control special interface computers, optical disk systems, and to provide file transfers for data such as high speed remote printing and plotting. For more detail, refer to 3.3.7.

3.3.9 Kennedy Inventory Management System (KIMS)

KIMS (see figures 3-3 and 3-4) serves NASA and contractor organizations at KSC and eight remote Government and commercial sites by providing operations information on almost one-half million logistics line items in a multi-account, multi-user, multi-site environment. A single logistical application, the KIMS operates in this environment.

KIMS provides on-line and batch inventory management information processing for approximately 1,114 logistics users executing almost 50,000 transactions each day. The system, consisting of over 860,000 lines of COBOL code, is available to users 24 hours per day, 7 days per week with the exception of one 6-hour period each Sunday in which preventative maintenance is performed.

The KIMS mainframe resides in rooms 205/209/230/243 of the Central Instrumentation Facility (M6-342) at KSC. A system printer cluster located in the mail room of the KSC Headquarters Building (M6-399) as well as several smaller remote laser printers located in work areas provide hard copy output to users.

Four tightly coupled processors constituting a Bull DPS 8000/84 processing cluster with its subsystems runs under Honeywell's GCOS 4020 operating system. The software environment is made up of IDS-II data base management system, TP-8 transaction processor, and GCOS file manager. Terminal communication is provided by a primary network of 4800 and 9600 baud four-wire circuits. A growing number of KIMS users are utilizing KSC's faster and more efficient Ethernet network to access this system. KSDN and PSCN also provide access to KIMS. KIMS supports FTP file transfers to other remote host systems.

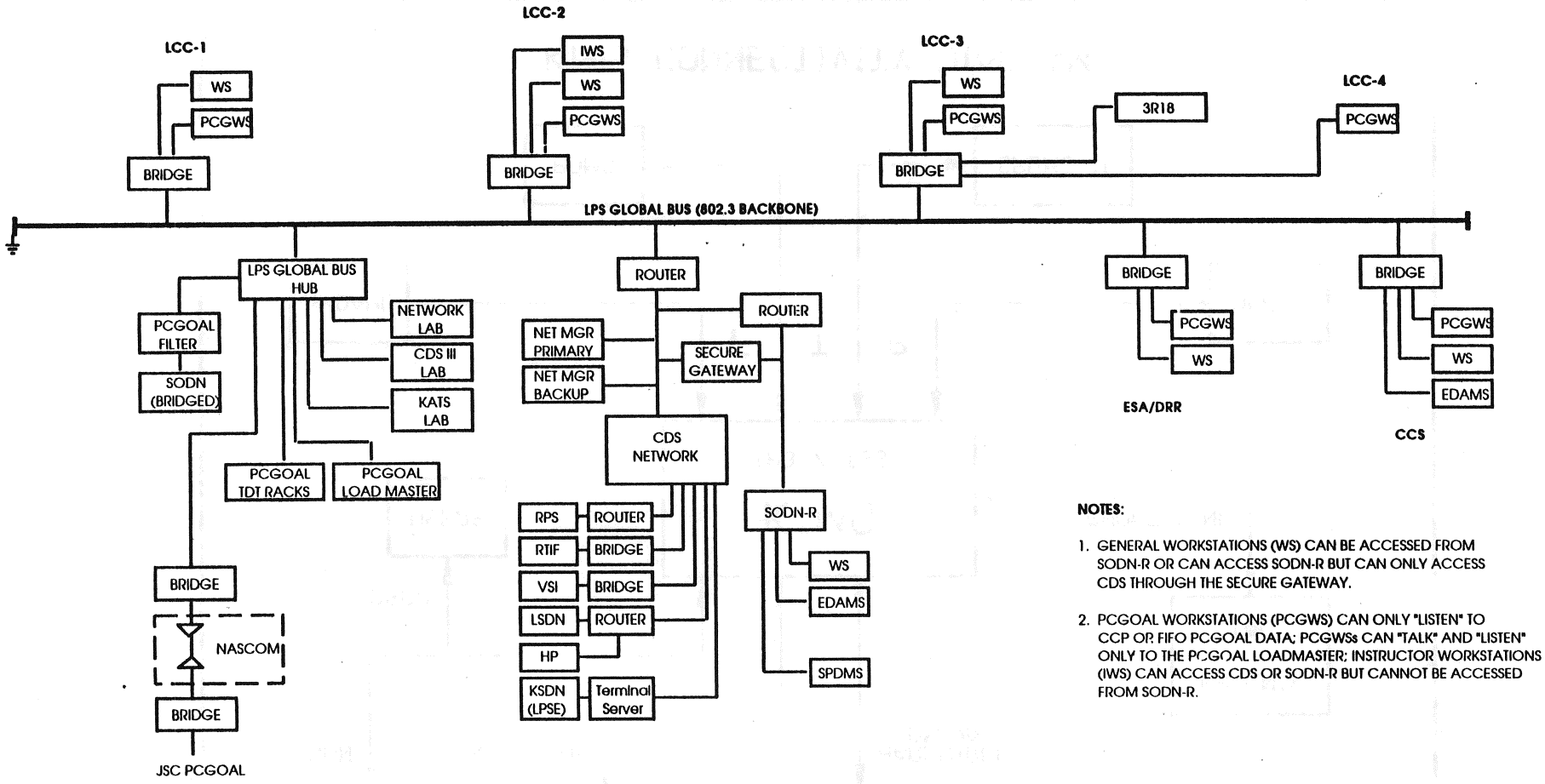


Figure 3-2. LPS Operational Network

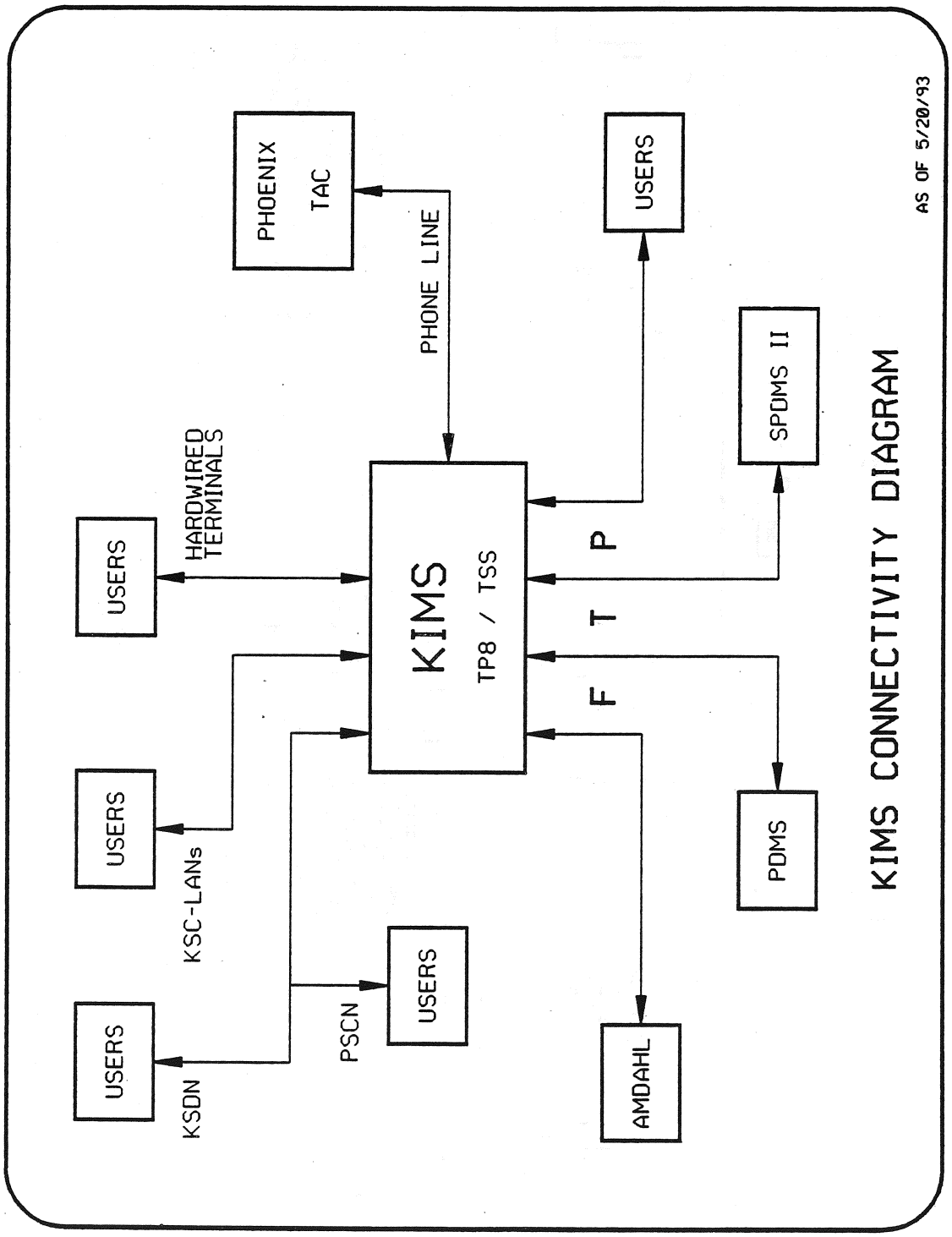
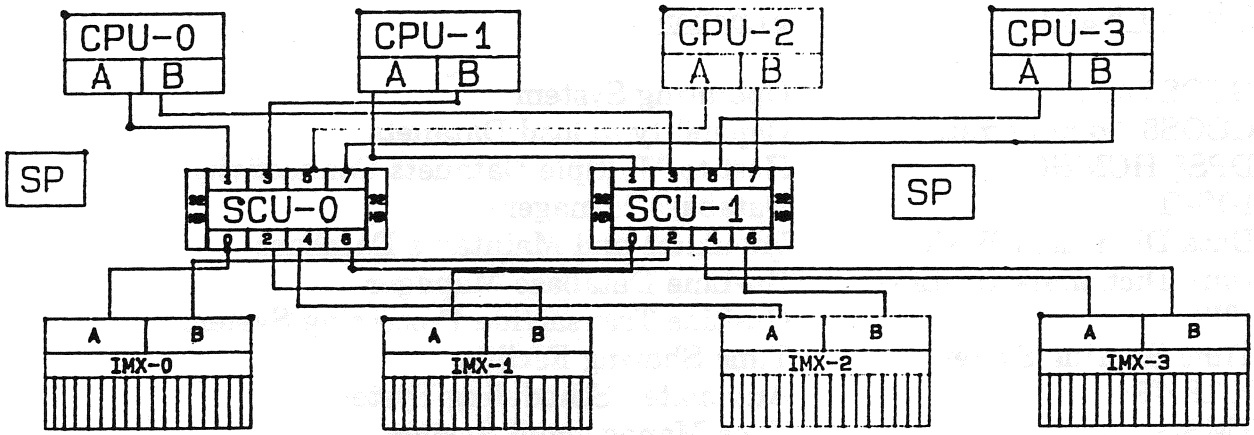


Figure 3-3. KIMS Connectivity

KENNEDY INVENTORY MANAGEMENT SYSTEM (KIMS)
DPS 8000/84
AS OF 8/24/93



PERIPHERALS

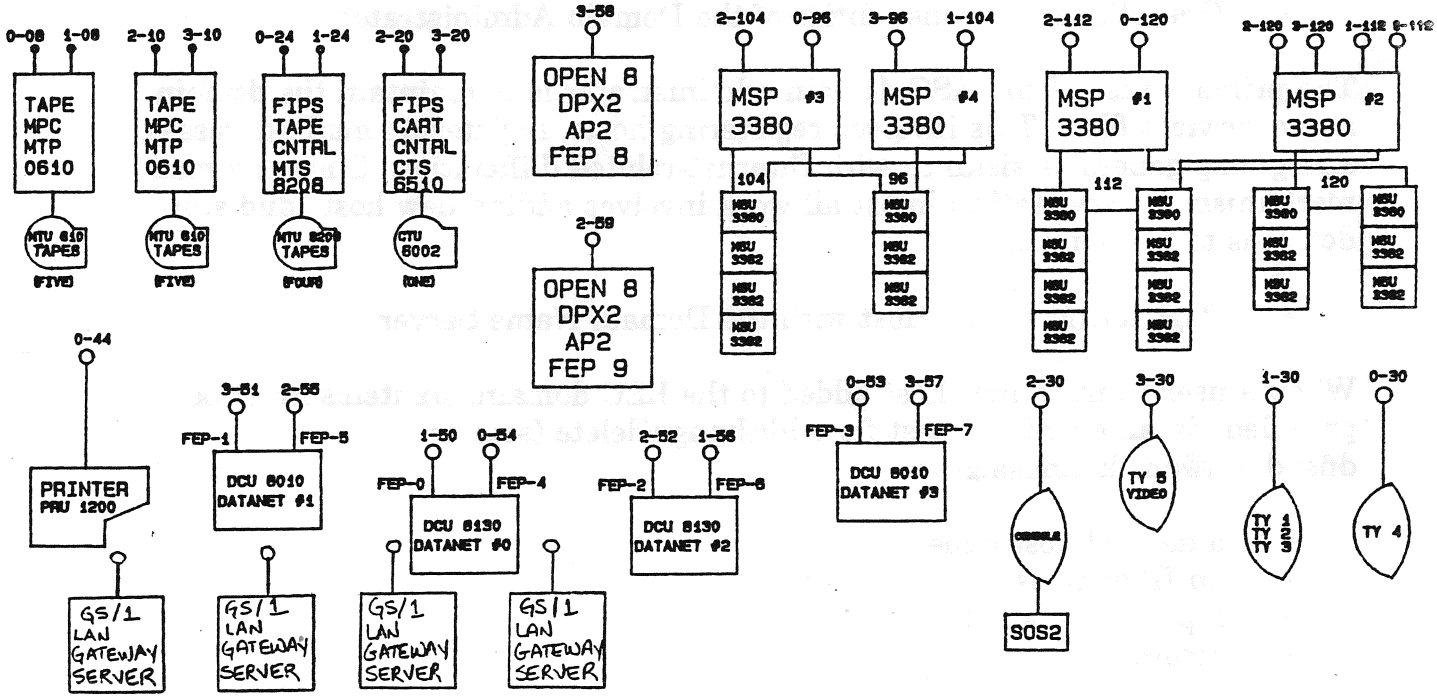


Figure 3-4. KIMS

The KIMS computing environment is stable. It is expected that routine software engineering activities involving maintenance and modifications to existing applications will proceed for the next few years.

Although the BOC will be responsible for the maintenance of KIMS application software, the contractor will not be required to provide hardware or systems software maintenance. Separate contracts presently provide these services and will remain in place throughout the life of the current KIMS computing environment.

Product Name	Function
GCOS8/4020.4	Operating System
GCOS8 Administrator	Capability to load Datanets
DPS8 HCMHC	Host to Multiple Datanets Connectivity
IDS-II	Database Manager
Data Dictionary Basic	Populates and Maintains Database
Data Dictionary On-Line	On-Line Database Manager
TP8	On-Line Transaction Processing System
Time Sharing System	Time Sharing Facility
HAPS-8	Automated Scheduling System
TMS-8	Tape Management System

3.3.10 KSC Domain Name Service (DNS)

- Operational Responsibilities of the Domain Administrator

The primary task of the KSC domain administrator is to maintain the domain name services files. This involves registering hosts, registering mail addresses, and giving general assistance with Internet-related difficulties. Since the mail mechanism is very static, almost all work involves adding new hosts and subdomains to the domain.

- Registering a New Host with the Domain Name Server

When a user wants a new host added to the KSC domain, six items must be provided via an e-mail request for add/change/delete (sent to dnsadmin@dns.ksc.nasa.gov):

- a desired hostname
- an IP address
- a point of contact
- record type

- current registration verification
- current registration delete request, if necessary

RFC 1101 provides guidance into Internet naming standards and limitations. Names cannot be longer than 24 characters, should begin with an alphabetic character, and, to avoid confusion, should not contain unusual or special characters.

3.3.11 Base Operations Network (BON)

The Base Operations Network is nested within the KDN network and receives its connection to the KMAN from the Admin-Hub. The BON consists of 34 ethernet segments spread through the industrial area and four ethernet segments within the LC-39 area. Currently, connectivity is being provided to HDQ, CIF, M&O, M6-744, BOB, Security and KIMS trailers, OHF, Environmental Health, and the CDSC within the Industrial Area. Connectivity within the LC-39 area is being provided through the SODN to segments in Complex C, LCC, and the Security offices.

3.3.12 Payload Data Management System (PDMS)

PDMS is a computer system supporting all aspects of payload processing at KSC. The PDMS-II system (see figure 3-5, PDMS-II Hardware Overview) consists of a central Digital Equipment Corp. (DEC) VAX cluster and over a thousand 386 and 486 based PC's running Client/Server and Terminal Emulation software. The older PDMS-I system consisted of a Honeywell DPS8 and a collection of HP 3000 and HP 1000 computer systems. The services provided by PDMS are broken into three major subsystems and each subsystem consists of a collection of applications as listed below:

- Relational Database (RD) Subsystem
  - Problem Reporting and Tracking System (QA)
  - Configuration Engineering (CE)
  - Work Implementation and Tracking (WIT)
  - Procurement System
  - Logistics Support System
- Project Management (PM) Subsystem
  - Mission Processing Schedule (MPS)
  - Payload Integrated Control Schedule (PICS)
  - Mission Manifest Analysis and Planning (MMAP)
  - Training and Tracking Support System (TTSS)

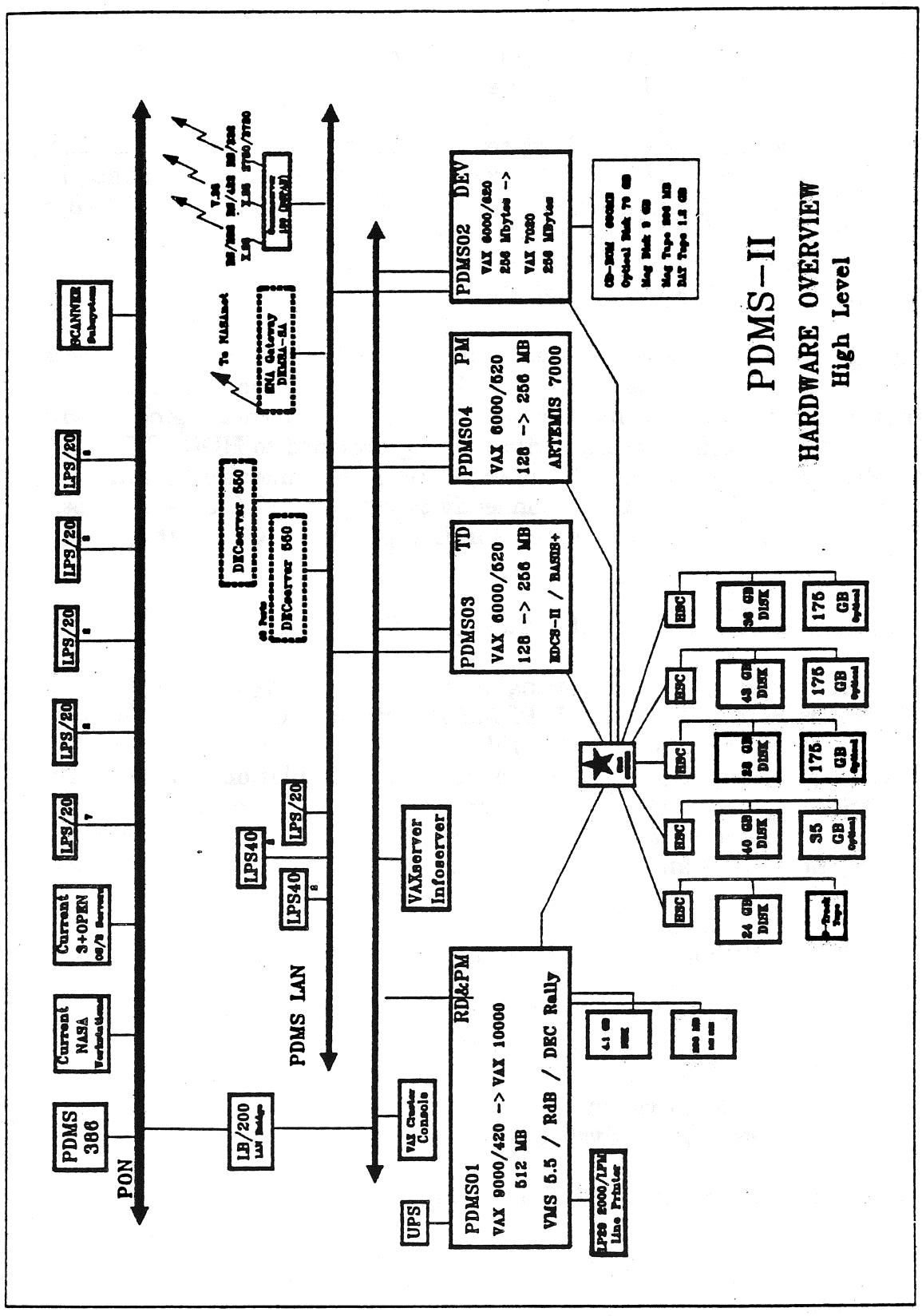


Figure 3-5. PDMS-II Hardware Overview

  - Expert Mission Planning and RePlanning Scheduling System (EMPRESS)

- Technical Documentation (TD) Subsystem

  - Documentation Creation
  - Documentation Configuration Control
  - Document Search and Retrieval
  - Electronic Document Review
  - Electronic Reports and Network News
  - Image Scanning System

Users can access PDMS services via software residing on Microsoft Windows/DOS based office workstations and OS/2 based local office servers. The central VAX host supports TCP/IP, OSI, Microsoft LAN Manager, DECnet, LAT, and NFS protocols. The workstation is running DEC Pathworks (an implementation of Microsoft LAN Manager over TCP/IP). Application software (see figure 3-6, Sample of Windows Desktop for PDMS Users) loaded on the workstation include:

- VT-340 terminal emulator for TCP/IP Telnet terminal based applications
- X-Windows/Motif server software
- Windows based TCP/IP Socket support
- Windows based Network News Transport Protocol (NNTP) News Reader
- File Transport Protocol (FTP) support
- Microsoft LAN Manager Network file and print services

3.3.13 NASA DE CAD/CAE Network

The NASA DE CAD/CAE Network (see figure 2-6) provides connectivity for the DE CAD/CAE workstations, including Intergraph, DEC, and PC's. The network communicates between Headquarters, O&C, EDL, and the CIF on BCDS Channel FM1. It provides KSC DECnet users a gateway to NSI-DECnet network, and supports TCP/IP, DECnet and XNS protocols. All IP addresses are registered in the cad.ksc.nasa.gov domain. The network contains 3 routers, 5 bridges, 10 comm servers, and 153 workstations.

3.3.14 Network Documentation System (NDS)

Being enhanced by NASA-DE and the Engineering Support Contractor (ESC) at KSC, the NDS will provide users with a centralized, on-line (self-executable) database for configuration control of KNE networks. Besides serving as a tool for documentation and identification of existing and proposed networks at KSC, the NDS will manage a common database repository for KNE users by not only allowing them access to view or to modify documentation containing information

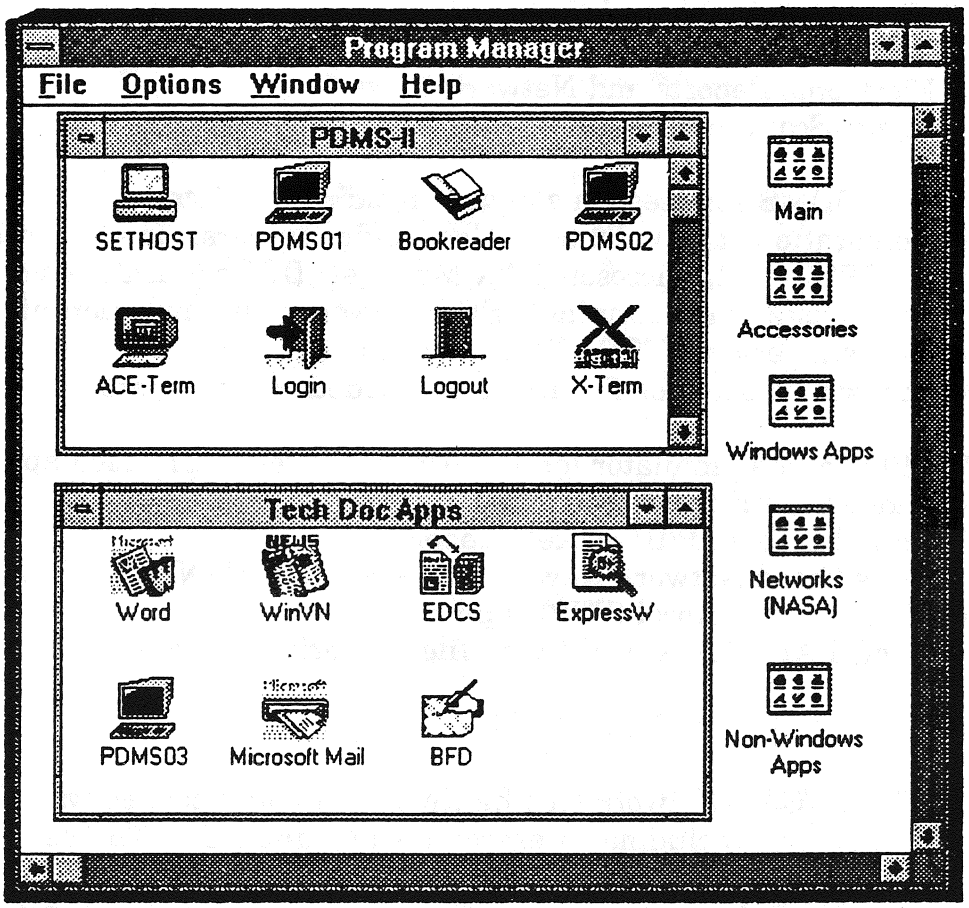


Figure 3-6. Sample of Windows Desktop for PDMS Users

on existing networks for maintenance purposes, but also will support the design of new networks. Through integration of its six primary database files, the NDS will identify all existing network cables and devices with a standardized labeling system. Its user-friendly report menus will include on-line data about the following items:

- Devices
- Cables
- Ports
- Users
- Points-of-Contact
- Node Addresses

Information from NDS databases could be downloaded from the appropriate servers throughout KSC over KNE networks to client workstations or to local network servers for easier access by users. Because it will offer an SQL-compatible graphical user interface (GUI), network users will be able to make rapid access and comparison of textual information in NDS databases. In addition, NDS will provide access to digitized CAD diagrams containing graphical schematics of network connections and configurations.

KNE users will be able to save time during design, installation, and testing of network equipment by taking advantage of NDS reports to verify network connectivity before beginning any of these tasks. By establishing a system baseline through consolidation of new or existing network configurations into its common databases, the NDS will afford users increased system maintainability during design and implementation phases.

To access and read the NDS facilities and network drawings, login as follows (via FTP or TELNET):

Open KSCDL1.ksc.nasa.gov or 128.159.166.1
Type ANONYMOUS <-- username
Type YOUR NAME <-- password

For additional information on these and other NDS features, contact Felix A. Soto Toro, DL-CMD-N, 867-2228.

3.3.15 The DE Integrated Engineering Computer System (IECS)

The Integrated Engineering Computer System (IECS) will provide a state-of-the-art computing environment to the Engineering Development (DE) Directorate and

its contractors. Initially the IECS will consist of a prototype system for evaluation, qualification, and demonstration of advanced workgroup concepts. The IECS will be implemented to facilitate future evaluation of migration paths to ATM and SONET-based network technologies. The IECS will provide:

- a current generation
- scaleable physical network to the user's desktop
- a common suite of workgroup software
- an integrated series of network file and computer servers
- a proactive user support capability to monitor, identify, and correct system anomalies

The initial IECS is a series of physical networks located at KSC that make up one logical network for use by DE workgroups to accomplish daily administrative requirements, as well as engineering design and test requirements. The physical design centers around switching concentrators and/or routers in the Headquarters building, the O&C, the LETF, and the EDL as required. Design, wiring drawings, system drawings, and labels will conform to the KSC Network Documentation System (NDS) standards (see 3.3.14).

The IECS will provide initial support for three classes of users: low, medium, and high speed/volume. The high capacity users are generally high performance workstations or servers/mainframes. The medium capacity users include engineering workstations or CAD workstations with frequent access to servers and user file servers; i.e., NT servers or Novell servers. The low capacity users are the general office personal computers and engineering workstations not requiring frequent server access.

High speed connections will be accommodated by direct FDDI connectivity to IECS. Medium and low capacity access to the IECS will be ethernet connected. To differentiate between low and medium capacity ethernets, the number of network devices (users) on an ethernet segment will be controlled. The guideline for medium capacity segments is 10 to 20 users per segment. Low capacity segments will support up to 84 connections per switched ethernet segment. Low and medium capacity users can be mixed on a segment; a medium capacity user will be equivalent to 6 low capacity users.

Facilities will be linked through a routed interface to the FDDI Transmission System (FTXS), or the existing KMAN backbone BCDS channel 5/S. KWAN connectivity will be provided through a routed interface to the BCDS channel 6/T at the central hub location. For further design criteria and performance requirements of the physical network equipment, see 79K33909.

The IECS routers, switching concentrators, and the intermediate distribution hubs will all be actively managed network devices. Network management will be provided by Simple Network Management Protocol (SNMP) compliant equipment. The network management system will provide a proactive user support capability to monitor, identify, and correct system anomalies.

IECS will be implemented to support workgroup distribution to allow the sharing of system resources in the most efficient manner; i.e., shared data and applications will be maintained on an individual segment wherever possible. IECS will standardize the basic user office software in order to maximize supportability and cross platform integration. The standard software environment will integrate Macintosh and IBM-PC with common file servers using Microsoft NT Server.

3.3.16 Program Support Communications Network (PSCN)

The PSCN is a versatile, digital WAN employing terrestrial transmission facilities that interconnect 18 NASA locations. (See figure 3-7, PSCNI Update and figure 3-8, PSCN Backbone Systems). The system provides NASA with:

(1) improved quality and variety of communications service.

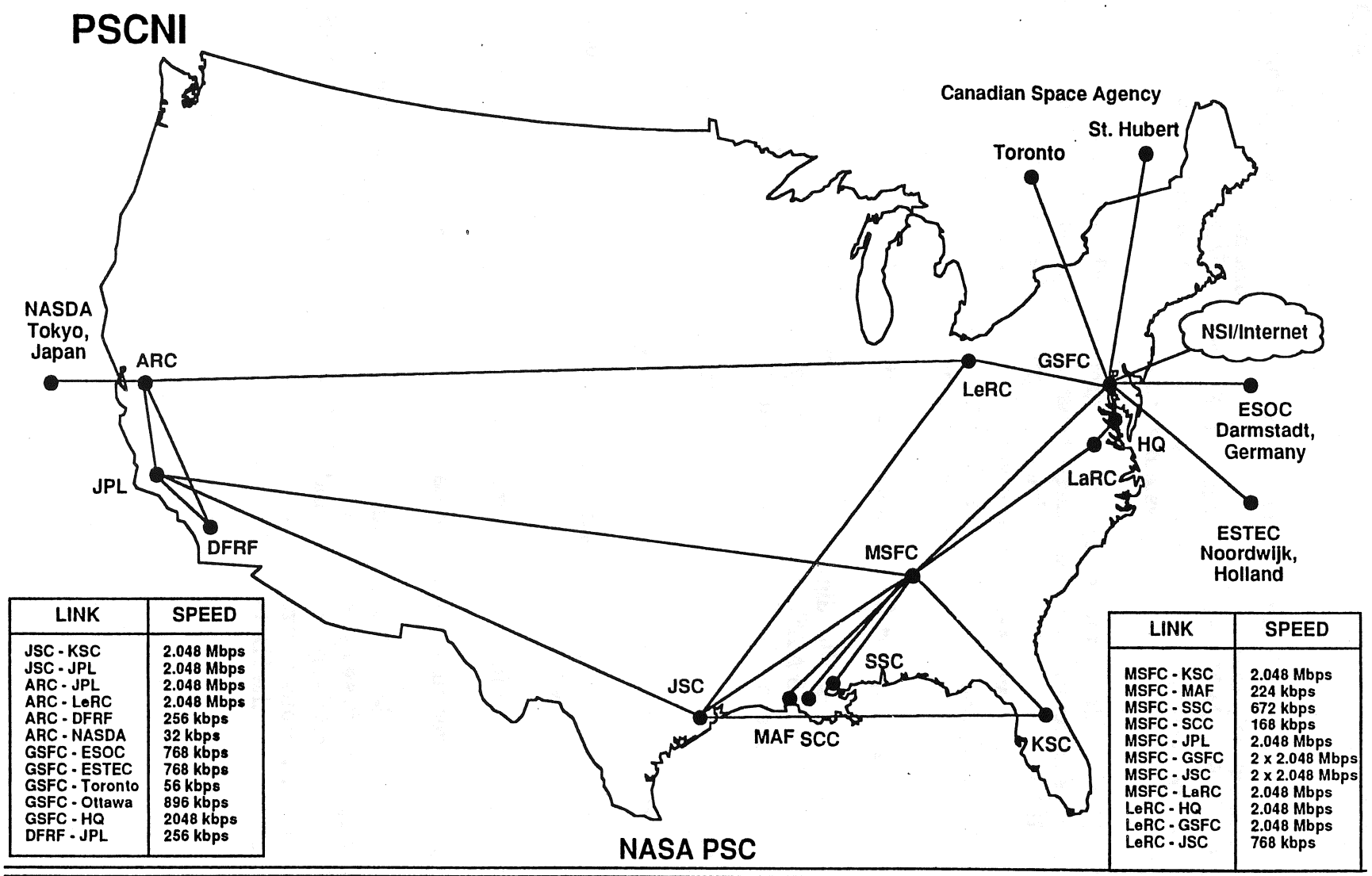
(2) rapid response to new or changed network services and requirements.

(3) advanced information exchange capabilities to reduce or avoid other NASA direct costs.

(4) better traffic data for future planning.

(5) improved maintenance of network configurations.

The PSCN provides service including long distance telephone communications, packet and circuit switched data communications, facsimile and electronic mail, voice and video teleconferencing, and the PSCNI connections between NASA centers and various contractor locations. The PSCN also provides the NASANet circuits between the IBM/SNA host at the various centers.



LINK	SPEED
JSC - KSC	2.048 Mbps
JSC - JPL	2.048 Mbps
ARC - JPL	2.048 Mbps
ARC - LeRC	2.048 Mbps
ARC - DFRF	256 kbps
ARC - NASDA	32 kbps
GSFC - ESOC	768 kbps
GSFC - ESTEC	768 kbps
GSFC - Toronto	56 kbps
GSFC - Ottawa	896 kbps
GSFC - HQ	2048 kbps
DFRF - JPL	256 kbps

LINK	SPEED
MSFC - KSC	2.048 Mbps
MSFC - MAF	224 kbps
MSFC - SSC	672 kbps
MSFC - SCC	168 kbps
MSFC - JPL	2.048 Mbps
MSFC - GSFC	2 x 2.048 Mbps
MSFC - JSC	2 x 2.048 Mbps
MSFC - LaRC	2.048 Mbps
LeRC - HQ	2.048 Mbps
LeRC - GSFC	2.048 Mbps
LeRC - JSC	768 kbps

Figure 3-7. PSCNI Update

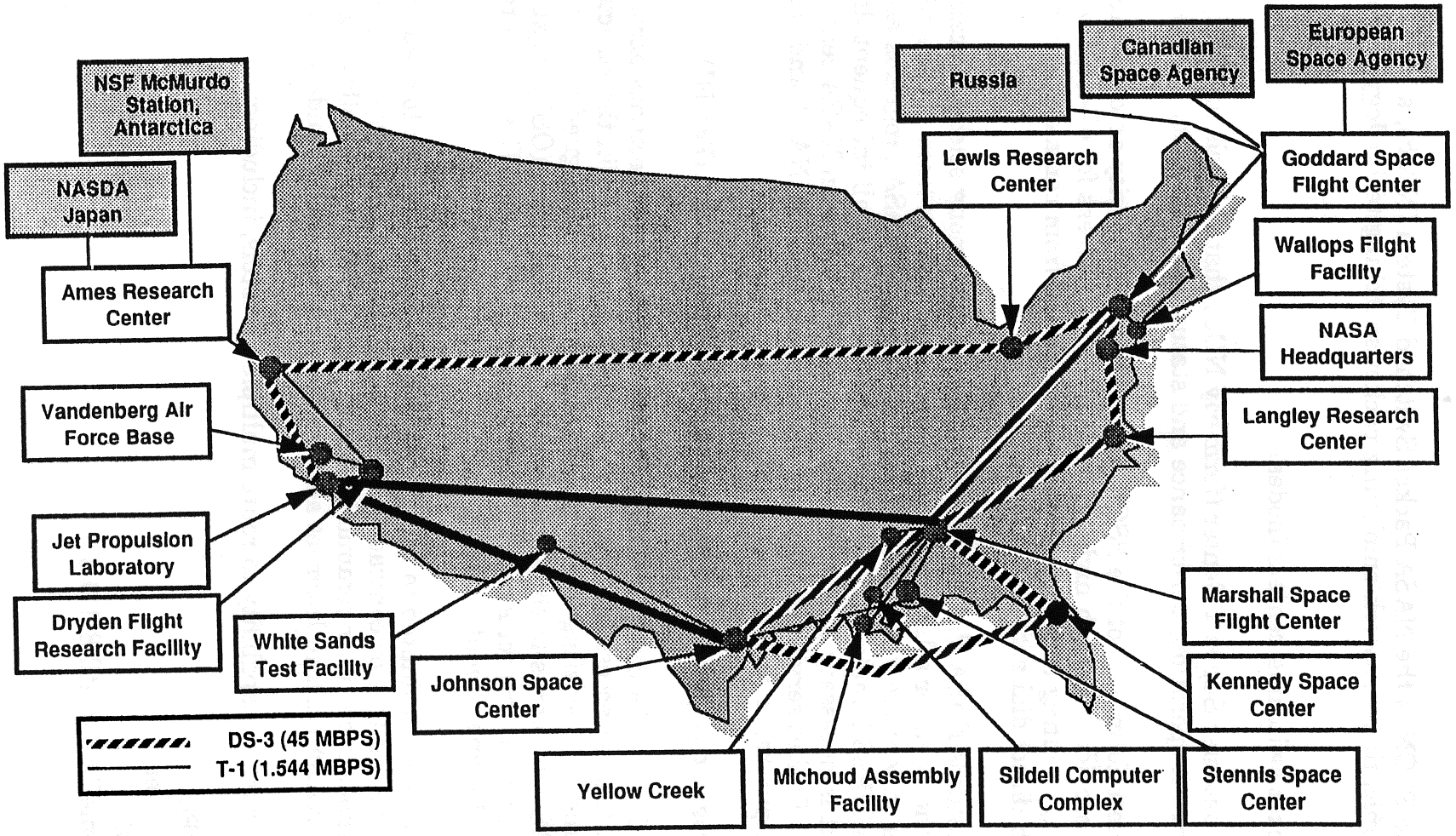


Figure 3-8. PSCN Backbone Systems

3.3.16.1 NASA Packet Switched System (NPSS)

A part of the PSCN is the NASA Packet Switched System (NPSS), a NASA-owned data communications network employing packet switching technology. The system consists of:

- packet switching centers (nodes)
- a Customer Support Center (formerly NCC) that controls and monitors network operation, performance and status 24 hours a day, 7 days a week

Together, these form part of the PSCN backbone. Connectivity among NASA locations is provided through high-speed trunk lines. Access for off-net users and supplementary routing is provided by leasing services from commercial vendors and through direct dial access.

The NPSS affords NASA the efficient transfer of data among selected locations, decreasing the need for a large number of dedicated private lines. It provides service for a wide variety of applications. In support of NASA programs and projects, the NPSS handles much of the interactive and small infrequent data transfer that is necessary for routine communications between NASA centers and contractors. Packet service is available through the NPSS to NASA and contractor host computers, as well as many public data bases.

3.3.16.2 Program Support Communications Network Internet (PSCNI)

The PSCNI is a NASA communications service providing connectivity across an established, limited access internet. The PSCNI operates within the structure of the PSCN and uses existing hardware and software. It is designed to provide a path for NASA networks to the Open Systems Interconnection (OSI). It applies Advanced Research Project Agency (ARPA) Internet Protocols (IP's) for network operation and management.

Designed for, but not limited to large file transfers between hosts located at different NASA centers or contractor LAN's and WAN's, PSCNI primarily serves the NASA space flight user communities. A special arrangement allows connections to the NASA Science Internet and the National Science Foundation Network.

The PSCNI has the capability to route multiple protocols, including:

- TCP/IP
- DECnet
- XNS
- AppleTalk (until 8-1-95)

- Novell IPX (until 8-1-95)
- ISO-OSI

The internet consists of a dedicated LAN at each designated PSCNI Gateway location. Each LAN is called the PSCNI LAN and employs standard Ethernet technology. LAN's are connected through routers and dedicated backbone circuits. Each LAN has serial connectivity to at least two other gateways to provide load balancing, redundancy and availability.

To report PSCNI problems, call the PSCN Network Management Group, (205) 961-4000, and ask for Dale Stinson or Kathy Gordon.

3.3.17 NASANet

NASANet is an agencywide SNI null network linking NASA SNA networks throughout the United States. (See figure 3-9, NASANet.) It consists of high speed Synchronous Data Link Control (SDLC) full duplex data links provided by PSCN. These links provide each site with file transfer and interactive access to the computing facilities at NASA locations.

Current access to NASANet at KSC is provided through the BOC, Amdahl, and SPDMS SNA networks.

NASANet is managed by MSFC under the direction of the NASANet/PSCN user's group. Johnson Space Center (JSC) provides technical direction and general network management support. Funding for NASANet is currently not budgeted and is being supported through MOSC (JSC/DPSD) utilizing existing resources. Other NASANet sites are also utilizing existing computer and technical resources, to assist in the overall effort.

The scope of the project is to provide NASA with a network management system for NASANet. This system will be used to plan, monitor, and control the agencywide SNI backbone network. The management system will provide:

- Data Communication Design and Engineering
- Network Systems Integration
- Performance Analysis
- Capacity Planning
- Problem Management
- Network Operations

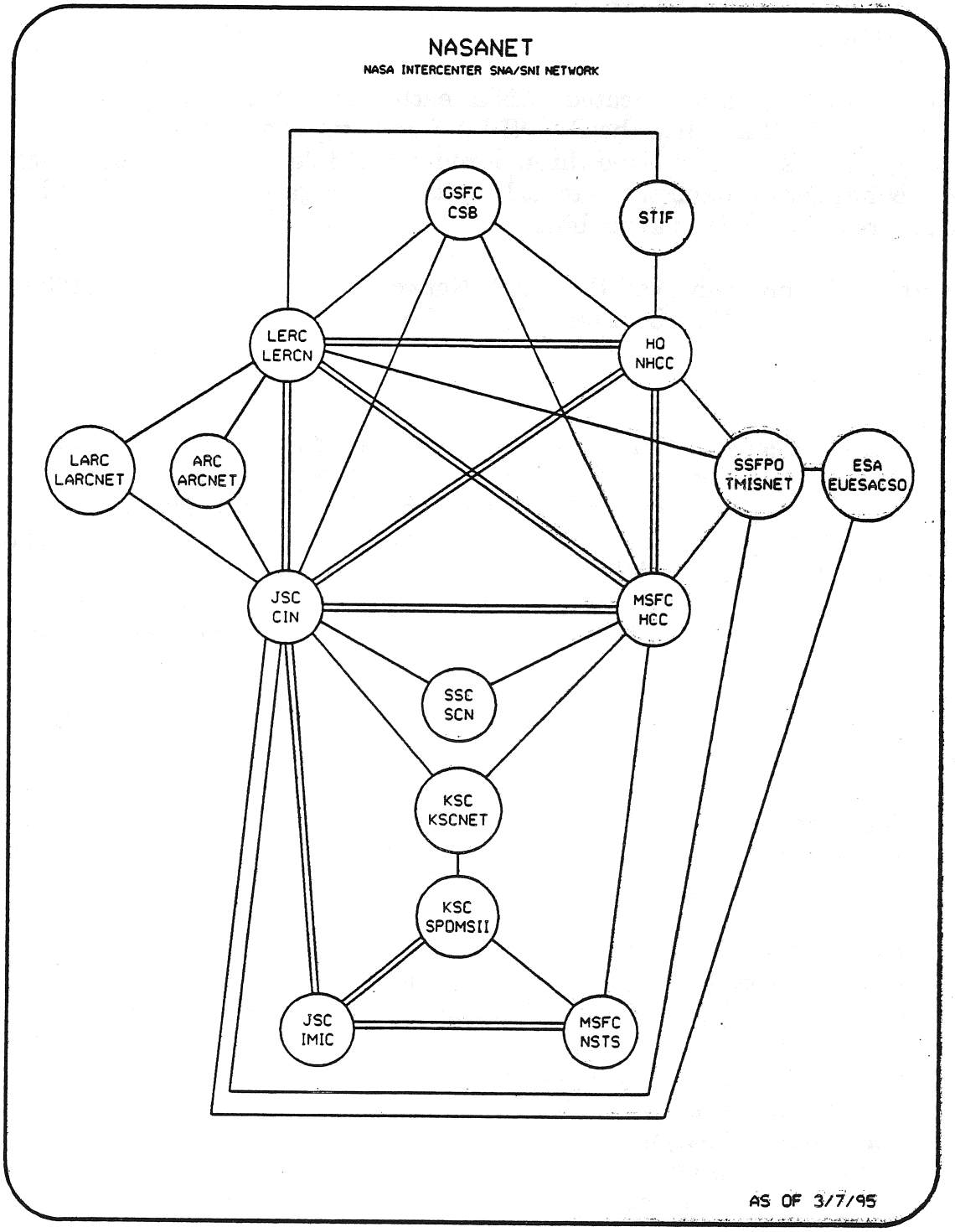


Figure 3-9. NASANet

3.3.18 NASA Science Internet (NSI)

The NSI user community consists of scientists and engineers from a broad range of science disciplines including astrophysics, earth sciences, solar system exploration, space physics, life sciences, and microgravity sciences. The NSI supports all NASA science flight missions, discipline research programs, and collaborating scientists at NASA Centers and elsewhere. NSI is not to be used for private gain or profit.

The NSI is a high-speed, multiprotocol, international network (see figure 3-10, NSI International) currently supporting DECnet, TCP/IP, and OSI protocols. In 1989, both the DECnet-based Space Physics Analysis Network (SPAN) and the TCP/IP-based NASA Science Network (NSN) were brought together in this country as a single network designated as the NSI. (See figure 3-11, NSI National.) By using multiprotocol circuits and routing, NSI was able to provide the NASA science community with higher speeds (up to 1.5 Mbps), and enable NASA supported communities using diverse computer platforms to communicate via the Internet. NSI offers both basic and priority services. NSI provides its basic network connectivity to data archives, computational facilities, and collaborators worldwide. This service provides an open, secure, shared network to assure mission success. Priority service builds on basic services and includes high-speed dedicated lines in addition to the basic services. To facilitate file transfer, E-Mail, and remote login between computers using TCP/IP and DECnet communications protocols, NSI provides its users with access to the larger Internet community by providing direct connections to other U.S. Government agency networks such as the National Science Foundation's NSFnet, the Department of Energy's ESNET, and mid-level networks in the United States and abroad. Backbone and end user connectivity is provided primarily by PSCN.

3.3.19 Network News

The Network News system (also called Usenet News) is a distributed bulletin board system that runs on hundred of thousands of computers worldwide. Usenet News users exchange views and information through written articles transmitted automatically between computers in the network. KSC has a number of Network News servers linked to other servers at each NASA center.

Over 2,000 newsgroups, organized by topic, currently reside on Usenet. New groups are created automatically by the network (after a vote of the network population) and old newsgroups are automatically deleted. Newsgroup topics are organized into a hierarchy that resembles a tree structure. The distribution of each newsgroup can be controlled by the newsmanager at each side.

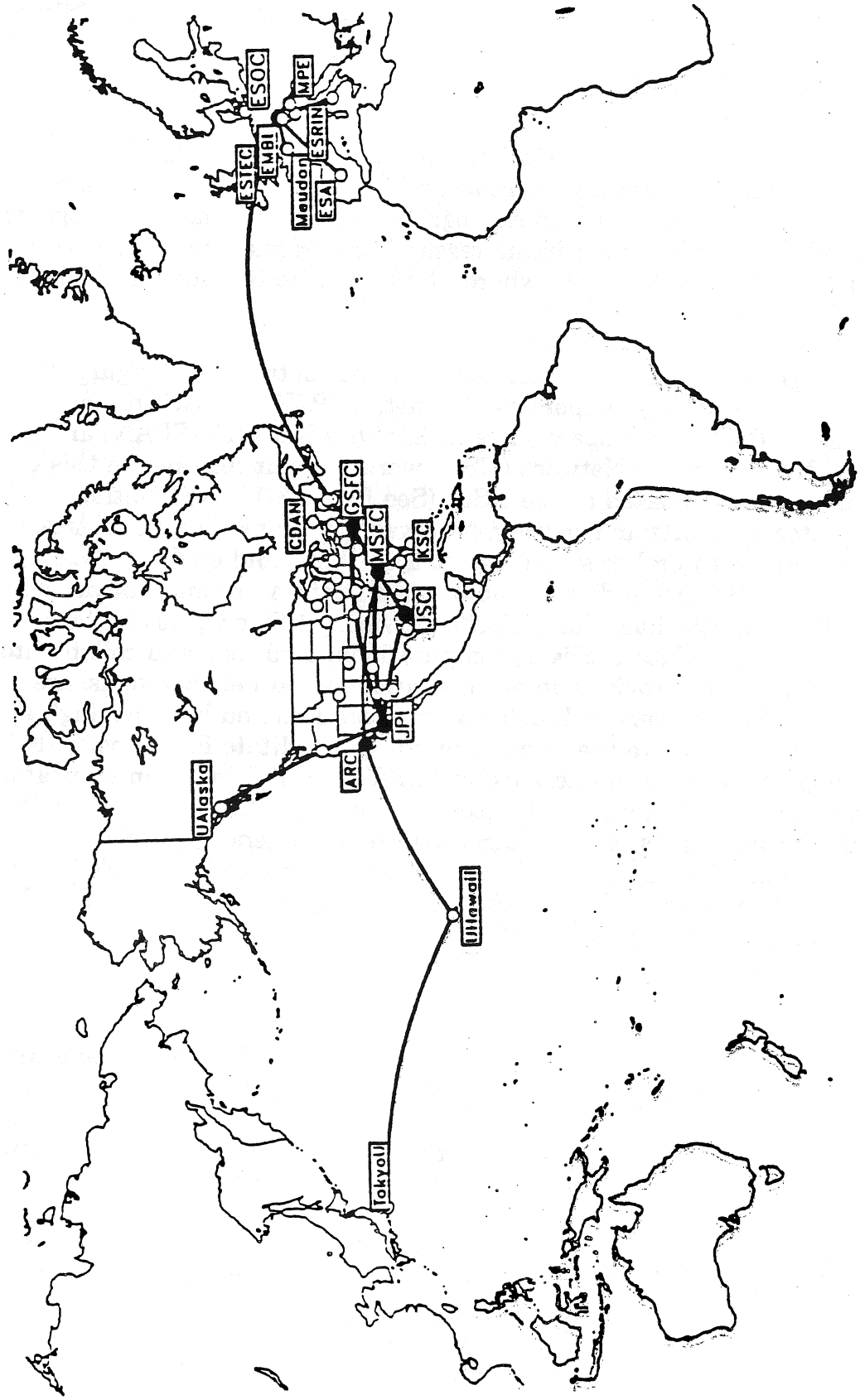


Figure 3-10. NSI International

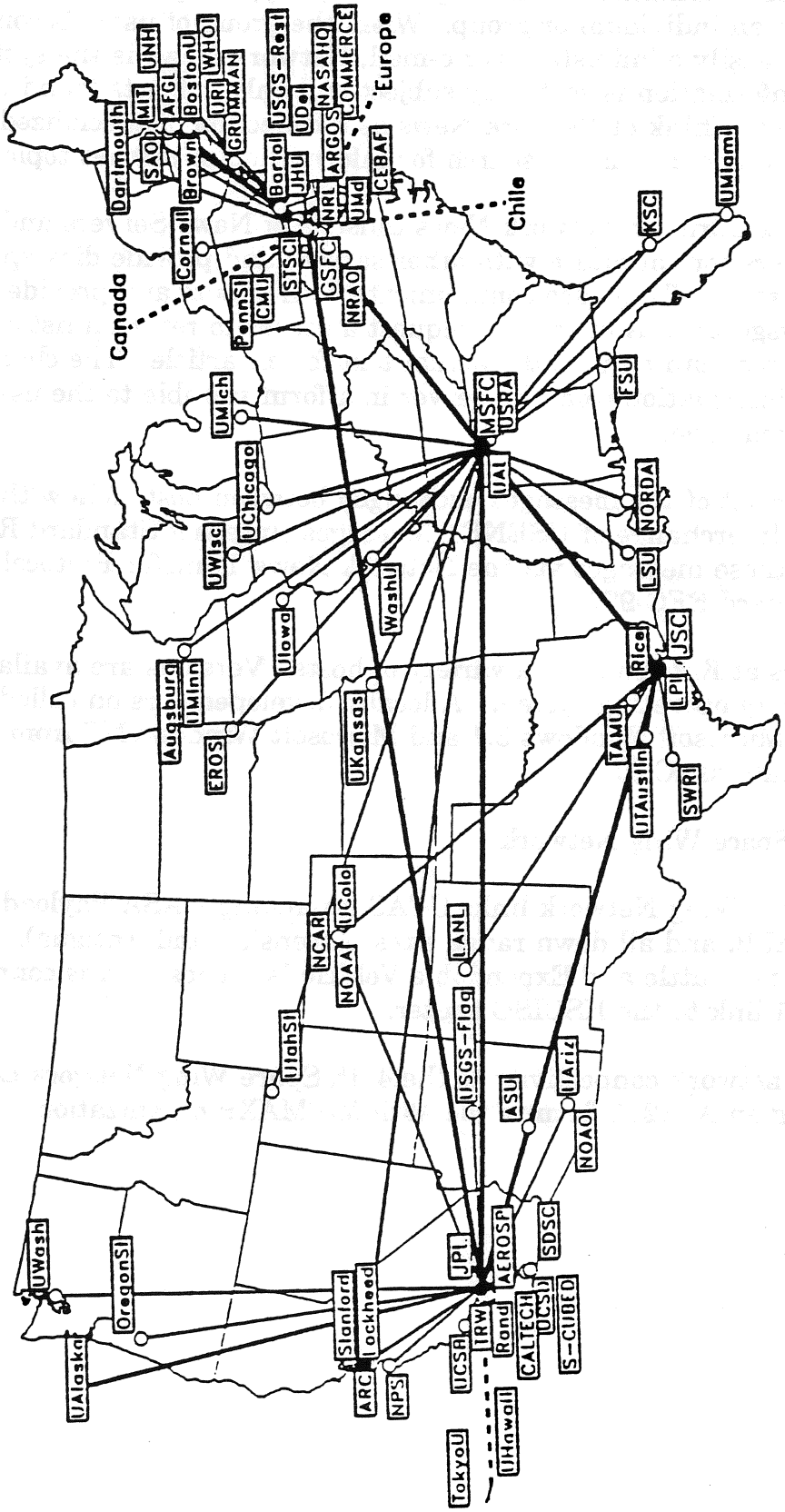


Figure 3-11. NSI National

Network News has many similarities to e-mail but differs in the way it organizes and distributes information. E-mail systems are typically used to send person-to-person mail to an individual or group. When the group of users becomes too large or dynamic to easily administer over e-mail, Network News is the system of choice. The information is sorted by subject and only subjects found interesting need to be read. Think of Network News as a collection of specialized magazines or journals that one can use to search for information or discuss topics.

The software comprising Network News consists of News Servers and News Clients. Servers communicate with other servers and provide disk space to store the actual message. They also communicate with clients and provide lists of available newsgroups. A client can request a server to return a list of articles for any newsgroup or can request the actual text for an article. The client formats and displays information from the server in a form suitable to the user interface on the client machine.

The actual format of the messages exchanged between hosts follow the Internet Standard for Interchange of USENET Messages (Internet Standard RFC-1036) and transfer these messages via the Network News Transfer Protocol (NNTP), internet Standard RFC-977.

Network news at KSC runs on a variety of hosts. Versions are available for practically every operating system. A locally developed version called WinVN is available for Microsoft Windows 3.1 and Microsoft Windows/NT from NASA Payload Operations (CM).

3.3.20 45th Space Wing Network

The 45th Space Wing Network links CCAS (excluding NASA Payload facilities on the PON), PAFB, and all down range sites (Ascension and Antigua). The network supports Space Shuttle and Expendable Vehicle launches, and is connected to KSC through a T-1 link to the KSCISO router.

Requests for network connectivity to the 45th Space Wing Network can be made by submitting an AF3215 form to the 45th MS/MAXP organization.

SECTION IV

NETWORK ORGANIZATIONS AND RESPONSIBILITIES

This section describes the NASA-KSC Directorates responsible for the KNE setup, management, operations and maintenance as spelled out in KMI 2520.4, "KSC Institutional Network Communications Development, Operations and Management." (See figure 4-1, KSC Network Management Flow.)

4.1 GENERAL RESPONSIBILITIES

KSC has three operational network organizations (CM, IM, and TM) and one network design and development organization (DE). In general, network physical connections shall be provided by one of the following operational organizations:

- TM shall provide SODN network connectivity in the Complex 39 area.
- IM shall provide KDN network connectivity in the KSC Industrial area with the exception of the payloads facilities.
- CM shall provide PON network connectivity in KSC payloads facilities and in NASA facilities located at CCAS.
- In facilities that are shared by TM, CM, and/or IM (i.e., HQS, CIF, EDL), agreements as to connection responsibility shall be established by Memorandum of Understanding (MOU) between CM, IM, and TM.

Organizations connecting to these networks are required to use networking protocols approved by the KSC Communications Steering Group (KCSG) for use at the Center. (See Section 7.1.2, Protocols.)

Approved network protocols and standards shall be recommended by a technical subgroup of the Internet Network Working Group (INWG). This subgroup consists of knowledgeable personnel from both NASA and contractor organizations within the KNE. Long term protocols to be used at KSC shall be in agreement with the Intercenter Council for Computer Networking (ICCN) recommendations.

- KSC representatives of the ICCN include:
  - D. Brown, HM-INF
  - P. Rogers, DL-CMD

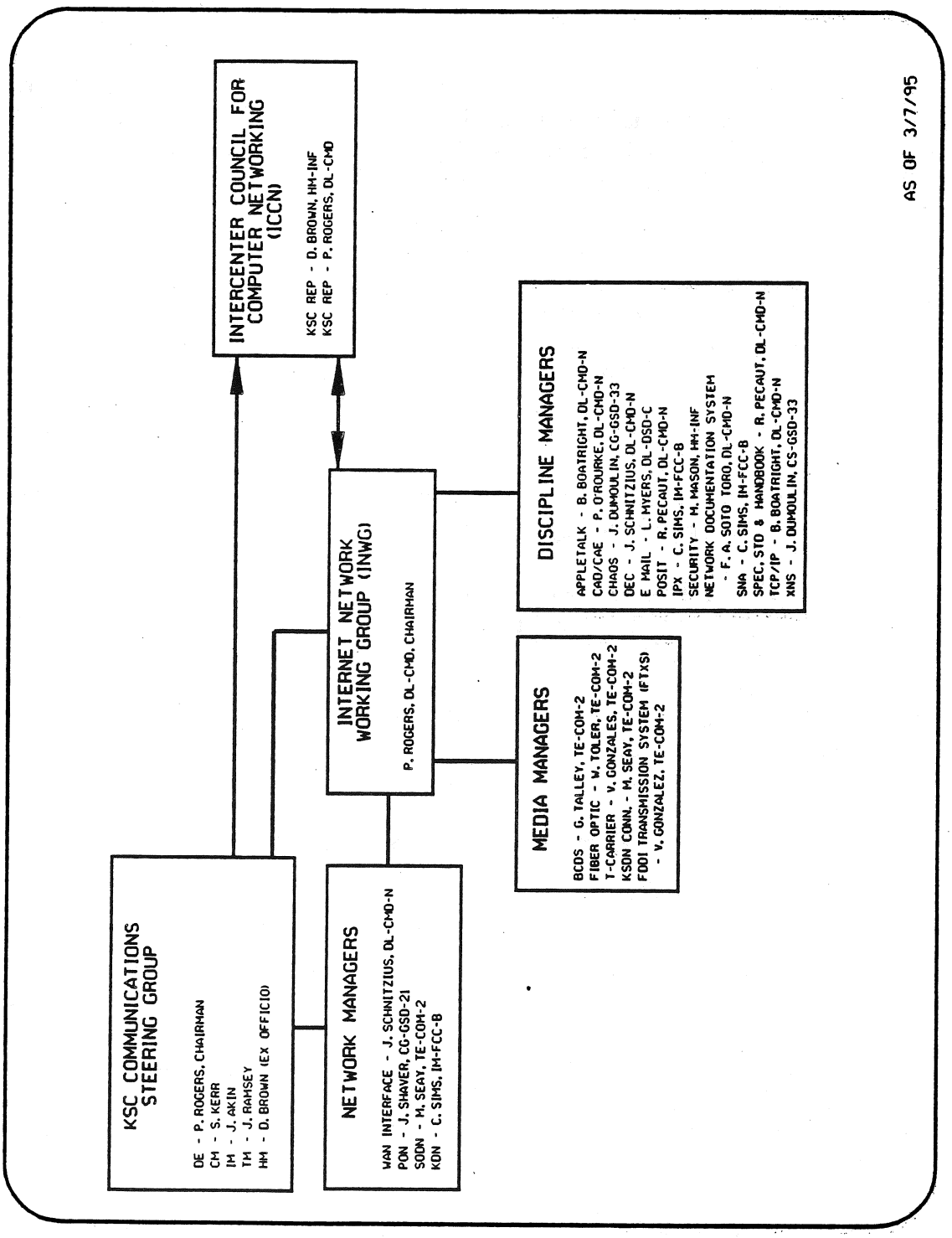


Figure 4-1. KSC Network Management Flow

The general use of metropolitan area links for server access shall be minimized until high speed wide area communications [i.e., Fiber Distributed Data Interface (FDDI)] have been implemented. Limited use would be considered on a case by case basis with the approval of the KSC Network managers. Broadband Communication Distribution System (BCDS) channel assignments in the KSC Industrial area and in Complex 39 shall be made by the KCSG. [See figure 6-1, BCDS Channel Assignments (North - LC-39 Area) and figure 6-2, BCDS Channel Assignments (South - Industrial Area).]

4.2 SPECIFIC ROLES AND RESPONSIBILITIES BY ORGANIZATION

4.2.1 Human Resources and Management Systems Office Directorate (HM)

The Human Resources and Management Systems Office, Information Management Office (HM-INF) is responsible for the Kennedy Management Instruction (KMI 2520.4) defining the networking roles and responsibilities of the CM, DE, IM, and TM Directorates.

4.2.2 Engineering Development Directorate (DE) is responsible for:

a. Managing the specifications and standards for communications systems at KSC.

b. Designing, developing, and implementing high speed communications systems at KSC with the cooperation and participation of the organization which will be responsible for the sustaining engineering, operations, and maintenance when the system is turned over for operation.

c. Representing KSC as primary development interface to the NASA Science Internet (NSI) and Program Support Communications Network Internet (PSCNI). This includes management and control of any necessary access routers until turnover to the organization responsible for operations and maintenance.

d. Developing and maintaining a KSC Network Handbook.

e. Developing and maintaining a KSC network test and evaluation capability for network technology determined by customer requirements documents.

f. Establishing a working group to develop operational policies and procedures for administration of Internet and Open System Interconnect (OSI) addresses at KSC.

g. Designing, developing and implementing a TCP/IP Domain Name Server and turn over to IM for operation, maintenance, and sustaining engineering.

h. Designing, developing and implementing KMail and future electronic mail technologies.

i. Designing, developing and implementing an FDDI transmission system at KSC.

j. Operating and maintaining a local area network (LAN) connected to a designated Industrial Area Broadband Cable Distribution System (BCDS) assigned channel for use as an R&D test bed available to all organizations at KSC.

4.2.3 Shuttle Management and Operations (TM) Directorate is responsible for:

a. Developing a Network Plan that describes the design, implementation, operation and management approach to Shuttle Operations Data Network (SODN) networking and the integrated relationship with the Payload Operations Network (PON) and the Kennedy Data Network (KDN).

b. Providing network services, as appropriate, to NASA/NASA contractor users involved in Shuttle activities who are serviced by the SODN.

c. Providing network connectivity to NASA/NASA contractor users located at Shuttle facilities in the KSC Industrial Area and the Complex 39 Area.

d. Providing Kennedy Switched Data Network (KSDN) services to all areas of KSC, including access control for any incoming external connections through KSDN.

e. Providing a Help Desk for all users of the SODN.

f. Providing operations, maintenance, and sustaining engineering for the Broadband Cable Distribution System (BCDS). The BCDS includes all passive and active broadband distribution electronics, cable, and headend equipment used in the distribution of data, video, and audio signals at KSC utilizing broadband technologies.

g. Providing operations, maintenance, and sustaining engineering for LAN equipment connected to LC-39 area BCDS, Shuttle Management assigned channels.

h. Providing operations, maintenance, and sustaining engineering for LAN equipment connected to Industrial Area BCDS, Shuttle Management assigned channels.

i. Operating and maintaining a Network Control Center to support these functions.

j. Operating, maintaining, and sustaining high-speed backbone FDDI transmission system.

4.2.4 Installation Management and Operations Directorate (IM) is responsible for:

a. Developing a Network Plan that describes the design, implementation, operation and management approach to KDN networking and the integrated relationship with the PON and SODN Networks.

b. Providing network services, as appropriate, to NASA/NASA contractor users involved in KSC activities who are serviced by the KDN.

c. Providing network connectivity to NASA/NASA contractor users located at base operations facilities in the KSC Industrial Area and the Cape Canaveral Air Station (CCAS) and Patrick Air Force Base (PAFB).

d. Providing operations, maintenance, and sustaining engineering for LAN equipment connected to Industrial Area BCDS, Center Support assigned channels.

e. Providing a Help Desk for all users of the KDN.

f. Designing, implementing, operating, maintaining and providing sustaining engineering for a Network Control Center to support these functions.

g. Providing operations, maintenance, and sustaining engineering for the primary KSC Domain Name Server.

h. Providing operations, maintenance, and sustaining engineering for the KMail service.

i. Providing operations, maintenance, and sustaining engineering for the Administrative Hub Router.

4.2.5 Payload Management and Operations (CM) Directorate is responsible for:

a. Developing a Network Plan that describes the design, implementation, operation and management approach to PON networking and the integrated relationship with the KDN and SODN Networks.

b. Providing network services, as appropriate, to NASA/NASA contractor users involved in Payload and Space Station activities who are serviced by the PON.

c. Providing network connectivity to NASA/NASA contractor users located at Payload facilities in the KSC Industrial Area and at CCAS.

d. Providing operations, maintenance, and sustaining engineering for LAN equipment connected to Industrial Area BCDS, Payload Operations assigned channels.

e. Operating and maintaining a Network Control Center to support these functions.

f. Providing a Help Desk for all users of the PON.

4.3 KSC COMMUNICATIONS STEERING GROUP (KCSG)

The KCSG is responsible for leading the development and coordination of long-range communications requirements, plans and funding. The group also reviews and assesses directorate (TM, CM and IM) network plans that describe approaches to networking and networks (KDN, PON, SODN) integration. The KCSG must also develop and issue directives which support the strategic interests of KSC as a whole.

The KSC Communications Steering Group is composed of:

- P. Rogers, DL-CMD, Chairman
- S. Kerr, CG-GSD
- J. Akin, IM-FCC
- J. Ramsey, TE-COM
- D. Brown, HM-INF (Ex Officio)

The Network Managers Group reports to the KCSG.

4.3.1 Network Managers Group

The Network Managers are responsible for implementing network communication policies and for the technical integration of KSC institutional networks. The Network Managers group is composed of the network's own system engineers and is organized as follows:

- WAN Interface - J. Schnitzius, DL-CMD-N
- PON - J. Shaver, CG-GSD-21
- SODN - M. Seay, TE-COM-2
- KDN - C. Sims, IM-FCC-B

4.3.2 Media Managers Group

Media Managers are responsible for managing the major KSC network media linking the network environments. A network medium is defined as a physical cabling system used to transmit information synchronously and asynchronously between institutional networks. The media and system engineers composing the group include:

- BCDS - G. Talley, TE-COM-2
- Fiber Optic - W. Toler, TE-COM-2
- T-Carrier - V. Gonzalez, TE-COM-2
- KSDN Connections - M. Seay, TE-COM-2
- FDDI Transmission System (FTXS) - V. Gonzalez, TE-COM-2

4.4 INTERNET NETWORK WORKING GROUP (INWG)

The Internet Network Working Group (INWG) is a technical working group consisting of the principals, Perry Rogers, chairman, and Jim Freeman, secretary. The INWG was created as a forum for discussion of various problems, solutions, and technical advances concerning the KSC network community. Participants are comprised of representatives from the major networks (KDN, PON, and SODN), design engineering, and technical and managerial areas of KSC. Any interested party at KSC is welcome to attend and participation is encouraged. The INWG meets monthly on the third Thursday, at 1300 hrs. The meeting room (HQ 3225) is generally announced the previous month, or in the monthly meeting minutes provided through distribution.

When planning a network design at KSC, it is advised to start by attending a meeting of the INWG and making a presentation of network requirements to the participants. A great deal can be learned and perhaps an avenue already exists to obtain the results you need. Information on times and location can be obtained from Jim Freeman at 867-7978.

Each month there are presentations and discussions of current issues concerning the network and systems environment at KSC. Subworking groups are assigned action items to investigate new technology, existing or potential problems, and to generate solutions to these problems. There is a monthly review and open discussion of action items.

The INWG is also tasked to distribute responsibility for protocol managers to monitor the geographical address distribution and to recommend ways and means to achieve proper distribution of networks, systems, and services within KSC.

4.4.1 Discipline Managers Group

A major subgroup to the INWG is the Discipline Managers group, composed of representatives from various protocols and systems, including:

- AppleTalk - B. Boatright, DL-CMD-N
- CAD/CAE - F. Rico-Cussi, DL-DSD-C
- CHAOS - J. Dumoulin, CG-GSD-33
- DEC - J. Schnitzius, DL-CMD-N
- KMail - L. Myers, DL-DSD-C
- POSIT - R. Pecaut, DL-CMD-N
- IPX - C. Sims, IM-FCC-B
- Security - M. Mason, HM-INF
- Specifications and Standards - R. Pecaut, DL-CMD-N
- TCP/IP - B. Boatright, DL-CMD-N
- XNS - J. Dumoulin, CG-GSD-33
- SNA - C. Sims, IM-FCC-B

4.4.2 INWG AppleTalk Protocol Working Group (APWG)

The KSC INWG APWG is comprised of representatives from each of the major AppleTalk networking organizations (KDN, PON, SODN, KSC WAN, ESC, and Rockwell) and is chaired by the DE representative, Bryan Boatright, DL-CMD-N.

This group, like the other INWG protocol working groups at KSC, serves a number of functions for the KSC networking community. The principal function of the APWG is to support:

- the NASA Intercenter Committee for Computer Networking (ICCN)
- the ICCN Appletalk Working Group
- the KSC Communications Steering Committee
- the KSC Internet Network Working Group

The AppleTalk Protocol Working Group also serves to:

- Provide a forum for addressing common KSC AppleTalk networking issues and concerns, and provide assistance to the KSC AppleTalk network service providers.

- Foster long-range planning in centerwide and agencywide AppleTalk networking technical and management solutions.

- Provide recommendations on AppleTalk networking policies and procedures to both KSC management and (through the KSC ICCN ATWG representatives and ICCN ATWG) the Intercenter Committee for Computer Networking Executive Council.

The APWG currently meets on an "as needed" basis, but will start regularly scheduled meetings in the near future. For additional information, contact Bryan Boatright at 867-7278.

4.4.3 INWG DECnet Protocol Working Group

Supporting KNE user interfaces to VAX computers for LAN's, WAN's and the NASA Science Internet (NSI), the KSC INWG DECnet Protocol Working Group (KSC INWG DPWG) consists of representatives from KSC facilities utilizing DECnet "area" equipment. DPWG plays a vital role in maintaining local area control and coordinating the configuration of the five DECnet areas at KSC because these interfaces have access to worldwide WAN links. Like other INWG protocol working groups, DPWG furnishes additional services to the networking community at KSC as well. Besides supporting INWG, it functions in an advisory capacity to such organizations as the NASA Intercenter Committee for Computer Networking (ICCN), the ICCN DECnet Working Group (ICCN DPWG), and the KSC Communications Steering Group.

Additional DPWG services include:

- Providing a platform for reviewing topics and concerns frequently encountered by KSC DECnet, and offering assistance when necessary.

- Reviewing long-range planning efforts for expanding DECnet links at KSC and proposing technical and management solutions for these expansion proposals.

- Presenting policy and procedural recommendations for DECnet networks not only to KSC management but also to the KSC ICCN Executive Council and its representatives.

Although DPWG currently meets only when required, it plans to have scheduled meetings on a regular basis very soon. To obtain more information about DPWG contact Mark Juhr at 867-3286.

4.4.4 SNA Protocol Working Group

Clark Sims, IM-FCC-B, heads this working group. SNA is a proprietary IBM protocol used by the Administrative Information Management (AIM) system. Because the AIM Amdahl computer is being moved to the Marshall Space Flight Center (MSFC), this group is currently working to establish dedicated T-1 links with channel extenders between KSC and MSFC. This will provide users the same connectivity as they would have if the Amdahl were still located at KSC.

4.4.5 TCP/IP Protocol Working Group

This group is in a state of transition. Its main purpose was to address a smooth transition to GOSIP. However, the Systems and Network Architecture Division of the National Institute of Standards and Technology (NIST) has forwarded recommendations to the Office of Management and Budget (OMB) that would rescind the mandate for government agencies to procure equipment conforming to the Government Open Systems Interconnection (OSI) Profile (GOSIP). It appears that GOSIP will be replaced by the new Profiles for Open Systems Internetworking Technologies (POSIT) which includes protocol stacks using standards issued by the Internet Engineering Task Force (IETF) which includes TCP/IP.

4.4.6 Other Protocol Working Groups

The XNS protocol has been discontinued at KSC. As a result, this working group is being disbanded.

SECTION V

INSTITUTIONAL NETWORK SECURITY POLICIES

5.1 INTRODUCTION

This section spells outs KSC policy regarding network security, including general network requirements, host responsibilities, and specific network responsibilities.

5.2 SECURITY POLICY

KSC computer security policy calls for appropriate functions and procedures to be implemented to defend KSC networks from misuse and attack. Priorities for network security are:

- to protect government resources
- to minimize disruption of service
- to support legal or administrative enforcement efforts

Automated information needs to be protected to preserve its confidentiality, integrity, and to promote availability. KMI 2410.4, "Assuring Security and Integrity of KSC Data Processing," calls for steps to protect data processing installations, systems, data, and associated telecommunications; to maintain continuity of operations; and to minimize the potential for improper use of systems and data. Lapses of computer security are to be promptly reported to appropriate officials, and systematic reporting of computer security program status is to be provided to senior management at KSC.

5.3 SCOPE OF KENNEDY NETWORK ENVIRONMENT (KNE) DATA APPLICATIONS

The KNE is intended for the support of most legitimate computer communications activities ranging from purely administrative communications, to the support of research and analysis. However, there are limits on the service that can be provided. Users and system managers need to be aware of the limits and need to consult with network service providers before using the networks.

5.3.1 Confidentiality

In general, information is broadcast over data networks. This means that any computer connected to the network can capture the data. For this reason, information that must be protected from disclosure can be transmitted over a network only when the risks are fully understood and accepted by data owners

and system managers, and appropriate controls have been instituted. Examples are "classified" national security information, Privacy Act information, and passwords.

5.3.2 Integrity and Availability

Networks are designed to reliably deliver transmitted information. However, it is possible for data to be accidentally or deliberately altered during transmission. It is also possible for network service to be interrupted by equipment or power failures, and deliberate disruption. For most KNE applications this is not a concern. However, life and mission critical applications may require a higher degree of reliability than can be provided by KNE. For this reason, "Operational" data should be placed on NASCOM rather than KNE.

5.3.3 Network User/Network Provider Dialogue

Network users and system managers are responsible for advising network managers of their requirements; i.e., their need for data confidentiality, integrity and network availability. There may be instances where a network cannot meet those requirements. Users then have the option of accepting the available service, supporting network enhancements or seeking alternative solutions to minimize risk.

Users also need to be sensitive to the fact that their reliance on, and expectations of the network may grow over time. It is not unusual for network use to begin as a productivity enhancement and become a service that is essential for the users' mission. Users must make the network manager aware of their changing needs if they expect security support to grow along with their use and dependence on the network.

5.4 Network Security Paradigm

All networks will strive to provide a high degree of transmission integrity and availability. Availability is to be provided by:

- Robust network protocols
- Network monitoring
- A strong support structure
- And, where appropriate, redundant network connections

Integrity is provided by the same first three bullets above.

A secure network depends on the cooperation of all hosts attached to the network. The smaller the network the easier it is to raise security to an acceptable level.

5.4.1 Network Responsibilities

Networks are responsible for transmission integrity; that is, delivering exactly what is sent. Networks must also maintain the availability of their service, especially for real-time, critical applications.

Although risk assessments cannot be done for networks (because it is usually not possible to determine the value of transmitted information), networks will have vulnerability assessments, covering how well and to what extent transmission integrity and availability are provided. Networks will be built or modified only after security implications have been considered and vulnerability assessments written or updated. These assessments must be made available to the connecting hosts.

Networks are also required to have emergency response plans for security incidents, especially hackers and malicious programs (e.g., "worms," "viruses").

Networks should be designed, built, operated and maintained with protection measures that are commensurate with their function and the hosts they are supporting (a host is defined as "a computer system with the ability to transmit or receive data via a network"). Architecture should be flexible enough to provide selective isolation and filtering of any node (a node is defined as "a point of connection to a network; a node may be a host or a device which joins two or more networks"). Network O&M procedures will document specific security standards and requirements.

While network managers cannot guarantee the security of their network, they can provide services which will foster a more secure environment. Rules of thumb for network managers:

- Use a firewall to limit access.
- Use a firewall to limit services to only those that are needed. Encourage services that are more easily secured. Avoid vulnerable services.
- Use a firewall to provide audit trails. Review them daily.
- Place domain name servers and e-mail servers outside the firewall. Use secure agents to retrieve information.

5.4.2 Host Responsibilities

Hosts are responsible for data confidentiality. Encryption is the most common method for protecting information from unauthorized disclosure. It requires that the sender and receiver use the same encryption algorithm and compatible keys. Once encrypted, information may be securely transmitted over any network or combination of networks.

User authentication is also a host responsibility. Common authentication schemes include passwords and challenge-response. If user authentication must be protected from disclosure during transmission, it is a host responsibility to do so.

Hosts are responsible for complying with the security requirements of the networks to which they connect. Network operations organizations may disconnect any host which does not or cannot meet its security requirements.

A good System Administrator with a priority of maintaining the security of their machines is the single best defense against unauthorized access. As the person responsible for the maintainance and operation of a computer system, the System Administrator is also responsible for its security. This person is sometimes the only user of the system, which is common for personal computers. With a network, the System Administrator's responsibilities are much more involved because of the greater complexities of the environment. Moreover, the network presents additional security risks. These risks also affect personal computers, but to a lesser degree, since they typically do not support services which can be accessed remotely via the network.

System administrators must have enough knowledge and skill to allow them to adequately secure their systems. They must understand that risks cannot be eliminated but can be reduced and managed by applying controls that prevent problems, detect problems, or facilitate recovery. Rules of thumb for good systems security:

- Keep up to date with published system vulnerabilities and their fixes.
- Disable unneeded system services.
- Minimize peer-to-peer relationships and review them constantly.
- Use TCP wrapper programs.
- Avoid logging in over a network as system administrator. Instead, log in from the console. If you must log in over the net, use one-time passwords or "smart cards".
- Use and review audit trails and system logs.
- Periodically have your system "penetration" tested.
- Plan on using digital signature technology for user and process authentication when it becomes available.

5.5 WARNING BANNER

The following banner should be displayed by any device allowing login from a network.

> This United States Government computing system is for authorized official use only. Unauthorized use or use for other than official U.S. Government business is a violation of Federal Law (18 USC). Individuals using this computing system are subject to having all of their activities on this system monitored and recorded without further notice. Auditing of users may include keystroke monitoring. Any individual who uses this system expressly consents to such monitoring and is advised that information about their use of the system may be provided to Federal law enforcement or other authorities if evidence of criminal or other unauthorized activity is found.

SECTION VI

KSC TRANSMISSION MEDIA AND STANDARDS

6.1 INTRODUCTION

This section describes various kinds of transmission systems used to link networks at Kennedy Space Center.

6.2 TRANSMISSION MEDIA

6.2.1 Broadband Communication Distribution System (BCDS)

The BCDS (see figures 6-1, 6-2, 6-3, and 6-4) provides a frequency division multiplexed radio (RF) communication network for video, audio, and two-way (synchronous) data transmissions. It provides for the distribution of composite video and provides a two-way path for data communications as a Local Area Network (LAN).

BCDS is an "Administrative" system and as such can be utilized to transport video and data traffic. BCDS is a coaxial cable distribution plant. When BCDS is freed of computer type network data, it can be better utilized for video distribution, offering more channels at more locations. Video distribution is what broadband coaxial cable plants and equipment are primarily designed for. The system is a sufficient media for transmitting to the users for television purposes. The only problem lies with the data channels where distance limitations can enable CSMA-CD timing collisions, which can result in lost or incorrect information. The OPF 1 can be served by the LC-39 BCDS using Ungerman-Bass or 3Com equipment. For SODN, 802.3 data service to OPF 3 may bottleneck if not properly managed by Data Networking Personnel.

The BCDS installed at the KSC Industrial Area, [known as Local Area Network-A (LAN-A)], provides these services to the following buildings:

- CIF
- Headquarters
- O&C
- Auditorium and Training Bldg.
- EDL
- CDSC
- LETF
- Prototype Shop

CH DES		CHANNEL	VISUAL		AURAL
		PROGRAMMING	CARRIER	NOTES	CARRIER
			(MHz)		(MHz)
G	20	NBC	157.25		161.75
H	21	CBS	163.25		167.75
I	22	ABC	169.25		173.75
7	7	KSC E. NEWS	175.25		179.75
8	8	CAPE WEATHER	181.25		185.75
9	9	C-SPAN	187.25		191.75
10	10	WEATHER CH	193.25		197.75
11	11	CNN HEADLINE	199.25		203.75
12	12	CNN	205.25		209.75
13	13		211.25		215.75
J	23	SPECIAL EVENTS	217.25		221.75
BB	38	OTV DEST 425	307.2625	NOTE 1	311.7625
CC	39	OTV DEST 426	313.2625	NOTE 1	317.7625
DD	40	OTV DEST 427	319.2625	NOTE 1	323.7625
EE	41	OTV DEST 428	325.2625	NOTE 1	329.7625
FF	42	OTV DEST 429	331.275	NOTE 2	335.775
GG	43	OTV DEST 430	337.275	NOTE 2	341.775
HH	44		343.2625	NOTE 1	347.7625
II	45		349.2625	NOTE 1	353.7625
JJ	46		355.2625	NOTE 1	359.7625
KK	47		361.2625	NOTE 1	365.7625
LL	48		367.2625	NOTE 1	371.7625
MM	49	LC-39 OTV PLAYBACK	373.2625	NOTE 1	377.7625
NN	50	SYSTEM PILOT	379.2625	NOTE 1	NONE
OO	51	LDAR	385.2625	NOTE 1	389.7625
PP	52		391.2625	NOTE 1	395.7625
QQ	53		397.2625	NOTE 1	401.7625
RR	54		403.25		407.75
SS	55		409.25		413.75
TT	56		415.25		419.75
UU	57		421.25		425.75
VV	58		427.25		431.75
WW	59	LSOC TRAINING	433.25		437.75
XX	60	NASA/EGG TRAINING	439.25		443.75
YY	61		445.25		449.75

Figure 6-1. BCDS Channel Assignments (North - LC-39 Area)

NOTE 1: OFFSET 12.5 KHz NOTE 2: OFFSET 25.0 KHz

CH DES		CHANNEL	VISUAL		AURAL
		PROGRAMMING	CARRIER	NOTES	CARRIER
			(MHz)		(MHz)
G	20	NBC	157.25		161.75
H	21	CBS	163.25		167.75
I	22	ABC	169.25		173.75
7	7	KSC E. NEWS	175.25		179.75
8	8	CAPE WEATHER	181.25		185.75
9	9	C-SPAN	187.25		191.75
10	10	WEATHER CH	193.25		197.75
11	11	CNN HEADLINE	199.25		203.75
12	12	CNN	205.25		209.75
13	13	PBS	211.25		215.75
J	23	SPECIAL EVENTS	217.25		221.75
BB	38	OTV DEST 425	307.2625	NOTE 1	311.7625
CC	39	OTV DEST 426	313.2625	NOTE 1	317.7625
DD	40	OTV DEST 427	319.2625	NOTE 1	323.7625
EE	41	OTV DEST 428	325.2625	NOTE 1	329.7625
FF	42	OTV DEST 429	331.275	NOTE 2	335.775
GG	43	OTV DEST 430	337.275	NOTE 2	341.775
HH	44	P/L DEST 372	343.2625	NOTE 1	347.7625
II	45	P/L DEST 373	349.2625	NOTE 1	353.7625
JJ	46	P/L DEST 374	355.2625	NOTE 1	359.7625
KK	47		361.2625	NOTE 1	365.7625
LL	48		367.2625	NOTE 1	371.7625
MM	49		373.2625	NOTE 1	377.7625
NN	50	SYSTEM PILOT	379.2625	NOTE 1	NONE
OO	51	LDAR	385.2625	NOTE 1	389.7625
PP	52		391.2625	NOTE 1	395.7625
QQ	53		397.2625	NOTE 1	401.7625
RR	54		403.25		407.75
SS	55		409.25		413.75
TT	56		415.25		419.75
UU	57		421.25		425.75
VV	58		427.25		431.75
WW	59	LSOC TRAINING	433.25		437.75
XX	60	NASA/EGG TRAINING	439.25		443.75
YY	61		445.25		449.75

Figure 6-2. BCDS Channel Assignments (South - Industrial Area)

NOTE 1: OFFSET 12.5 KHz **NOTE 2: OFFSET 25.0 KHz**

LC-39 AREA BCDS FREQUENCY ALLOCATION

DATA CHANNELS WITH (192.25 MHz) OFFSET

INBOUND				OUTBOUND			
CH DES	LOWER CHANNEL BOUNDARY MHz	SYSTEM	UPPER CHANNEL BOUNDARY MHz	CH DES	LOWER CHANNEL BOUNDARY MHz	SYSTEM	UPPER CHANNEL BOUNDARY MHz
. T-7	5.75		11.75	11	198		204
T-8	11.75		17.75	12	204		210
T-9	17.75		23.75	13	210		216
T-10	23.75		29.75	J	216		222
T-11	29.75	STATUS MON.	35.75	K	222	STATUS MON.	228
T-12	35.75		41.75	L	228		234
T-13	41.75	*SODN	47.75	M	234	SODN	240
T-14	47.75	*SODN	53.75	N	240	SODN	246
2'	53.75	*SODN	59.75	O	246	SODN	252
3'	59.75		65.75	P	252		258
4'	65.75		71.75	Q	258		264
4A'	71.75		77.75	R	264		270
5'	77.75	**KDN(IMT)	83.75	S	270	KDN(IMT)	276
6'	83.75		89.75	T	276		282
FM1'	89.75		95.75	U	282		288
FM2'	95.75	***SODN	101.75	V	288	SODN	294
FM3'	101.75		107.75	W	294		300
A2'	107.75	MAINT. COMM	113.75	AA	300	MAINT. COMM	306

NOTES:

* FAIRCHILD DATA REMODULATOR (18MHz)

** UNGERMANN-BASS INC. DATA REMODULATOR (6MHz)

*** 3 COM DATA REMODULATOR (6MHz)

DK/KSC-DL-3572/ LC39 AREA BCDS

Figure 6-3. LC-39 BCDS Frequency Allocations

INDUSTRICAL AREA BCDS FREQUENCY ALLOCATION

DATA CHANNELS WITH (192.25 MHz) OFFSET

INBOUND				OUTBOUND			
CH DES	LOWER CHANNEL BOUNDARY MHz	SYSTEM	UPPER CHANNEL BOUNDARY MHz	CH DES	LOWER CHANNEL BOUNDARY MHz	SYSTEM	UPPER CHANNEL BOUNDARY MHz
T-7	5.75		11.75	11	198		204
T-8	11.75		17.75	12	204		210
T-9	17.75		23.75	13	210		216
T-10	23.75		29.75	J	216		222
T-11	29.75	STATUS MON.	35.75	K	222	STATUS MON.	228
T-12	35.75	PON(MIS)	41.75	L	228	PON(MIS)	234
T-13	41.75	SODN	47.75	M	234	SODN	240
T-14	47.75	SODN	53.75	N	240	SODN	246
2'	53.75	SODN	59.75	O	246	SODN	252
3'	59.75	KDN	65.75	P	252	KDN	258
4'	65.75	KDN	71.75	Q	258	KDN	264
4A'	71.75	KDN(SS)	77.75	R	264	KDN(SS)	270
5'	77.75	KDN(IMT)	83.75	S	270	KDN(IMT)	276
6'	83.75	KDN(WAN)	89.75	T	276	KDN(WAN)	282
FM1'	89.75	KDN(CAD/CAE)	95.75	U	282	KDN(CAD/CAE)	288
FM2'	95.75	PON(REDUN.)	101.75	V	288	PON(REDUN.)	294
FM3'	101.75	PON(OPS)	107.75	W	294	PON(OPS)	300
A2'	107.75	MAINT. COMM	113.75	AA	300	MAINT. COMM	306

DK/KSC-DL-3572/INDUSTRICAL AREA BCDS

Figure 6-4. Industrial Area BCDS Frequency Allocations

- MDSS Bldg. - Gateway
- Space Station Processing Facility

The other BCDS, Local Area Network-C (LAN-C), serves these LC-39 Area buildings:

- VABR
- MFF
- OSB
- VAB
- LCC
- PCC
- OPF 1, 2, and 3

The broadband (LAN-C) system will be best utilized as is for the purpose of local, satellite television channels. The data channels should be incorporated on a fiber network for more distance and stability. No changes will be necessary for television channels only.

The headend for LAN-C is in the VABR. The BCDS is compliant with the IEEE 802.7 (Broadband) standard.

6.2.2 Multiplexed Data Transmission System, Fiber-based

As another transmission alternative for subrate data, the Grass Valley Model 87 MUX Data Multiplexer, used in conjunction with the analog wideband transmission system, can accept four DC to 128 Kb/s and four DC to 512 Kb/s data signals and modulates each onto an FM carrier in the 500 kHz to 9 mHz range. The resulting carriers are added together to produce a signal which can be transmitted over conventional 10 mHz wideband equipment. Selectable inputs allow for RS-422 or RS-423.

6.2.3 Wideband Transmission System (WBTS), Copper-based

The WBTS receives, equalizes, amplifies, and transmits baseband video, voice communications, and data signals within a frequency range of 30 Hz to 4.5 mHz. Wideband links are formed between facilities by connecting transmitter and receiver equipment through 16 gauge PEVL, 124 Ohm balanced underground cable. They are linked in tandem to provide point-to-point circuits.

6.2.4 Wideband Transmission System (WBTS), Fiber-based

As a replacement for the copper based transmission equipment, as well as new wideband circuit requirements, analog fiber optic based equipment was implemented into the Center's system. These systems, like their copper predecessors, operate in a single channel mode thus utilizing a fiber per signal. To support the transmission of RS-250-B Short Haul Studio to Transmitter Line (STL) video, the systems are required to accept a 12 mHz composite video signal.

In addition to a video signal, the equipment can handle an analog signal ranging from 10 mHz to 12 mHz, or a digital data signal from 10 bits/second to 8 Mb/s. While multi or single mode fiber can be used, the predominant configuration on the Center is LED's on multi-mode at 1300 nanometers.

6.2.5 T-Carrier Transmission System, Fiber-based

The T-Carrier transmission system is a network of T1's and fractional T1's at 29 KSC facilities and 6 CCAS facilities. It also provides T3 (45 Mbps) services between KSC (CDSC) and CCAS (XY). This system is divided into two phases.

Phase 1, which is implemented, consists of M13 multiplexers, 8T1 multiplexers, test stations, office repeaters, and data customer interface via CSU/DSU.

Phase 2 is currently being implemented to upgrade all multiplexers to full aggregate capacity, and install Synchronous Optical Network (SONET). TCXR phase 2 will also install uninterrupted power systems (UPS) at all major KSC and CCAS facilities (17 total). The TCXR system currently supports point-to-point voice and/or data transmission to signals conforming to industry standards such as DS-1, V.35, RS 449/422, or RS232-D. Once phase 2 gets finalized it will also support STS-1, OC-3, DS-3 at CDSC, SSPF, VABR, PSCN, LCC, and O&C facilities.

6.2.6 Fiber Distributed Data Interface (FDDI) Transmission System (FTXS)

The Fiber Distributed Data Interface (FDDI) Transmission System (FTXS) is the latest addition to the KSC networking environment, specifically in the area of KSC Metropolitan Area Networking Services (KMAN). This system is intended to initially supplement and eventually replace the MAN and WAN data services currently provided by the two KSC BCDS systems. This system is providing a highly reliable class of FDDI services to each of the major NASA facilities at KSC and CCAS with the capacity to expand to provide FDDI service to all facilities served by the NASA KSC fiber optic cable plant. By providing common FDDI services to the facility level, the FDDI to Ethernet and/or Token Ring interfaces supporting the facility can be optimized for the individual requirements of the

systems in the facilities (i.e., multiport routers, FDDI file servers, multimedia ethernet concentrators, FDDI-Token Ring bridges, etc.). This system is capable of delivering LAN services to a much larger geographical area than is supported by the current BCDS data channel technology due to its fiber-based (rather than copper-based) architecture. Additionally, FDDI is able to provide a significantly higher throughput than the existing BCDS data channels with a higher level of survivability.

The layout of the system is three interconnected FDDI rings, one serving each of the major campus areas at KSC/CCAS (KSC Industrial Area, LC-39 Area, and CCAS Industrial Area). (See figure 6-5, FDDI Transmission System.) Each ring is defined by a pair of large FDDI (or hub) concentrators located in the same facility as where the fiber optic cable is "starred" from in its respective campus area to minimize utilization. The area hubs are interconnected by a high performance, fully redundant FDDI-FDDI bridge to provide high throughput, high availability, and fiber-optic based backbone services to each of the major campus areas at KSC and NASA facilities at CCAS. (See the facilities list below.) Each facility with multiple FDDI requirements will contain small FDDI (or "satellite") concentrators to consolidate these FDDI connection requirements and increase the efficiency of the fiber plant utilization between the facility and the area hub. Facilities with only one FDDI interface requirement will not utilize a satellite concentrator, as no significant financial benefits will result from these installations, but will exhibit the same level of network availability as the facilities with satellite concentrators. This system is highly modular in nature, and additional facilities can be supported by adding a minimal amount of equipment in the local campus area hub and in the facility to be added.

Future plans include expansion to additional facilities at KSC, interconnection with the Air Force Eastern Space and Missile Command (ESMC) FDDI backbone (located at CCAS and PAFB) through a KSC FDDI WAN Isolation Router, a migration to/or interface with an Asynchronous Transfer Mode/Synchronous Optical Networking (ATM/SONET) based architecture and the addition of a "virtual FDDI LAN" networking capability to the system. Other possible enhancements include the activation of additional fiber optic cable paths between the area hubs (for increased system survivability), and an upgrade of the FTXS management system.

Facilities to be supported by FTXS:

<u>KSC INDUSTRIAL AREA</u>: CDSC (KSC Ind. Area Hub), CIF, HQ, O&C, SSPF, HMF, EDL, LETF

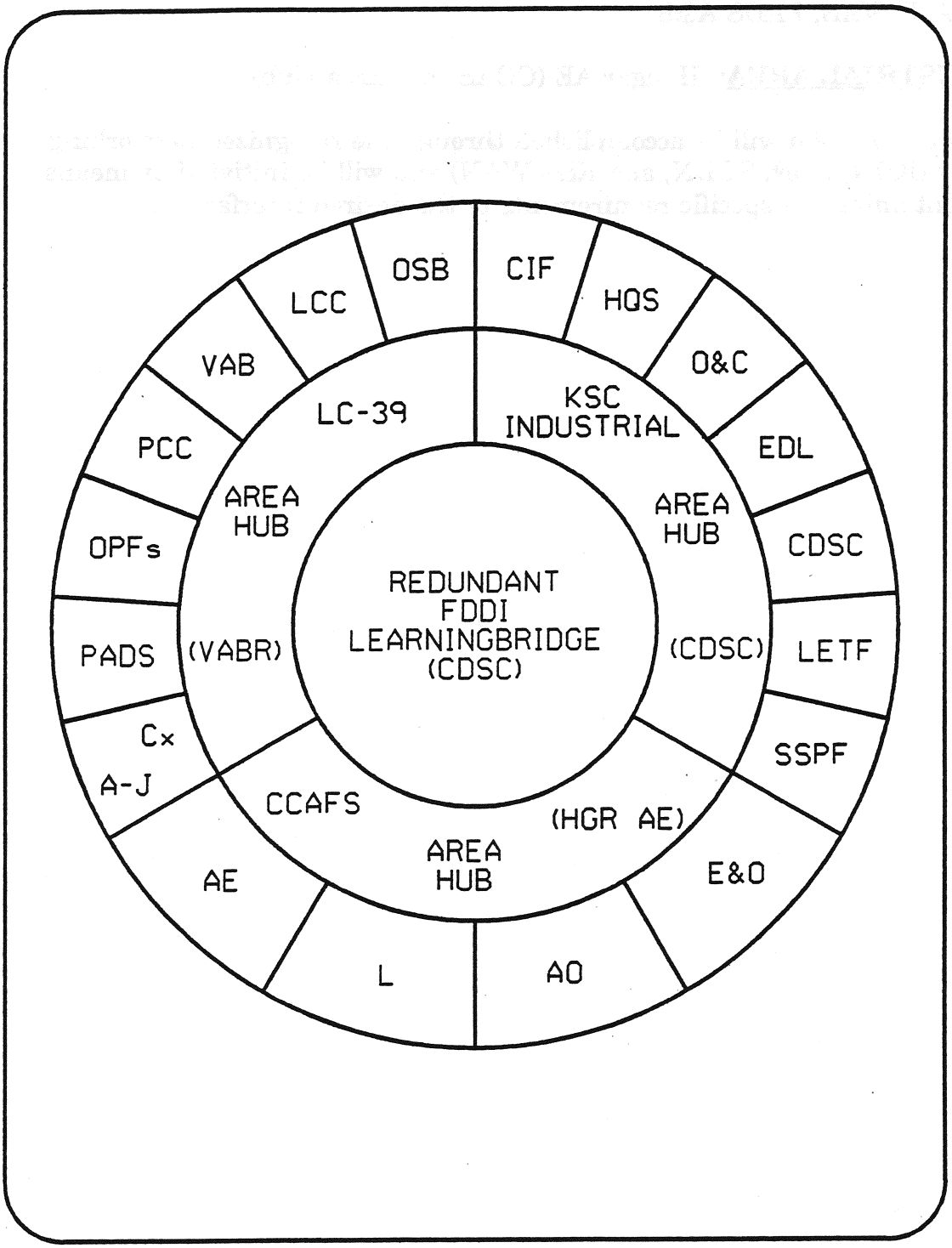


Figure 6-5. FDDI Transmission System

KSC LC-39 AREA: VABR (LC-39 Area Hub), OSB, PCC, LCC, Modular Office Complexes (A-J), VAB, PADS A&B

CCAS INDUSTRIAL AREA: Hangar AE (CCAS Ind. Area Hub)

Interfaces to this system will be accomplished through the recognized networking organizations (KDN, PON, SODN, and KSC WAN) and will be initiated by means of an ESR containing the specific requirements of the desired interface(s).

SECTION VII

NETWORK PROTOCOLS (STANDARDS)

7.1 STANDARDS AND DESIGNS

KSC Network Environment designs and implementations are based on standards which apply to the physical network and to the higher layer protocols. The KNE's physical standards follow the IEEE 802.3, 802.5, and FDDI. Protocols follow the accepted norms for the approved protocols on the KNE or as modified by the Protocol Managers. These standards may require configuration modifications for proper operation in the KNE.

7.1.1 Ethernet Cable and Layout Specifications

Consult the "Wiring and Physical Plant Guidelines, Methods and Standards Document" (published by ZATYKO Associates).

7.1.2 Protocols

Protocols approved and actively managed on the KMAN include:

- DECnet
- IP Suite
- XNS
- AppleTalk Phase II
- OSI
- Novell-IPX
- System Network Architecture (SNA)

7.2 KNE PROTOCOL DOMAINS

The KNE is a multiple protocol system. It is designed to allow unrelated protocols to coexist simultaneously on the same network without interference. Each protocol must be approved for use on the KNE and have a Protocol Manager appointed. These protocol domains are described in the following paragraphs.

7.2.1 DECnet Domain

One of the network protocols used within the KNE is DECnet, a family of software and hardware communications products implemented in accordance with Digital Network Architecture (DNA) specifications to enable computer systems to participate in a network environment. DECnet in the KNE is used by DEC VAX,

MicroVAX, and PDP machines, as well as a number of IBM mainframes, PC's, and Apple Macintosh microcomputers.

Assuming one has adequate access privileges, DECnet allows users to perform:

- interactive login to remote DECnet hosts with the "SET HOST" command
- allows files to be copied between hosts with the "COPY" command
- can perform task-to-task communications across a network (programs performing I/O operations among various hosts)
- and includes electronic mail for machines running DEC's VMS operating system.

Connections can also be made directly to X.25 networks (e.g., Telnet), to IBM SNA hosts through DEC's DECnet/SNA gateway systems and to the IBM 3081 of the NASA Space and Earth Sciences Computing Center through an Interlink gateway. All DECnet networking functions are subject to the system and file security constraints imposed by host operating systems.

7.2.2 IP Domain

The Internet Protocol (IP) domain of the KNE is mainly comprised of DOS and UNIX based systems, but also includes DEC VAX and IBM mainframes and a steadily increasing number of workstations, PC's, and Macintosh microcomputers. Developed by the U.S. Department of Defense in the late 1960's, IP is currently employed by many major global networks such as MILnet. IP is not vendor dependent. It has served as a defacto network standard for a majority of mainframe and supercomputers, and some facets of IP are incorporated in the emerging OSI network protocol. This has come about primarily through the standardization of the protocol by the Department of Defense.

Assuming one has adequate access privileges, IP allows users to:

- perform remote login to other hosts with the "TELNET" command
- execute (in many systems) procedures on remote hosts through the use of remote UNIX shells with the "RSH" command
- to move files between hosts and look at remote directories, either anonymously or with login identification, with the "FTP" command
- and allows for the exchange of electronic mail between users through the use of the Simple Mail Transfer Protocol (SMTP).

IP networking functions are subject to the security constraints imposed mainly by host operating systems.

7.2.3 XNS Domain

The Xerox Network System (XNS) protocol, developed by Xerox Corporation, is used in the KNE primarily by 3Com microcomputer local area networks and Bridge Communication devices such as bridges, routers, gateways and terminal servers. 3Com uses the XNS protocol to provide IBM PC compatibles and Macintosh computers in a local area network with resource sharing capability, both printers and disk, from a file server. 3Com's electronic mail software allows for the exchange of messages, including binary files, between IBM PC compatibles and Macintosh computers. 3Com users and resources in the KNE are easier to locate through the use of a central name server. Terminal emulation software and bridge communication servers provide access to VAX's and IBM mainframes in the KNE.

7.2.4 AppleTalk Phase II Domain

The AppleTalk protocol is widely used throughout the KSC and PSCNI networking environments. The AppleTalk Filing Protocol (AFP) provides a mechanism for accessing files across a network, and is widely supported by a large number of third-party vendors (including Novell, Microsoft, DEC, Banyan, and Farallon). A wide variety of shared network services for the end user are supported using a series of upper layer application service protocols to provide all printing, peripheral access, file sharing, mail, and directory services.

The AppleTalk protocol currently uses the RTMP (Routing Table Maintenance Protocol) to provide dynamic network route update information to the routers. Using the Phase II implementation, these updates occur at 30 second intervals but only include the information on the routes to the networks best reached by that specific gateway. This was a major improvement over the Phase I implementation, which had every gateway rebroadcasting the entire internetwork route table to every other gateway (in effect, repeating the routing information it had just learned to the gateway that provided that information).

Current migration plans for AppleTalk include the development of a more efficient Wide Area Network routing protocol that would limit routing updates to only when changes occur in the network, rather than at fixed time intervals. Additional proposed modifications to the protocol include the replacement of the Name Binding Protocol (NBP) and other network service protocols (which are optimized for the Local area rather than the Wide area) with an X.500 based Directory Services functionality to advertise and access network services (such as printers, file servers, and mail servers). This would provide for a more efficient delivery of

Local and Wide Area Network services than is possible with the existing protocol. Other work involves the redevelopment of the AppleTalk protocol stack so that it becomes transport-independent (i.e., is able to use other protocols to deliver the upper layer application services). These new implementations will be integrated into the KNE as required to best meet the identified networking requirements.

7.2.5 OSI Domain

The OSI protocol domain is new and evolving in response to the development of the Government Open System Interconnect Profile (GOSIP) by the National Institute of Standards and Technology (NIST) and the institutionalization of this profile as a Federal Information Processing System (FIPS) Standard to assure the open connectivity of government computer systems. Although the FIPS standard went into effect in August 1990, requiring all systems procured after that date to comply with the OSI protocol suite, this directive is currently being changed to reflect the findings and suggestions contained in a report by the Federal Internetworking Requirements Panel (FIRP) issued May 31, 1994. The OSI protocol is being evaluated in a testbed operated by DL-CMD-N and the ESC contractor, but the emphasis is no longer on developing a larger network based on OSI so that all existing systems at KSC migrate to that protocol. This testbed is currently being used to test an IPX to IP Gateway and will be used to test new networking products which may help KSC meet the new directive.

7.2.6 Novell - IPX

This protocol is a variation on Xerox Network Systems (XNS). One major difference between IPX and XNS is that they do not use the same Ethernet encapsulation format. A second difference is that IPX uses Novell's proprietary Service Advertisement Protocol (SAP) to advertise special network services. A file server is one instance of a service that is typically advertised.

Novell's node ID's are 48-bit quantities, represented by dotted triplets of four-digit hexadecimal numbers. A Novell router will have interfaces on more than one physical network. Physical networks are identified by 32-bit numbers written in hexadecimal.

7.2.7 System Network Architecture (SNA) Protocol

System Network Architecture (SNA) was originally released in 1974 to allow IBM customers to construct their own private networks, both hosts and subnets.

An SNA network consists of a collection of machines called nodes, of which there are four types:

- Type 1 nodes are terminals.
- Type 2 nodes are controllers, machines that supervise the behavior of terminals and other peripherals.
- Type 4 nodes are front end processors, devices whose function is to relieve the main CPU of the work and interrupt handling associated with data communications.
- Type 5 nodes are the main hosts themselves, although with the advent of low-cost microprocessors, some controllers have acquired some host-like properties. There are no type 3 nodes.

Each node contains one or more Network Addressable Units (NAU's). An NAU is a piece of software that allows a process to use the network. Each NAU has a network address. To use the network, a process must connect itself to a NAU, at which time it can be addressed and can address other NAU's.

There are three kinds of NAU's:

- Logical Unit (LU), to which user processes can be attached.
- Physical Unit (PU), a special NAU associated with each node, used by the network to bring the node online, take it offline, test it, and perform similar administrative functions.
- System Services Control Point (SSCP) of which there is usually one per type 5 node and none in the other nodes, has complete knowledge of, and control over, all the front ends, controllers, and terminals attached to the host. The collection of hardware and software managed by an SSCP is called a domain.

SECTION VIII

NETWORK SPECIFICATIONS

8.1 INTRODUCTION

The KSC network design organizations are responsible for the establishment of networks in accordance with industry standards and specifications. This section lists the standards and specifications applicable to KSC.

Standards to be discussed include:

- Open Systems Interconnection (OSI)
- Government Open System Interconnections Profile (GOSIP)
- Industry/Government Open Systems Specification (IGOSS)
- Government Network Management Profile (GNMP)

Industry Specifications include:

- Institute of Electrical and Electronic Engineers, Inc. (IEEE)
- National Fire Protection Association (NFPA)
- International Standards Organization (ISO)
- Electronic Industries Association (EIA)
- International Telecommunication Standard (CCITT)
- American National Standards Institute, Inc. (ANSI)

Reference copies are maintained by the KSC Networks Specifications, Standards and Documentation Group (call Ray Pecaut, DL-CMD-N, at 867-7278).

8.2 OPEN SYSTEMS INTERCONNECTION (OSI)

The concept of OSI (Open Systems Interconnection) was developed to enable heterogenous computer systems to interoperate in a data communication

environment. This means that users on one host can communicate with users on another host without specific knowledge of the characteristics of the other machine.

To reduce design complexity, the OSI architecture is organized as a series of layers or levels, each one built upon its predecessor. Specific communications functions are contained in each layer. The purpose of each layer is to offer certain services to the higher layers, shielding those layers from the details of how the offered services are actually implemented.

The N layer on one machine converses with the N layer on another machine. The rules and conventions used in this conversation are collectively known as the N layer protocol. The entities composing the corresponding layers on different machines are called peer processes. In other words, the peer processes at the N layer that communicate use the N layer protocol. (Figure 8-1, ISO Model GOSIP Version 1 OSI Architecture illustrates this scenario.)

Some of the principles of the OSI Reference Model [ISO 1] are:

- each layer performs a well-defined function,
- minimal information flows across layer boundaries, and
- internationally standardized protocols should be "derivable" from the functionality of each layer.

The OSI Reference Model deals with communications functionality. There are seven layers in the OSI Reference Model. These layers are referenced in the GOSIP FIPS. They include:

- Physical Layer
- Data Link Layer
- Network Layer
- Transport Layer
- Session Layer
- Presentation Layer
- Application Layer

Each layer has a protocol specification, or a set of rules governing dialogue between peer processes (processes at the same level), and a service definition, which describe an abstract interface to the next higher level. Each of the layers uses the services of the next lower layer; in turn each layer provides a service to the next higher layer. (See figure 8-2, ISO Model GOSIP Version 2 OSI Architecture.)

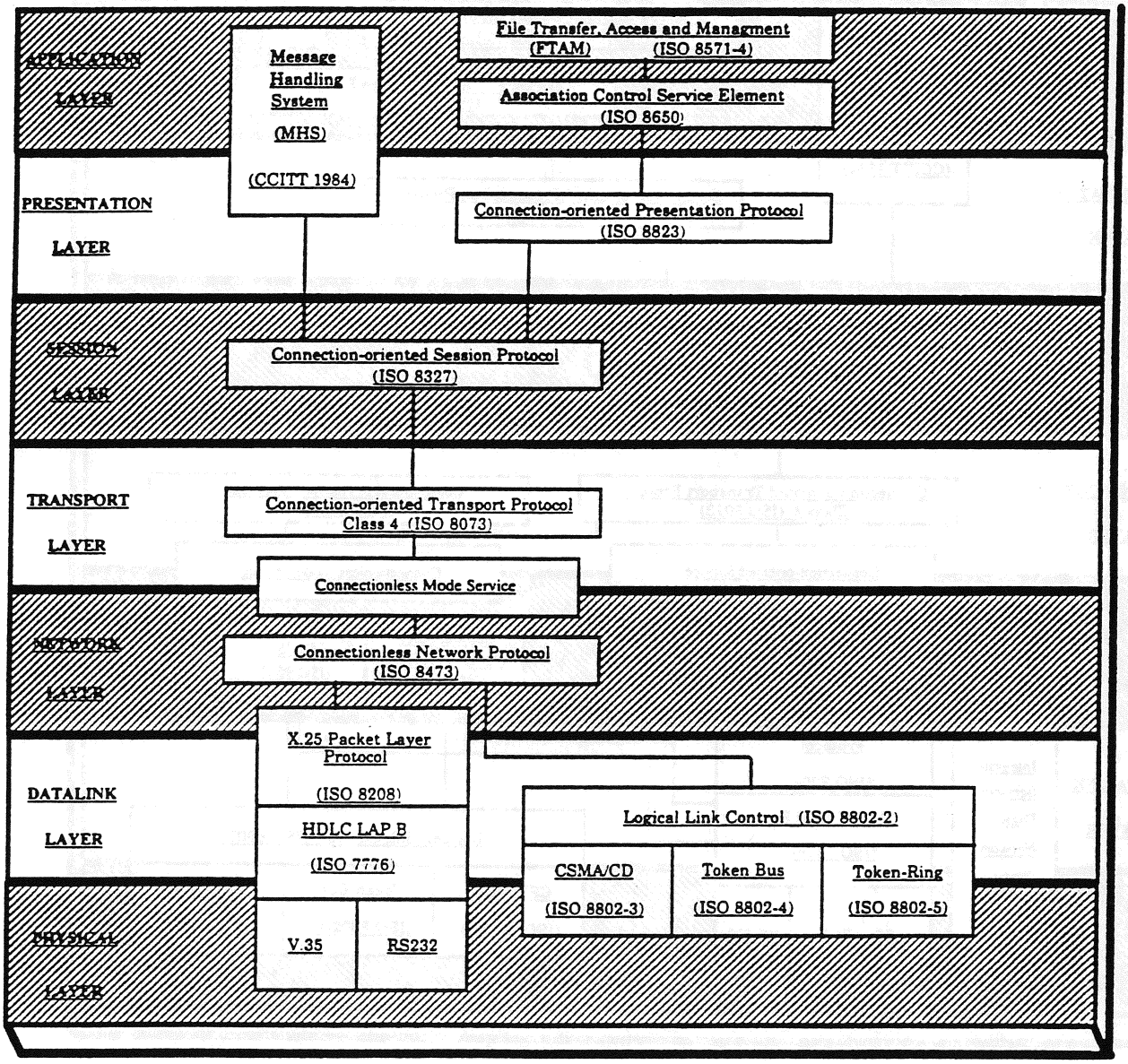


Figure 8-1. ISO Model GOSIP Version 1 OSI Architecture

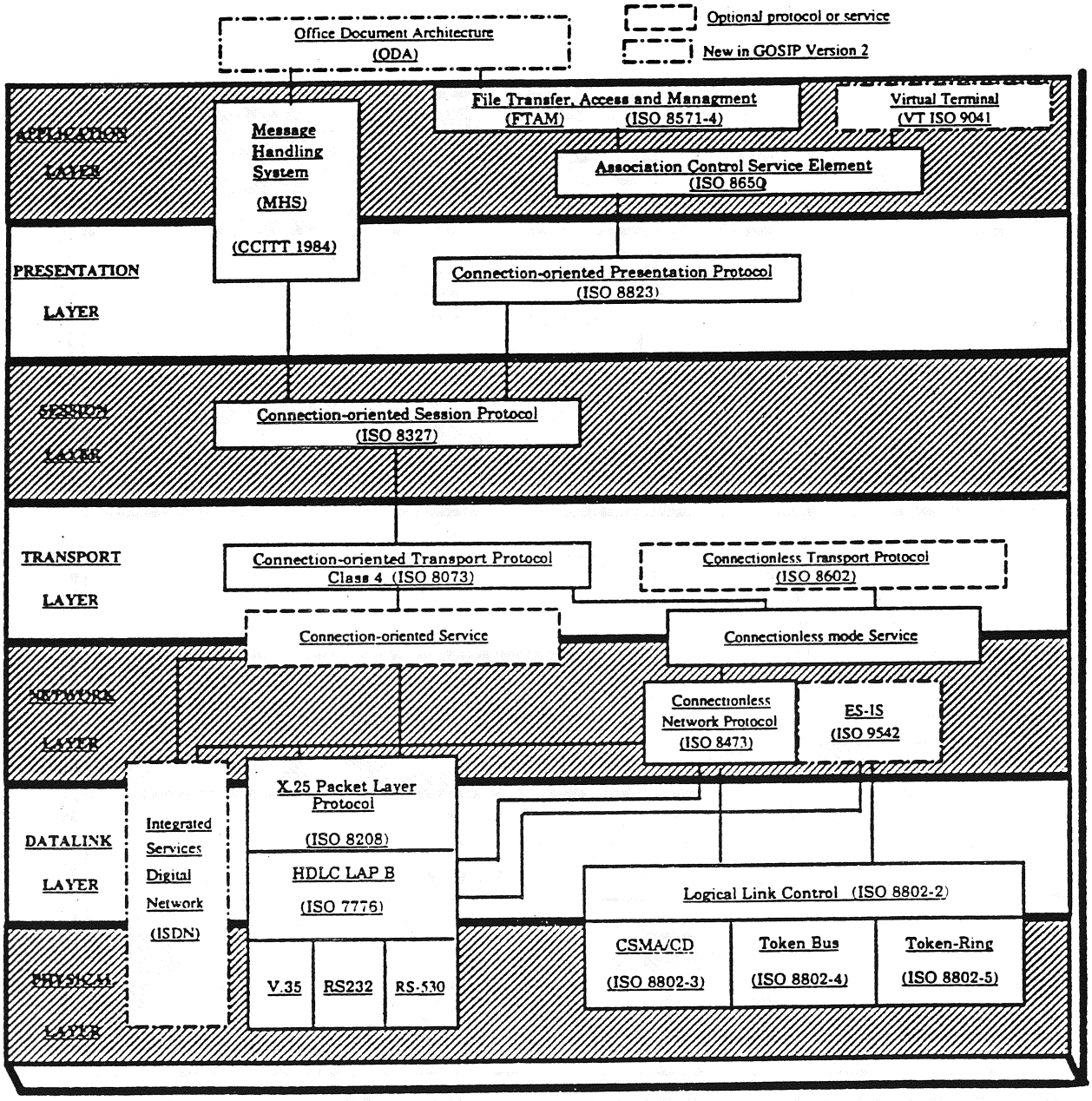


Figure 8-2. ISO Model GOSIP Version 2 OSI Architecture

Layers 1 through 3 define machine-to-machine communication via intermediate systems. Layer 4 defines end-system to end-system communication, and layers 5 through 7 address user-oriented functionality.

The interface definitions and the protocol layer definitions indicate that each layer may be modified independently of the adjacent layer, and that processes at a certain layer need not have detailed knowledge of processes occurring at other layers. Though work remains to be done, detailed standards are now in place for the entire seven layers, and the focus is on developing products based on OSI that the user can use.

Work done by implementor groups, such as the MAP/TOP group and the NIST Workshop for Implementors of OSI, serves to further define OSI in the context of specific systems and applications. Demonstration events which have taken place serve to highlight accomplishments and to provide a practical forum to illustrate the workability of OSI in a practical sense. The Enterprise Networking Event (ENE) in June 1988 was the first major OSI product exhibition.

8.2.1 OSI and Kennedy Space Center

To date the only OSI implementations within the bounds of KSC networks are those in test configurations. A major test configuration is under development within DL-CMD-N at this time, and this configuration will provide the main test bed for development of the GOSIP compliant systems to be implemented in the near future. For further information contact R. Pecaut, DL-CMD-N, 867-7278.

8.3 GOVERNMENT OPEN SYSTEM INTERCONNECTION PROFILE (GOSIP)

A major multinational thrust has been underway for the past decade to move to Open Systems Interconnection (OSI) environment through the adoption of a common set of protocols. OSI would enable networks to transition from using diverse incompatible proprietary protocols to the use of compatible nonproprietary common protocols suite.

Recognizing the growing importance and benefit of systems' interoperability, the United States Government mandated the use of selected OSI protocols in 1988 when it adopted Federal Information Processing Standard (FIPS) 146, Government Open Systems Interconnection Profile (GOSIP). The objective of GOSIP was to achieve interconnection and interoperability of computers and systems that are acquired from different manufacturers in an open systems environment. Beginning in 1990, GOSIP has been required by Federal Government Agencies when acquiring computer networking products and services and communications systems or services providing equivalent functionality. Standards are added to

GOSIP as requirements grow and products become available based on new standards. The current GOSIP Version 2 (FIPS 146-1) became effective in October 1992. The NASA response to this mandate was to initiate a proactive effort. NASA developed a policy statement outlining its endorsement of the FIPS 146 mandate and planning and achieving compliance was accomplished.

The GOSIP standards were expected to displace the Internet Protocol Suite and proprietary protocols, because they were a result of the international standards process and were expected to be implemented worldwide. For many reasons this goal to migrate to GOSIP was unrealized.

The Federal Internetworking Requirements Panel (FIRP) was established by the National Institute of Standards and Technology (NIST) in 1993 to reassess Federal requirements for open systems networks, and to recommend policy on the Government's use of networking standards. The panel was chartered to recommend actions which the Federal Government can take to address the short- and long-term issues of internetworking and convergence of networking protocols - particularly the Internet Protocol Suite (IPS) and Open Systems Interconnection (OSI) protocol suite and, when appropriate, proprietary protocols. The Panel was created at the request of the Office of Management and Budget in collaboration with the Federal Networking Council and the Federal Information Resources Management Policy Council. The Panel developed a proposal for federal internetworking whose vision described a seamless National Information Infrastructure, providing a full range of integrated communications connectivity among Federal Agencies and from Federal Agencies to the public sector. It is expected that the results of their work will be issued as Profiles for Open Systems Internetworking Technologies (POSIT) FIPS 146-2.

8.3.1 GOSIP Overview

Due to the change in emphasis outlined in 8.3, this section has been deleted and will be updated to reflect POSIT (FIPS 146-2) when it is released.

8.3.2 GOSIP at Kennedy Space Center

Currently the Intercenter Council for Computer Networking (ICCN), which was tasked to prepare the NASA GOSIP Transition Plan, is working on the NASA Open Internetworking Environment (OIE) Plan. KSC is actively involved in the development of this plan. The ICCN goal is to "improve the interoperability, security, and performance of networks, foster sharing and accessibility of information, assist the development of applications and the transfer of high performing computer technologies to others." The ultimate aim is to converge the government to a single interconnected, interoperable, standards-based

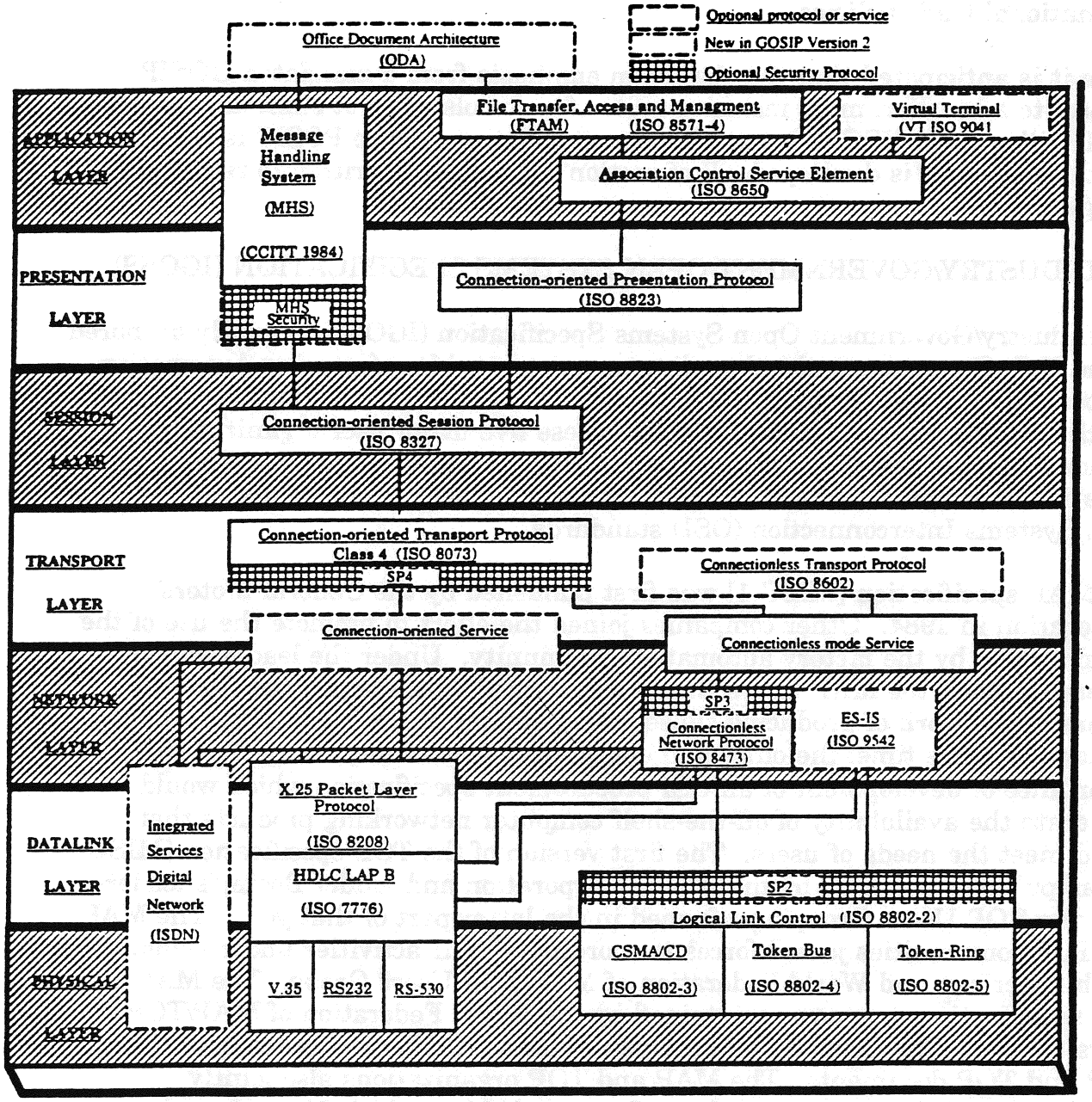


Figure 8-3. ISO Model, Framework for OSI Security

internetworking environment, to reduce the costs of computer network systems by increasing alternative sources of supply and to facilitate the use of advanced technology by the Federal Government. Federal preferred profiles should be supportive of open international voluntary standarization processes, international public sector information technology harmonization processes, and U.S. international trade policies.

While it is anticipated that the change in emphasis from a mandated GOSIP protocol to a broader, more inclusive suite of protocols will not eliminate the use of GOSIP, it's role at KSC is not at all clear at this time. Once POSIT is released and the OIE Plan is developed, all of section 8.3 will be rewritten to reflect these changes.

8.4 INDUSTRY/GOVERNMENT OPEN SYSTEMS SPECIFICATION (IGOSS)

The Industry/Government Open Systems Specification (IGOSS) is jointly authored by the U.S. Government, the Canadian government, Manufacturing Automation Protocol (MAP) User Group, the Technical and Office Protocol (TOP) User Group, and the electric power industry. Each of these five major user organizations have previously issued their own procurement files to coordinate the acquisition and operation of computer networking products and services based on the international Open Systems Interconnection (OSI) standards.

The MAP specification [MISC 1] was first published by the General Motors Corporation in 1984. Other companies joined the effort to promote the use of the OSI protocols by the factory automation community. Under the leadership of General Motors, the MAP Users Group was formed which supported General Motors in the work of producing subsequent versions of the MAP specification. Around the same time, the office and engineering community recognized the importance of development of an OSI procurement specification which would accelerate the availability of off-the-shelf computer networking products that would meet the needs of users. The first version of the TOP specification [MISC 2] was published in 1985 by the Boeing Corporation and, under Boeing's leadership, the TOP Users Group was formed in the latter part of that year. The MAP and TOP communities joined forces to coordinate their activities under common North American and World Federation of MAP/TOP Users Group. The MAP and TOP specifications are now maintained by the World Federation of MAP/TOP Users Groups. The Corporation for Open Systems (COS) distributes both the MAP and TOP documents. The MAP and TOP organizations also jointly organized the Enterprise Networking Event in 1988 at which 52 vendors demonstrated that OSI products can be used to solve real business problems.

In late 1986, the National Bureau of Standards (NBS), now the National Institute of Standards and Technology (NIST) initiated development of the Government Open Systems Interconnection Profile (GOSIP). A Federal interagency group of experts was formed, and evolved into the GOSIP Advanced Requirements Group, that now has the responsibility for promulgating each new version of GOSIP. The NIST chairs this group and has editing responsibility for the document. At the time the first draft of GOSIP was written, the MAP and TOP specifications were nearing stability, vendor OSI implementations were being successfully demonstrated, and commercial OSI products were just entering the marketplace.

The intent of GOSIP is to transmit Federal user requirements to vendors and to encourage vendors to build OSI products satisfying those requirements. The GOSIP, unlike the MAP and TOP documents, is a mandate. GOSIP mandates that Federal agencies acquire OSI products when acquiring the services provided by the OSI protocols referenced in the document. Since the GOSIP must be referenced in Federal procurement requests, where applicable, GOSIP contains only those OSI protocols which are expected to be implemented in vendor products. The MAP and TOP documents included some specifications of OSI protocols which those communities wanted the vendors to implement in the future. Accordingly, although informal coordination has existed between the MAP/TOP and Federal communities, the protocols in GOSIP have tended to be a subset of the protocols in the union of the MAP and TOP documents.

In order to promote interoperability among computer systems supplied to the electric power industry, the Electric Power Research Institute (EPRI) initiated the Utility Communications Architecture (UCA) project. The first phase of the project identified the information requirements within an electric utility. Subsequent phases identified appropriate standards for inclusion in Version 1 of the UCA specification. The UCA document, like the MAP and TOP documents, is a specification of user requirements. Twenty utility companies participated in the review of the draft document, which was then formally released to the vendor community.

EPRI continues to have the responsibility for maintaining the UCA specification. OSI protocols are the foundation on which Version 1 of the UCA specification is based. The UCA authors were knowledgeable of the MAP, TOP, and GOSIP documents and recognized the importance of aligning specifications so that vendors would not be forced to build a different set of products for each new user community.

In April 1987, the Canadian federal government announced a new policy on OSI. This policy, which applies to all Canadian government departments, endorses OSI as an Information Technology (IT) strategy in preference to any manufacturer-specific or installation-specific architecture, and requires that departments and

agencies state a clear preference for OSI-based products and services in their procurements. In order to assist users to migrate to OSI, work began in 1987 to develop the Canadian Open Systems Application Criteria (COSAC). This work is led and coordinated by the Treasury Board Secretariat (TBS) which is responsible for Canadian government IT standards and policy. COSAC comprises endorsements of the OSI based standards, OSI functional profiles, and guidance documents, all of which are published as Treasury Board Information Technology Standards. In producing COSAC, maximum alignment with other government and international specifications has also been an objective. Thus, cooperation between the five user communities to produce the IGOSS is just a formal extension to what has existed informally for some time.

8.5 GOVERNMENT NETWORK MANAGEMENT PROFILE (GNMP)

Business and governments continue deployment of voice and data communication networks at an increasing pace. The deployment of these networking devices is generating intense pressure for suppliers to provide network management products as well. Suppliers are responding with capable, but incompatible, network managers. The result in most large organizations today is a loose confederation of multi-vendor systems managed by a variety of network management products. The situation in a typical company is illustrated in figure 9-4, Network Management in a Non-Integrated Manner. In the example, five different terminals are required to manage all the network assets, and nowhere is an integrated view available.

The solution of this dilemma depends upon an integrated network management system. For the company illustrated in figure 8-4, a solution such as that shown in figure 8-5, Network Management in an Integrated Manner, might be feasible. All five network managers (the two LAN managers, the WAN manager, the telecommunications manager, and the PBX manager) remain in place, using proprietary means to manage specific resources. Four network management integrators have been added: one integrates the LAN managers, one integrates the telecommunications managers, one integrates the WAN manager and the LAN integrator, and one integrates the telecommunications and data communications integrators. Implementation of such a hierarchical network management system requires a standard for network management information exchange between integrators, and between integrators and managers. In figure 8-5, interfaces requiring such a standard are shown with broken lines connecting the label "GNMP."

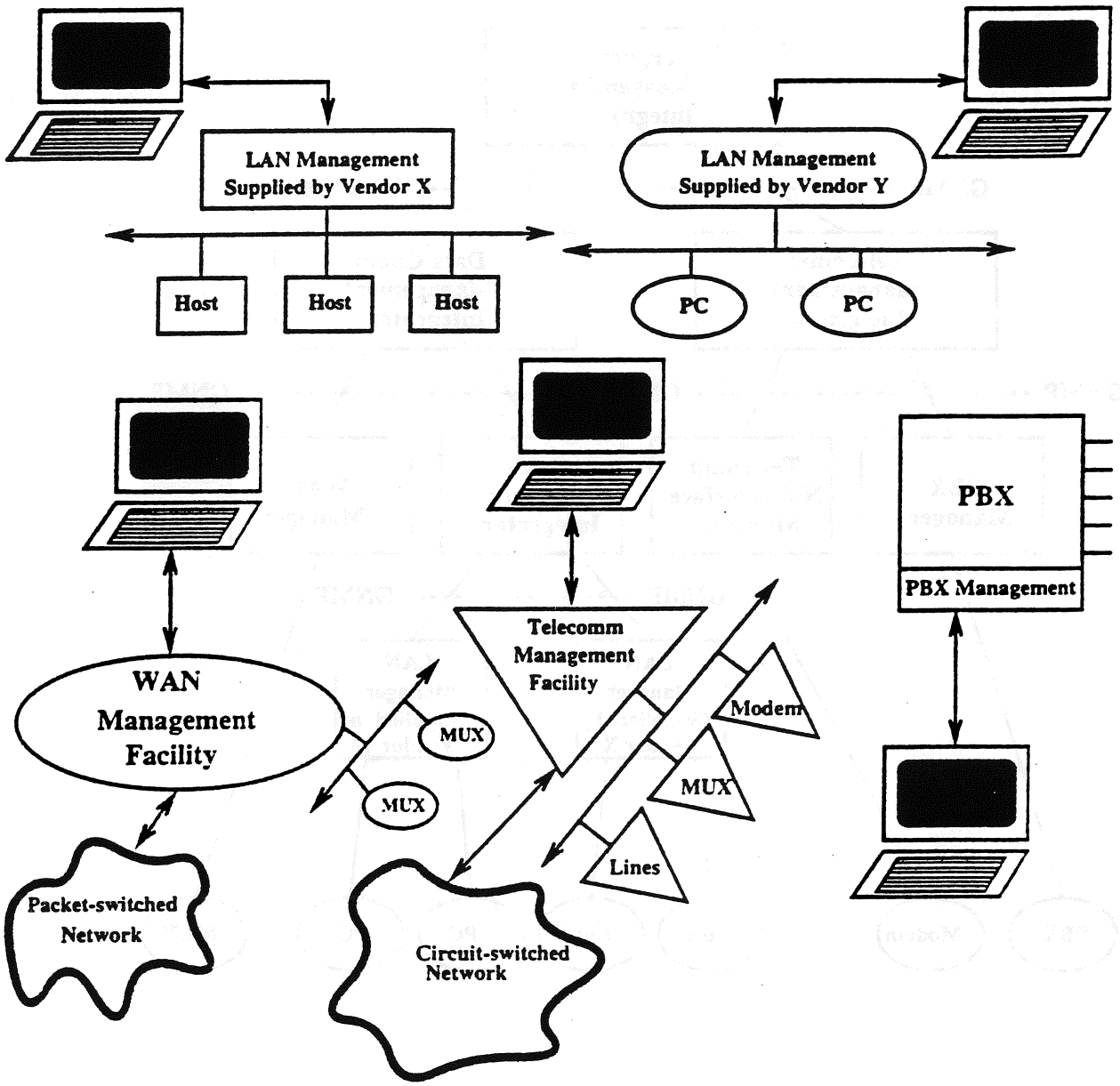


Figure 8-4. Network Management in a Non-Integrated Manner

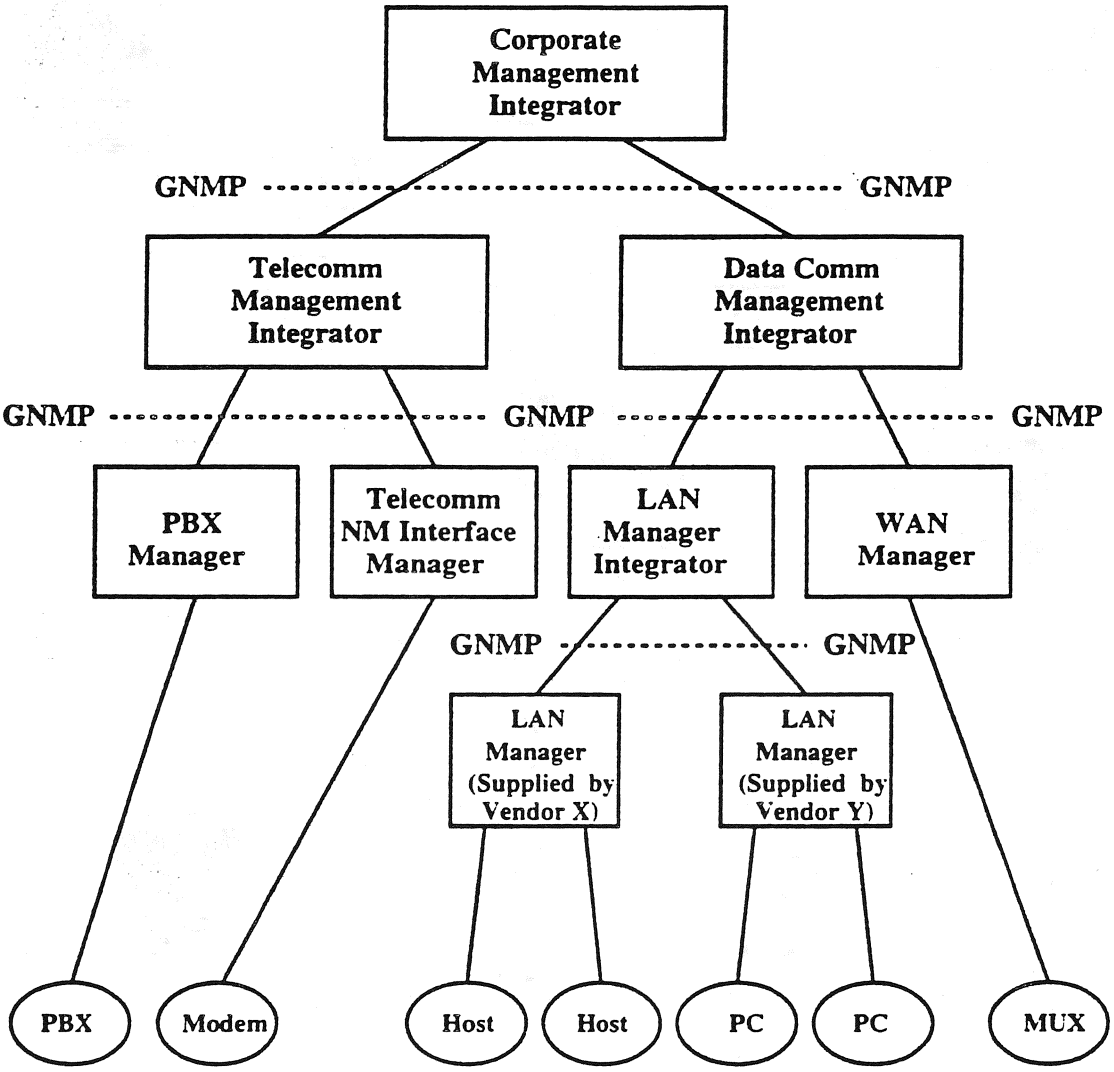


Figure 8-5. Integrated Network Management Using GNMP

The Government Network Management Profile (GNMP) specifies a standard for the exchange of management information between integrators and between integrators and managers. The GNMP specification can also be used between managers and network elements, should the network elements possess sufficient computing capability. The scope of the GNMP encompasses a set of protocols for multi-vendor communications, a set of general-purpose management functions, and a standard set of managed object definitions. This scope addresses only the exchange of management information in a standard way in order to achieve integration of management systems and components made independently by a variety of suppliers.

Other important issues are outside the scope of the GNMP. Consider, for example, the analysis of management information. For any operational network management system, raw management data must be collected, stored, calculated, and correlated to provide useful outputs for network planning, fault prediction, and billing. Requirements in these areas are outside the scope of the GNMP and must continue to be specified directly by the Acquisition Authority.

Human-Machine Interface (HMI) is also outside the scope of the GNMP. The Acquisition Authority must continue to specify any requirements regarding presentation and ease of use. The usual issues of configuration and sizing of network management components are also outside the scope of the GNMP. The Acquisition Authority must continue to plan the deployment and sizing of specific integrators and managers in accordance with operational requirements. The GNMP, then, addresses a single, significant network management integration problem: interoperability between network management components.

8.6 SPECIFICATIONS AND STANDARDS LIST

8.6.1 Institute of Electrical and Electronic Engineers, Inc. (IEEE)

IEEE Std. 802.1a	Overview of Local Area Networks (LAN's) and Metropolitan Area Networks (MAN's) Specifications
IEEE Std. 802.1d	Local Area Networks (LAN's) MAC Transparent Bridging Standards
IEEE Std. 802.3	System Considerations for Multi-Segment Type 10BASE-T 10 Mb/s Baseband Networks (Section 13) and Medium Attachment Unit and Baseband Medium Specification, Type 10BASE-T (Section 14)

IEEE Std. 802.3a	Medium Attachment Unit and Baseband 1988 Medium Specifications, Type 10BASE2 (Section 10)
IEEE Std. 802.3c	Repeater Unit for 10 Mb/s Baseband 1988 Networks (Section 9)
IEEE Std. 802.4	Standard for Local Area Network Token Bus Access Method, Physical Layer Specification
IEEE Std. 802.5	Token Ring access method and physical layer specifications
IEEE Std. 802.7	Recommended Practices for Broadband Local Area Network
Version 2, The Ethernet	A Local Area Network: Data Link Layer and Physical Layer Specification, DEC Intel and Xerox Corporations, Version 2.0, November 1982.

8.6.2 National Fire Protection Association (NFPA)

NFPA No. 70	National Electric Code

8.6.3 International Standards Organization (ISO)

ISO 8877[12]	Information Processing System - Interface Connectors and Contract Assignments for ISDN, Basic Access Interface Located at Reference Point S and T
ISO DIS10589	Intermediate System to Intermediate System (IS-IS)
ISO IS9542	End System to Intermediate System (ES-IS)
ISO IS843	Connectionless Networking Protocol (CLNP)
ISO 2593	Data Communication 34 Pin DTE/DCE Interface Connector and Pin Assignments

8.6.4 Electronic Industries Association (EIA)

RS-232-E	Interface Between Data Terminal Equipment and Data Communications Equipment Employing Serial Binary Data Interchange
RS-310-B	Panels and Associated Equipment
RS-449/530	General Purpose 37-Position and 9-Position Interface for Data Terminal Equipment and Data Circuit Terminating Equipment and Employing Serial Binary Data Interchange
RS-422-A	Electrical Characteristics of Balanced Voltage Digital Interface Circuits
EIA/TIA-568, 569	Commercial Building Telecommunications Wiring Standard

8.6.5 Consultative Committee for International Telephone and Telegraph (CCITT)

V.35	Data Transmission at 48 kbps using 60-108k Hz group band.

8.6.6 American National Standards Institute, Inc. (ANSI)

X3.139	FDDI Token Ring Media Access Control Standard
X3.148	FDDI Token Ring Physical Layer Protocol Standard
X3.166	FDDI Token Ring Physical Layer Medium Dependant Standard
X3T9.5	FDDI Station Management (REV 6.2)

(Application for copies may be obtained from the American National Standards Institute, 1430 Broadway, New York, New York 10018.)

8.7 INTERNET ENGINEERING TASK FORCE (IETF) REQUESTS FOR COMMENTS (RFC'S)

RFC's are a set of public documents that define the internet. At KSC, an RFC Library is maintained by the DE Networks Section, DL-CMD-N, Networks Specifications, Standards and Documentation Group. These documents are available via FTP. Contact the group for transfer information. All KSC these RFC's are available via anonymous FTP to titan.ksc.nasa.gov and are crossreferenced, indexed, and keyword searchable.

APPENDIX A: ACRONYMS AND ABBREVIATIONS

A&DC	Administrative and Data Communications
ADP	Automatic Data Processing
AFP	AppleTalk Filing Protocol
AIM	Administrative Information Management
ANSI	American National Standards Institute
APP II	AppleTalk Phase II
BCDS	Broadband Communication Distribution System
BCSS	Boeing Computer Support Services
BOB	Base Operations Building
BOC	Base Operations Contractor
BWOTN	Bionetics Work Order Tracking Network
CAD	Computer Aided Drafting
CAE	Computer Aided Engineering
CCAS	Cape Canaveral Air Station
CCITT	Consultative Committee for International Telephone and Telegraph
CCMS	Checkout, Control and Monitoring Subsystem
CDS	Central Data Subsystem
CDSC	Communications Distribution and Switching Center
CIF	Central Instrumentation Facility
CM	Payload Management and Operations Directorate
COS	Corporation for Open Systems
COSAC	Canadian Open Systems Application Criteria
CPU	Central Processing Unit
DAS	Dual Attach Station
DE	Engineering Development Directorate
DECnet	Digital Equipment Corporation Network
DNA	Digital Network Architecture
DNS	Domain Name Server
DOD	Department of Defense
DTE	Data Terminal Equipment
EDI	Electronic Data Interchange
EDL	Engineering Development Laboratory
EMIG	Electronic Mail Implementors Group
ENE	Enterprise Networking Event
EPRI	Electric Power Research Institute
ESC	Engineering Support Contract
ES/IS	End System to Intermediate System
FDDI	Fiber Distributed Data Interface
FIPS	Federal Information Processing System
FOIRL	Fiber Optic Inter Repeater Link

FRR	Flight Readiness Review
FTP	File Transfer Protocol
FTXS	FDDI Transmission System
FY	Fiscal Year
GNMP	Government Network Management Profile
GOSIP	Government Open Systems Interconnection Profile
GSE	Government Support Equipment
GSFC	Goddard Space Flight Center (Greenbelt, MD)
GUI	Graphical User Interface
HM	Human Resources Management Systems Office Directorate
HMI	Human-Machine Interface
HQS	Headquarters
Hz	Hertz
IBM	International Business Machine
ICCN	Intercenter Council for Computer Networking
ICD	Interface Control Document
IECS	Integrated Engineering Computer System
IEEE	Institute of Electrical and Electronic Engineers
IETF	Internet Engineering Task Force
IGOSS	Industry/Government Open Systems Specification
IGRP	Interior Gateway Router Protocol
IM	Installation Management and Operations Directorate
INWG	Internet Network Working Group
IOS	Integrated Operations System
IP	Internet Protocol
IPS	Information Processing System
IPX	Internet Packet Exchange
IS/IS	Intermediate System to Intermediate System
ISO	International Standards Organization
IT	Information Technology
ITU	International Telecommunications Union
JSC	Lyndon B. Johnson Space Center (Houston, TX)
kbps	Kilobits per second
KCSG	KSC Communications Steering Group
KDN	Kennedy Data Network
kHz	Kilohertz
KIMS	Kennedy Inventory Management System
KIN	Kennedy Institutional Network
KMI	Kennedy Space Center Management Instruction
KMAN	KSC Metropolitan Area Network
KNE	KSC Network Environment
KSC	John F. Kennedy Space Center
KSDN	Kennedy Switched Data Network
KSDNBN	KSDN Bridged Network

KWAN	KSC Wide Area Network
LAN	Local Area Network
LAT	Local Area Transport
LAVC	Local Area VAX Cluster
LC-39	Launch Complex 39
LCC	Launch Control Center
LDAR	Lightning Detection and Radar
LED	Light Emitting Diode
LETF	Launch Equipment Test Facility
LLC	Logical Link Control
LON	LPS Operational Network
LPS	Launch Processing System
LSDN	LPS Software Development Network
LSOC	Lockheed Space Operations Company
LU	Logical Unit
MAC	Media Access Control
MAI	Metropolitan Area Interface
MAP	Manufacturing Automation Protocol
mbps	Megabits per second
MDS-F	Multiplex Data System - Fiber
MDTS	Multiplexed Data Transmission System
mHz	Megahertz
MMPSE	Multiple Mission Payload Support Equipment
MOA	Memorandum of Agreement
ms	Millisecond
MSFC	Marshall Space Flight Center
N&A	Naming and Addressing
NASA	National Aeronautics and Space Administration
NASANet	NASA Network
NASCOM	NASA Communications (Network)
NAU	Network Addressable Unit
NBP	Name Binding Protocol
NBS	National Bureau of Standards
NCC	Network Control Center
NCP	Network Control Processor
NDIS	Network Device Interface Specification
NDS	Network Documentation System
NetBIOS	Network Basic Input/Output System
NetBEUI	NetBIOS Extended User Interface
NFPA	National Fire Protection Association
NFS	Network File System
NHB	NASA Handbook
NIC	Network Interface Card
NICOLAS	Network Information Center On Line System

NIST	National Institute of Standards and Technology
NMI	NASA Management Instruction
NMTAG	Network Managers Technical Advisors Group
NSC	Network Steering Committee
NSI	NASA Science Internet
O&C	Operations and Checkout Building
O/E	Optical to Electrical
OAS	Office Automation System
OIS	Operational Intercommunication System
OMB	Office of Management and Budget
OPF	Orbiter Processing Facility
OSB	Operations Support Building
OSI	Open Systems Interconnection
OTV	Operational Television
PAWS	Paging Area Warning System
PCC	Processing Control Center
PDMS	Payload Data Management System
PEM	Privacy Enhanced Mail
PGOC	Payload Ground Operations Contractor
PMS	Permanent Measurements System
POCS	Photo Optic Control System
PON	Payload Operations Network
POSIT	Profiles for Open Systems Internetworking Technologies
ppm	Pulses per minute
pps	Pulses per second
PSB	Payload Support Building
PSCN	Program Support Communications Network
PSCNI	PSCN Internet
PSTF-R	Payload Span Test Facilities - Replacement
PU	Physical Unit
RDBMS	Relational Data Base Management System
RFC	Requests for Comments
RIP	Routing Information Protocol
RPC	Remote Procedure Call
RTMP	Routing Table Maintenance Protocol
SACS	Security Access Control System
SAS	Single Attach Station
SCAN	Shuttle Connector Analysis Network
SDLC	Synchronous Data Link Control
SDS	Shuttle Drawing System
SMTP	Simple Mail Transfer Protocol
SNA	System Network Architecture
SNMP	Simple Network Management Protocol
SODN	Shuttle Operations Data Network

SONET	Synchronous Optical Network
SPAN	Space Physics Analysis Network
SPC	Shuttle Processing Contractor
SPDMS	Shuttle Processing Data Management System
SPX	Sequential Packet Exchange
SQL	Structured Query Language
SSCP	System Services Control Point
SSPF	Space Station Processing Facility
SSPN	Space Shuttle Program Network
SSPO	Space Shuttle Program Office
STL	Studio to Transmitter Line
TBS	Treasury Board Secretariat
T&CD	Timing and Countdown
TCP	Transport Control Protocol
TCTS	T-Carrier Transmission System
TCXR	T-Carrier Transmission
TLC	Technical Learning Center
TM	Directorate of Shuttle Management and Operations
TMIS	Technical and Management Information System
TOP	Technical and Office Protocol
UCA	Utility Communications Architecture
UPS	Uninterruptible Power Supply
UUCP	UNIX-to-UNIX Copy
VAB	Vehicle Assembly Building
VABR	VAB Repeater
VMS	Virtual Memory System
WAD	Work Authorization Document
WAI	Wide Area Interface
WAN	Wide Area Network
WBTS	Wideband Transmission System
WWW	World Wide Web
XNS	Xerox Network System

APPENDIX B: DEFINITIONS

Backbone: The medium that connects major facilities at KSC. The Broadband Communications Distribution System is a backbone.

Bridge: A device that connects two LAN's, at the media access control (MAC) sublayer of the data link layer, and isolates traffic between the different segments of the networks by examining the destination addresses of the frames placed on the network by individual devices.

Discipline Manager: Individuals responsible for a communication protocol, E-mail system, GOSIP compliance, specification/standards and the KSC Network Handbook. These persons (see Section 5.4.1) are responsible for the Technical Administration of their specific discipline. See Figure 5-1. Specific task of communication protocol discipline manager is to oversee successful migration to OSI.

Dual Connected (Homed): In a dual-ring local area network, a connection both to the primary, active ring and to a secondary ring that provides redundancy in case of cable or system failure.

Ethernet: A baseband LAN technology originally developed by the Xerox Corp. and now widely accepted and supported by most LAN manufacturers. Technically speaking, Ethernet is different from the later developed IEEE 802.3 standard now used for specifying LAN's; nevertheless, the term Ethernet is still most frequently used to refer to such LAN's.

External Interface: A device that connects the network to a private LAN or a wide area network (WAN) external to the network, and performs router, bridge or gateway functions.

Fiber Distributed Data Interface (FDDI): A standard for fiber optic data transmission systems being developed by the American National Standards Institute (ANSI) and associated working groups, that will make fiber optic components from different manufacturers compatible with each other by specifying parameters such as data transmission rate (100 Mb/sec and above), power supply requirements, packaging and components. The FDDI local area networks will support up to 500 stations in a ring topology with circumference of up to 100 km, with dual rings to provide redundancy in case of cable or system failure.

Fiber-Optic Inter-Repeater Link (FOIRL): Fiber-optic signaling methodology based on the IEEE 802.3 fiber-optic specification.

Firewall: A hardware or software mechanism set up to protect the network from incoming traffic. A firewall typically is used to isolate from the network any external interface which is attached to, and has the capability of depositing on, the network.

Gateway: A device used to connect networks with radically different communications architectures. The gateway converts the facilities of one architecture to equivalent facilities in the other, thus allowing data to pass back and forth between the two networks.

Government Open Systems Interconnection Profile (GOSIP): Defines a common set of protocols and protocol options to be used by the U.S. Government agencies as they implement Open Systems Interconnection (OSI) networking products. The GOSIP protocols are designed to provide greater functionality and increased competition between vendors of hardware and software products to the Government.

Hub (major): The router that interfaces to the WAN and MAN.

Hub (minor): The router that connects to an interface off a major hub.

IEEE 802.3: Ethernet LAN protocol specifying an implementation of the physical layer and MAC sublayer of the link layer. IEEE 802.3 utilizes CSMA/CD access to a variety of speeds over a variety of physical media. One physical variation of IEEE 802.3 (10Base5) is very similar to Ethernet.

IEEE 802.5: Token Ring LAN - IEEE LAN protocol specifying an implementation of the physical layer and MAC sublayer of the link layer. IEEE 802.5 utilizes token passing access at 4 or 16 Mbps over shielded twisted pair wiring. Token Ring is supported via multiple media (fiber, UTP and STP. - Not recommended over UTP but certified).

Local Area Network (LAN): A communications network connecting various hardware devices together within a building by means of a continuous cable or an in-house voice data telephone system.

Media Access Control (MAC) Sublayer: The lower portion of the OSI model data link layer. The MAC sublayer is concerned with media access issues, such as whether token passing or contention will be used.

Multiprotocol Router: An OSI layer 3 device that can decide which of several paths network traffic will follow based on some optimality metric. Also called a

gateway (although this definition of gateway is becoming increasingly outdated), routers forward packets from one network to another, based on network-layer information.

Network: A web of interconnected nodes, incorporating telecommunications facilities and services that permits communications between and among the nodes. A physical network consists of transmission facilities, switching systems, and interface specifications. A logical network may be a subset of the above, sharing transmission facilities and services.

Node: A computer, workstation, PC, gateway, router, bridge, server, or other uniquely identifiable device attached to a segment of the network, which joins two or more networks.

Open System Interconnection (OSI): An international standardization program, facilitated by ISO and CCITT to develop standards for data networking, that facilitates multivendor equipment interoperability.

Protocol: A standard method of "handshaking" between network devices. This handshaking defines how information is exchanged between devices and what to do in the event of a fault.

Repeater: A device for physically extending and electrically isolating segments of a network cable. All signals sensed on one segment are "repeated" on the other segment.

Router: An inter-networking device that can dynamically route frames over a network, guided by parameters such as the quality of service required and the amount of traffic in the network. Routers are used most often to connect LAN's to wide area networks when both run the same network layer and higher layer protocols.

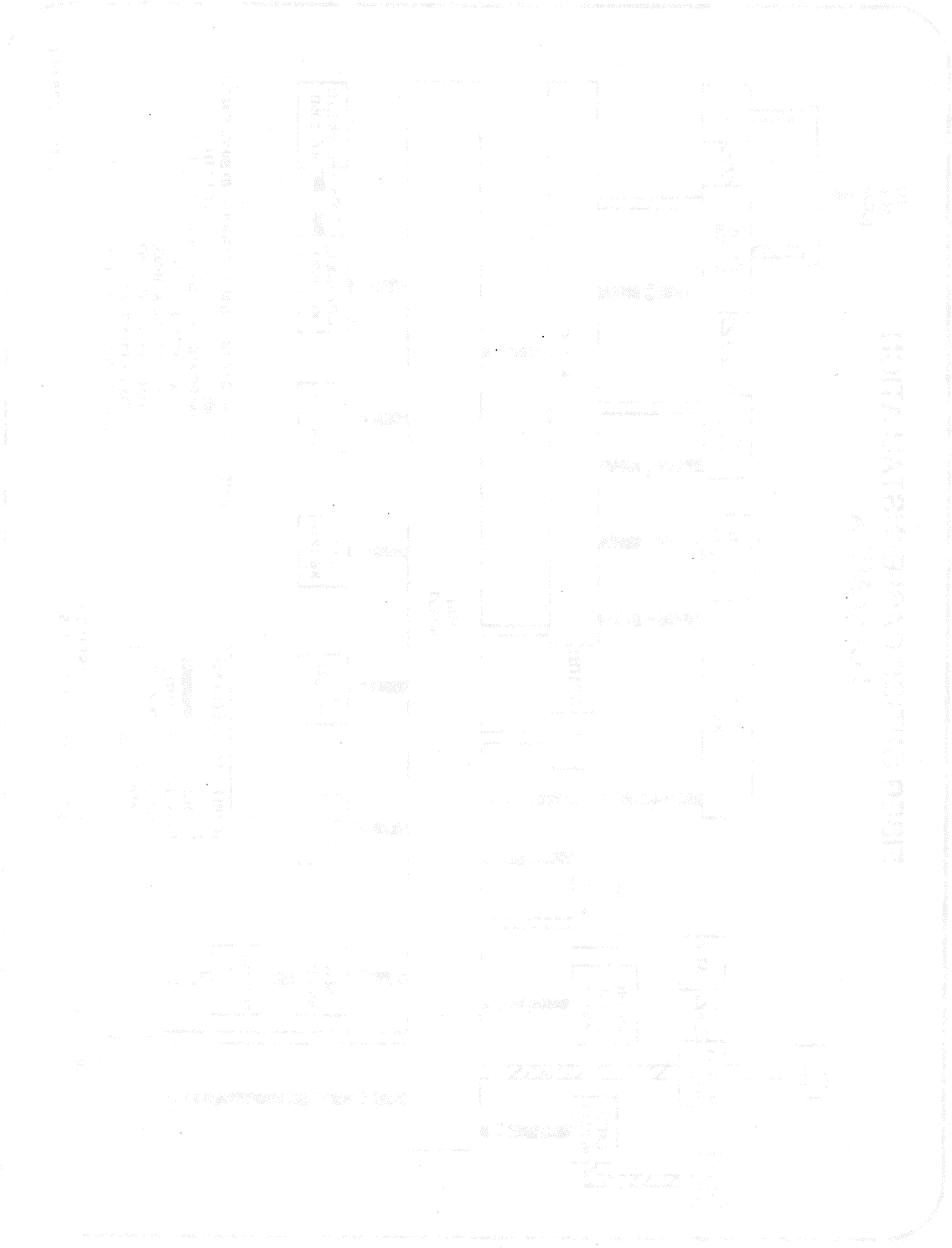
Simple Network Management Protocol (SNMP): The Internet network management protocol. SNMP provides a means to monitor and set network configuration and runtime parameters.

System Network Architecture (SNA): A large, complex, feature-rich network architecture developed in the 1970s by IBM.

Tunneling: The encapsulation of one protocol within another in order to gain advantages inherent in the encapsulating protocol such as routability or standardization. The advantages gained are usually achieved at the expense of network bandwidth and processing time on the source and destination hosts.

Wide Area Network (WAN): A system consisting of a set of nodes that are interconnected by a set of links, and generally covers a large geographic area.

APPENDIX C: PHYSICAL NETWORK ILLUSTRATIONS



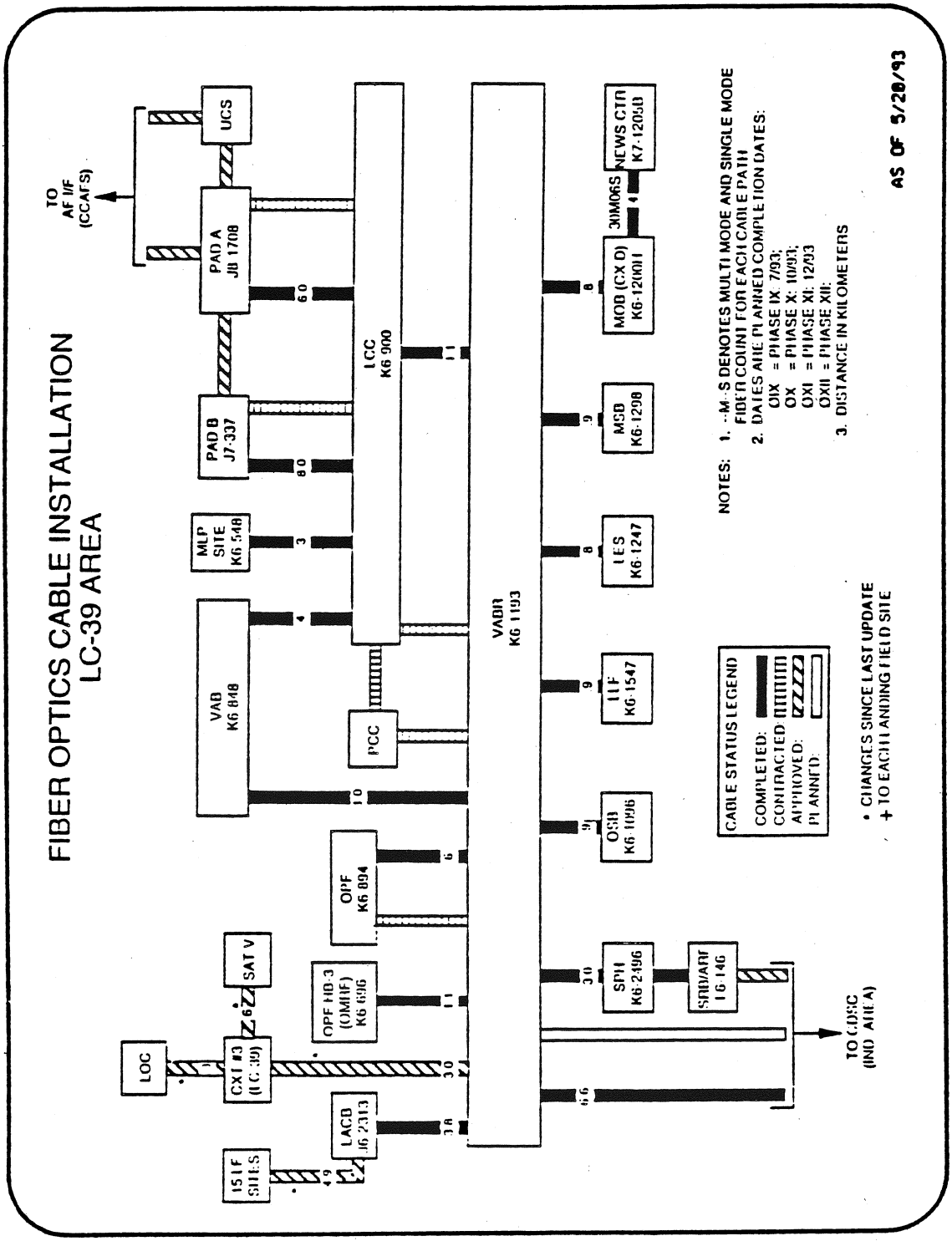


Figure 1. Fiber Optics Cable Installation - LC-39

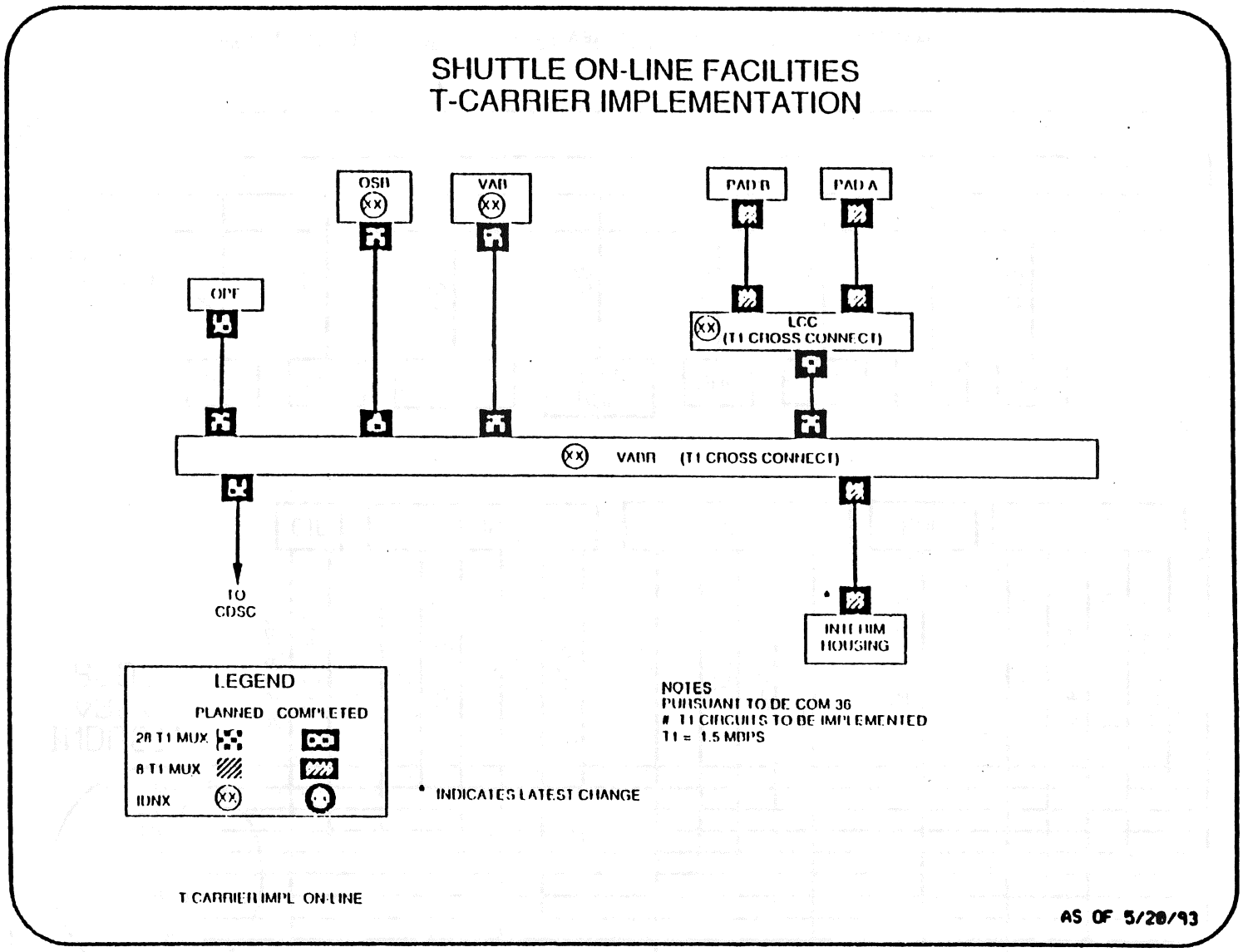


Figure 2. KSC LC-39 Area Facilities T-Carrier Implementation

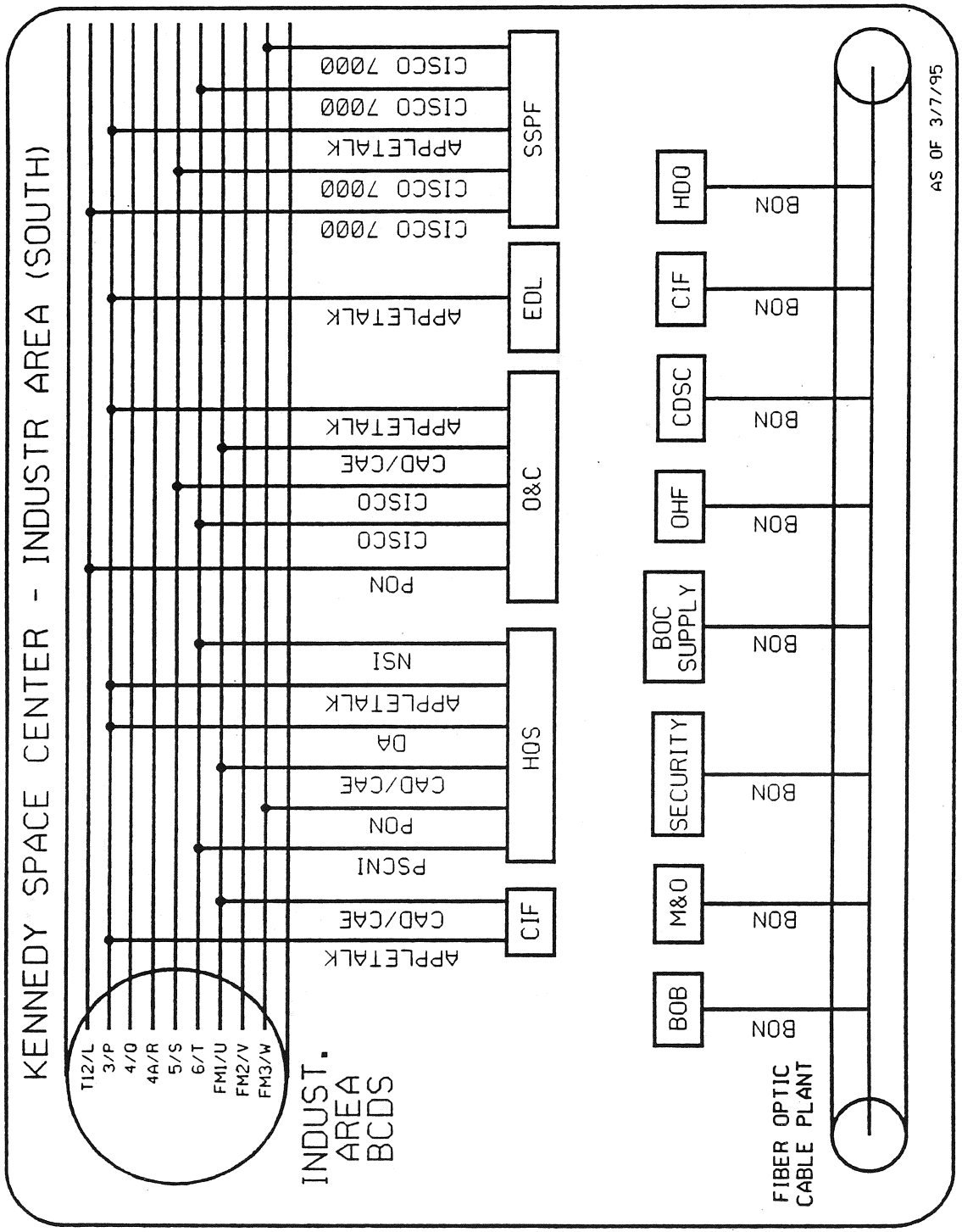


Figure 3. KSC Network Physical Layout - Industrial Area

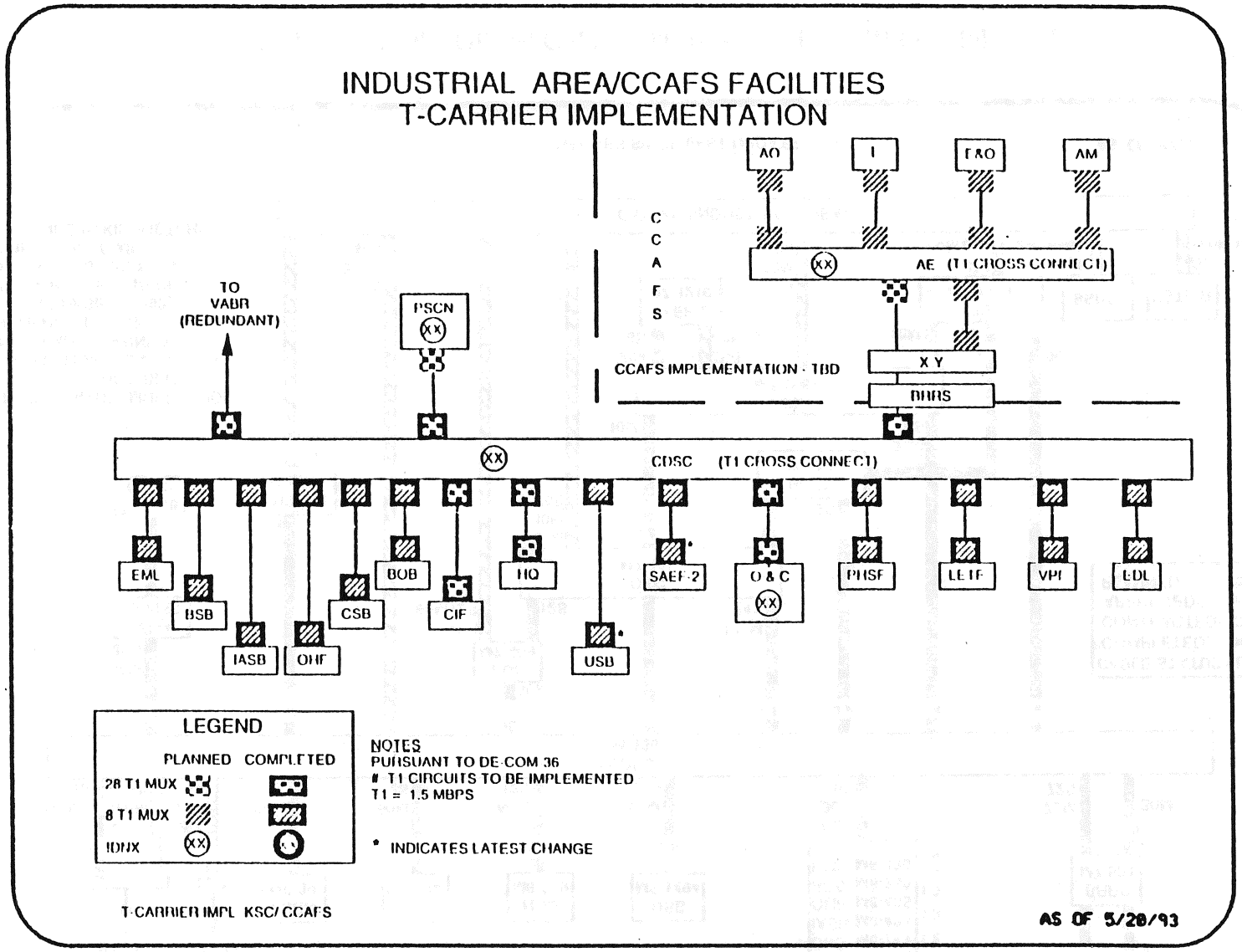


Figure 4. KSC Industrial Area/CCAS Facilities T-Carrier Implementation

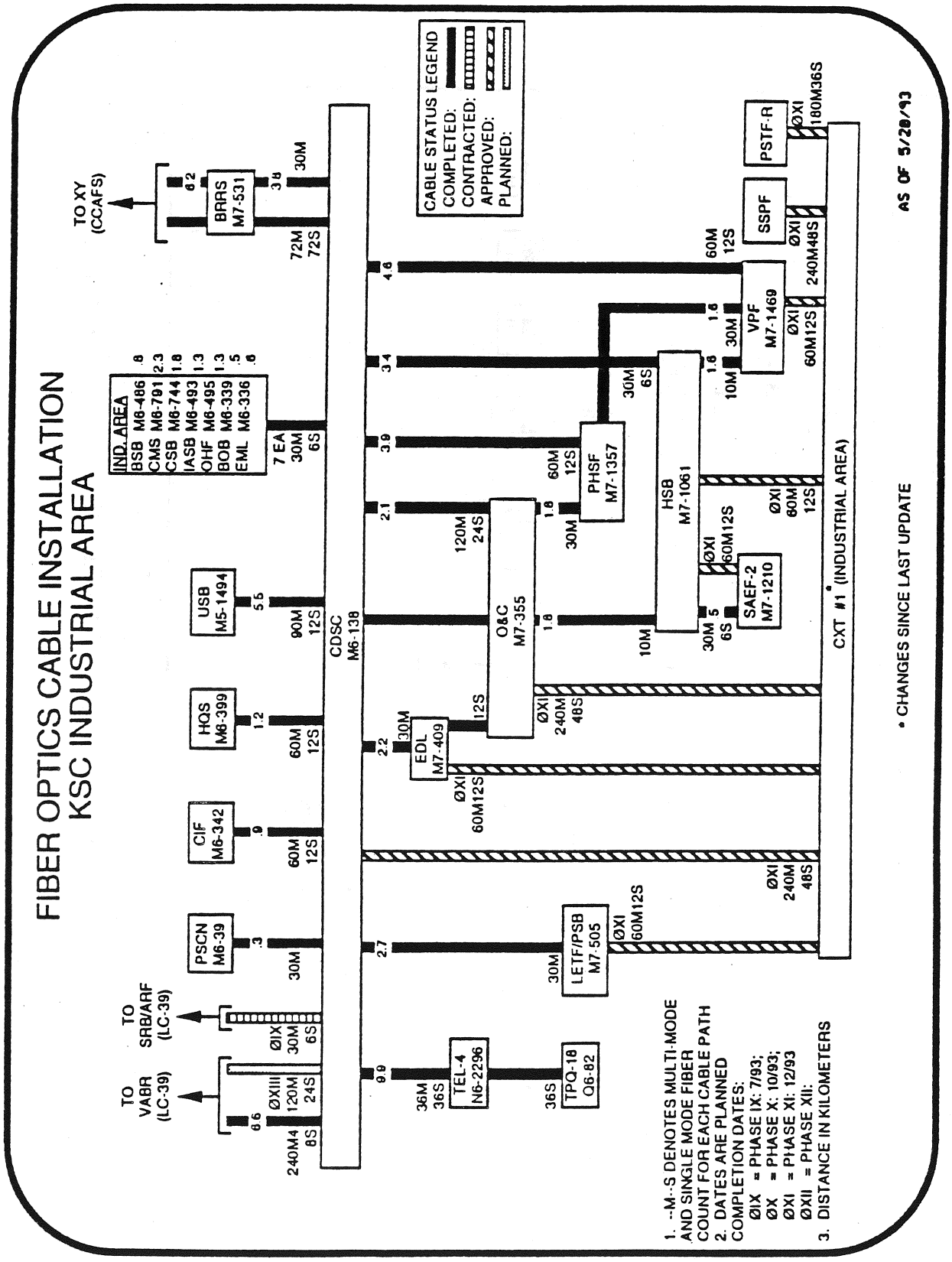


Figure 5. Fiber Optics Cable Installation - KSC Industrial Area

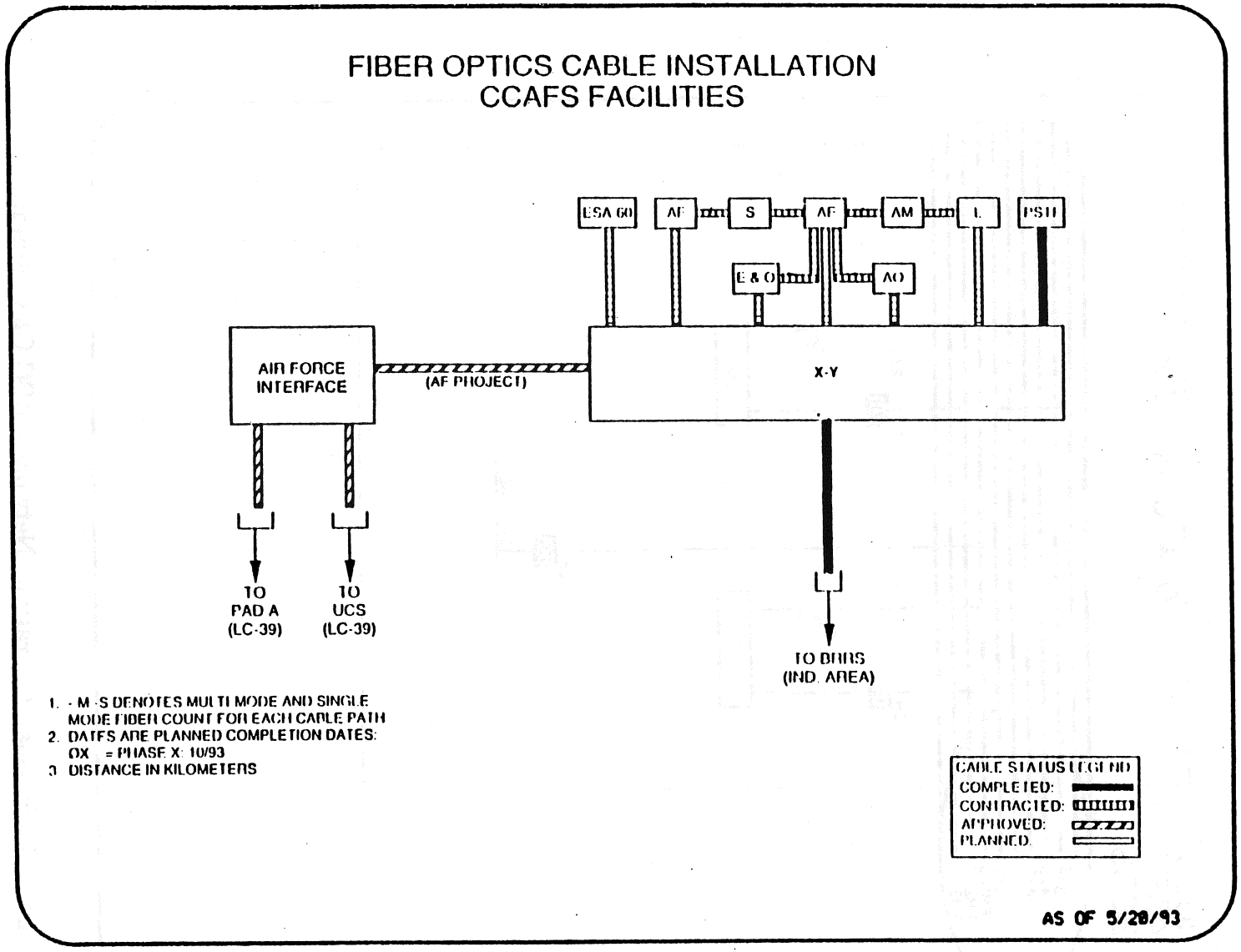


Figure 6. Fiber Optics Cable Installation CCAS Facilities (South)

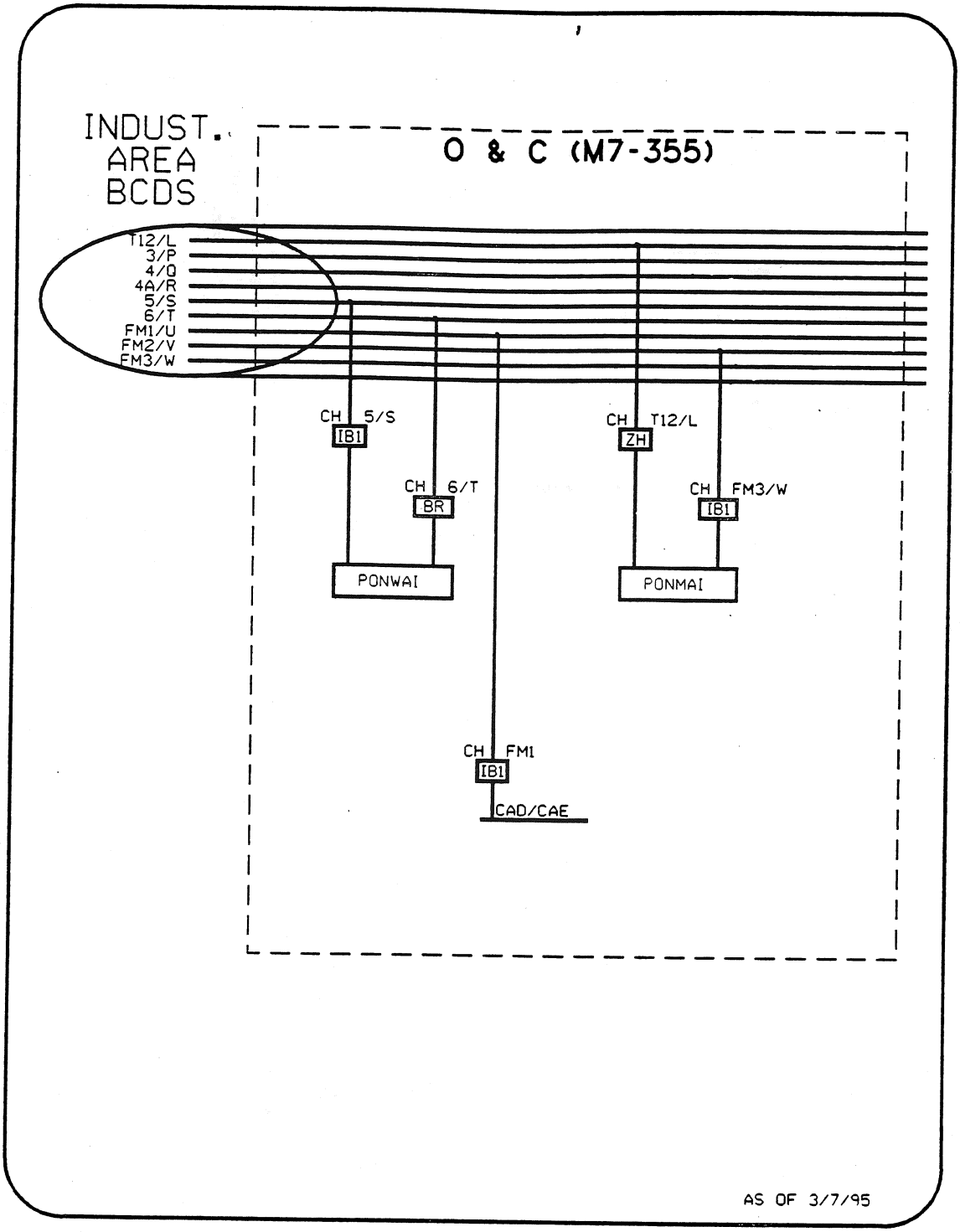


Figure 7. Payload Operations Network - KSC O&C Building

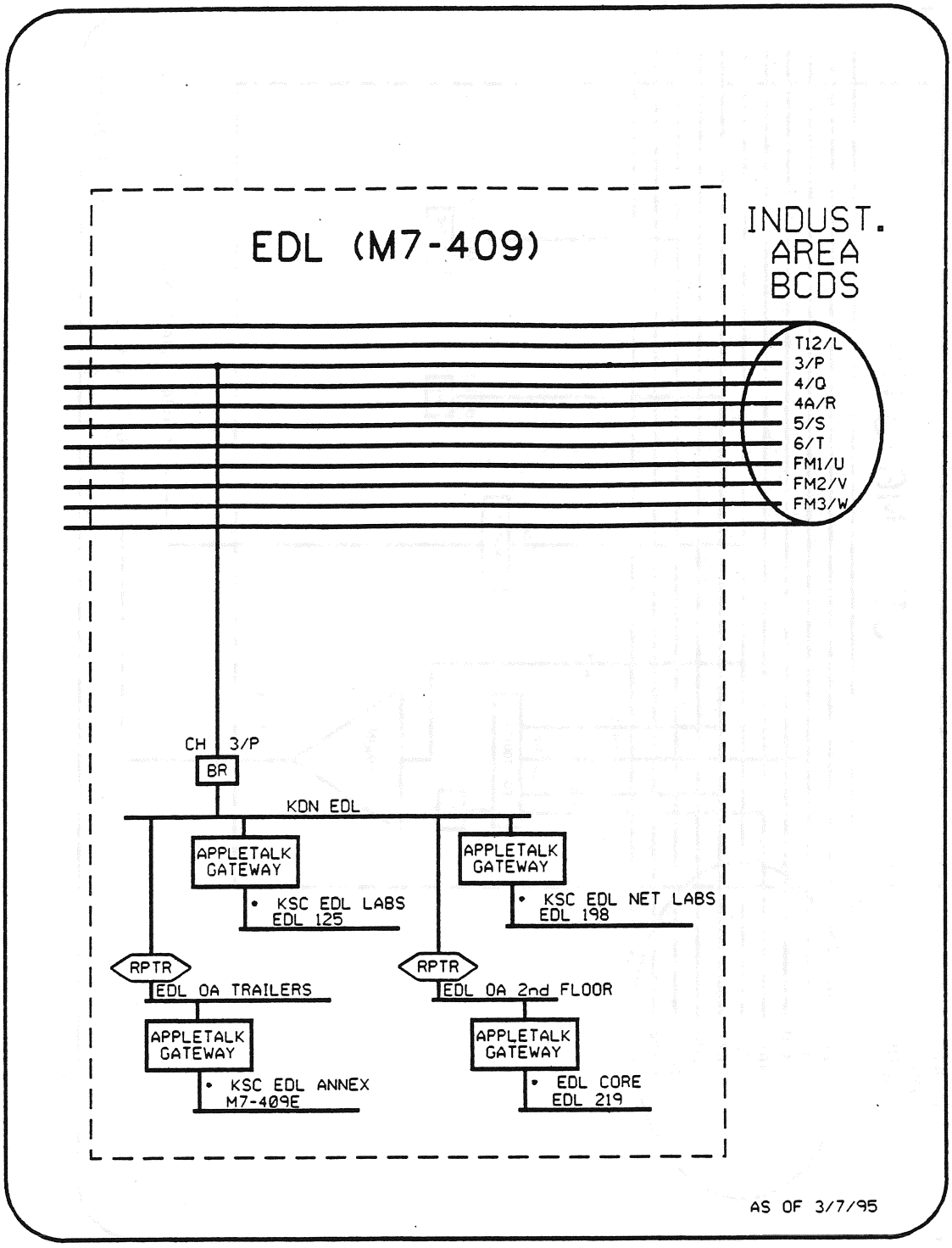


Figure 8. EDL Broadband Connections

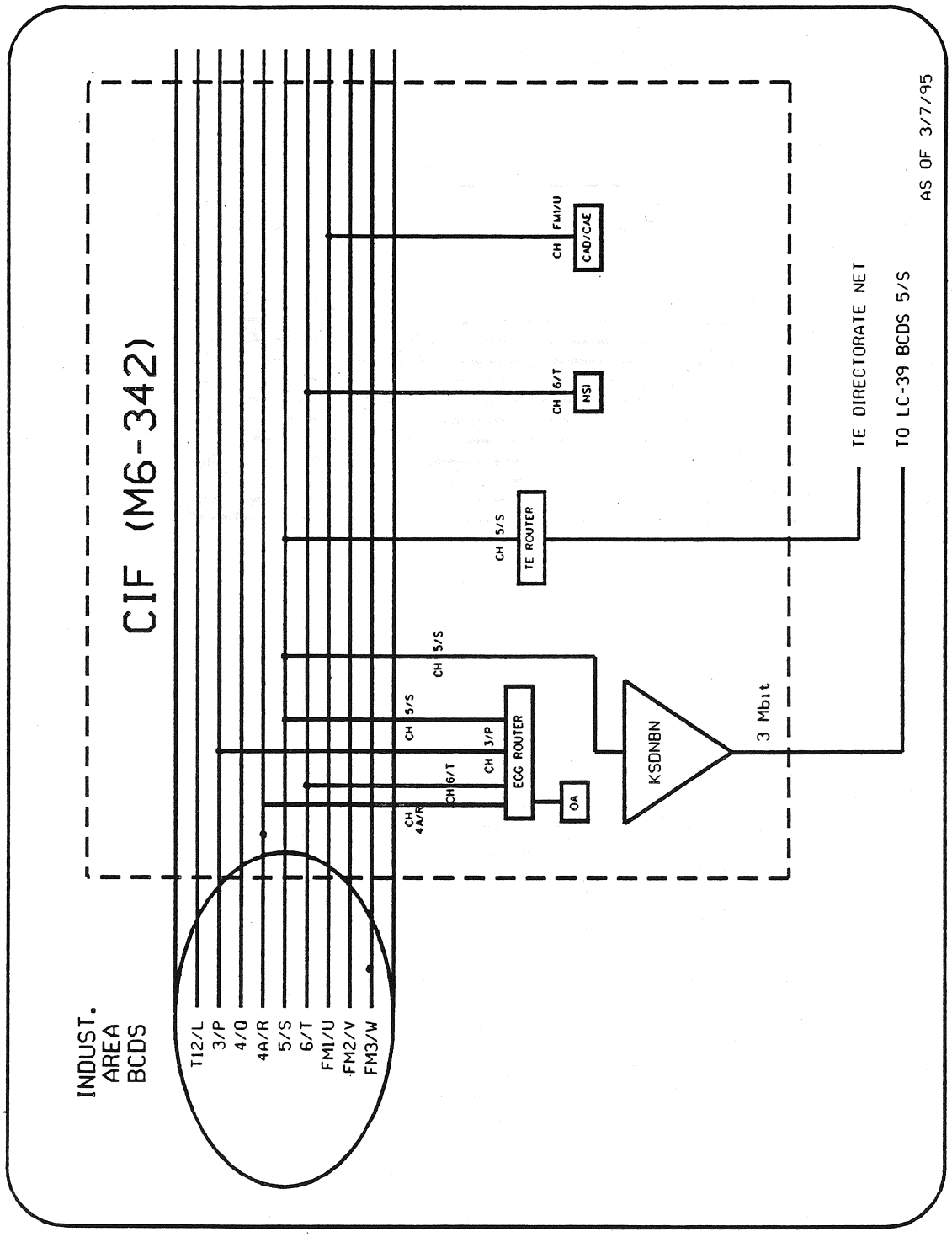


Figure 9. CIF Broadband Connections

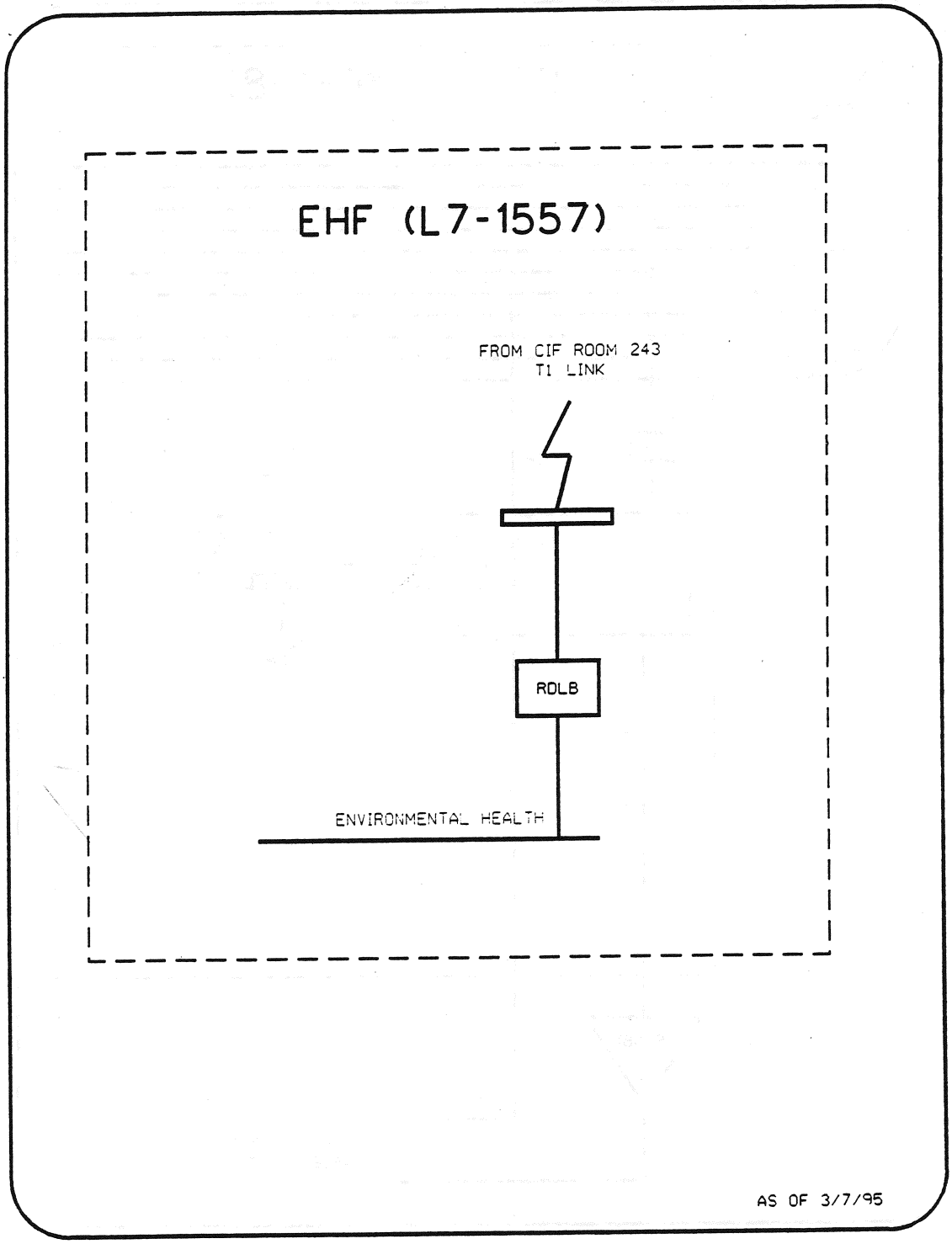


Figure 10. Environmental Health Facility Broadband Connection

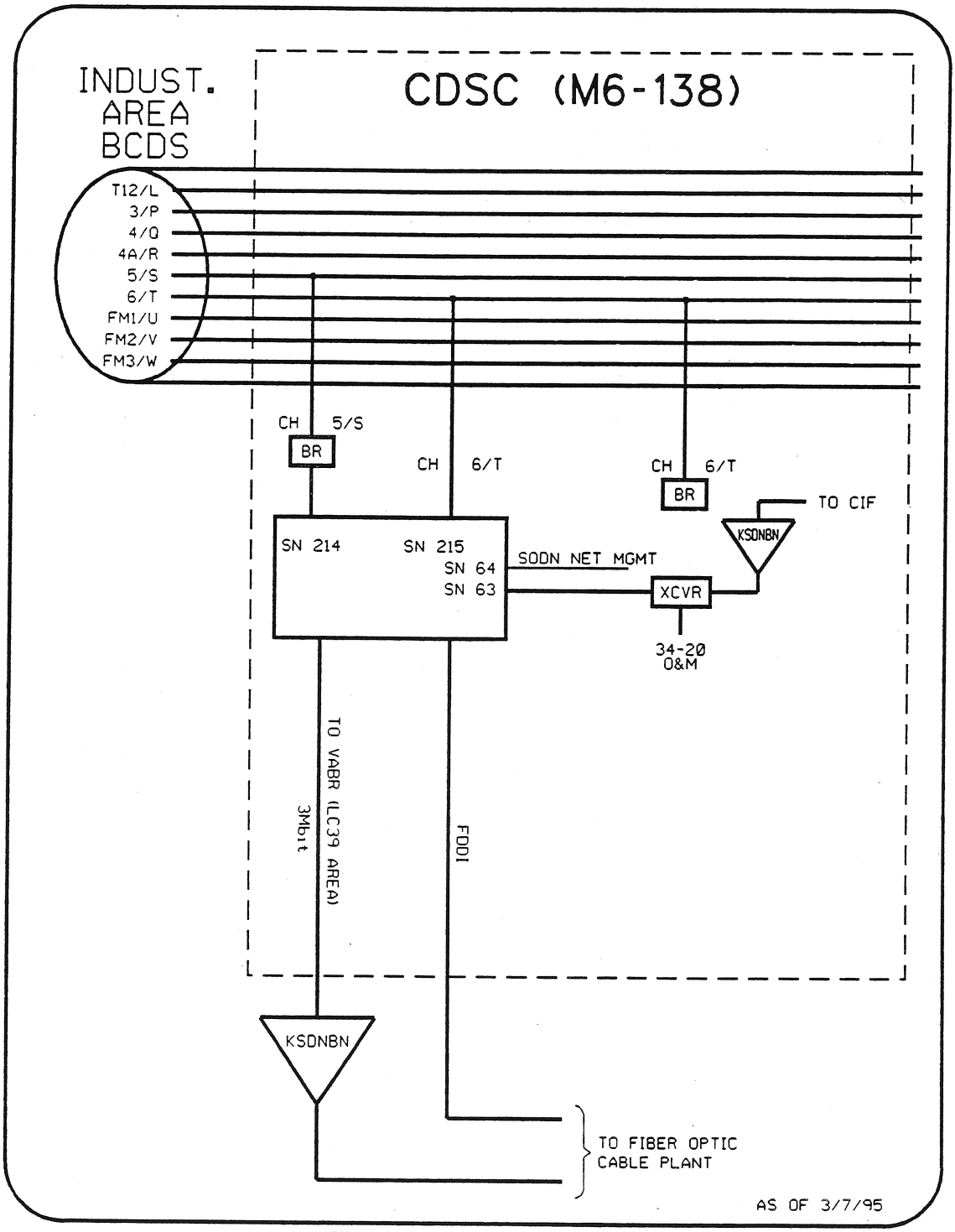


Figure 11. CDSC Broadband Connections

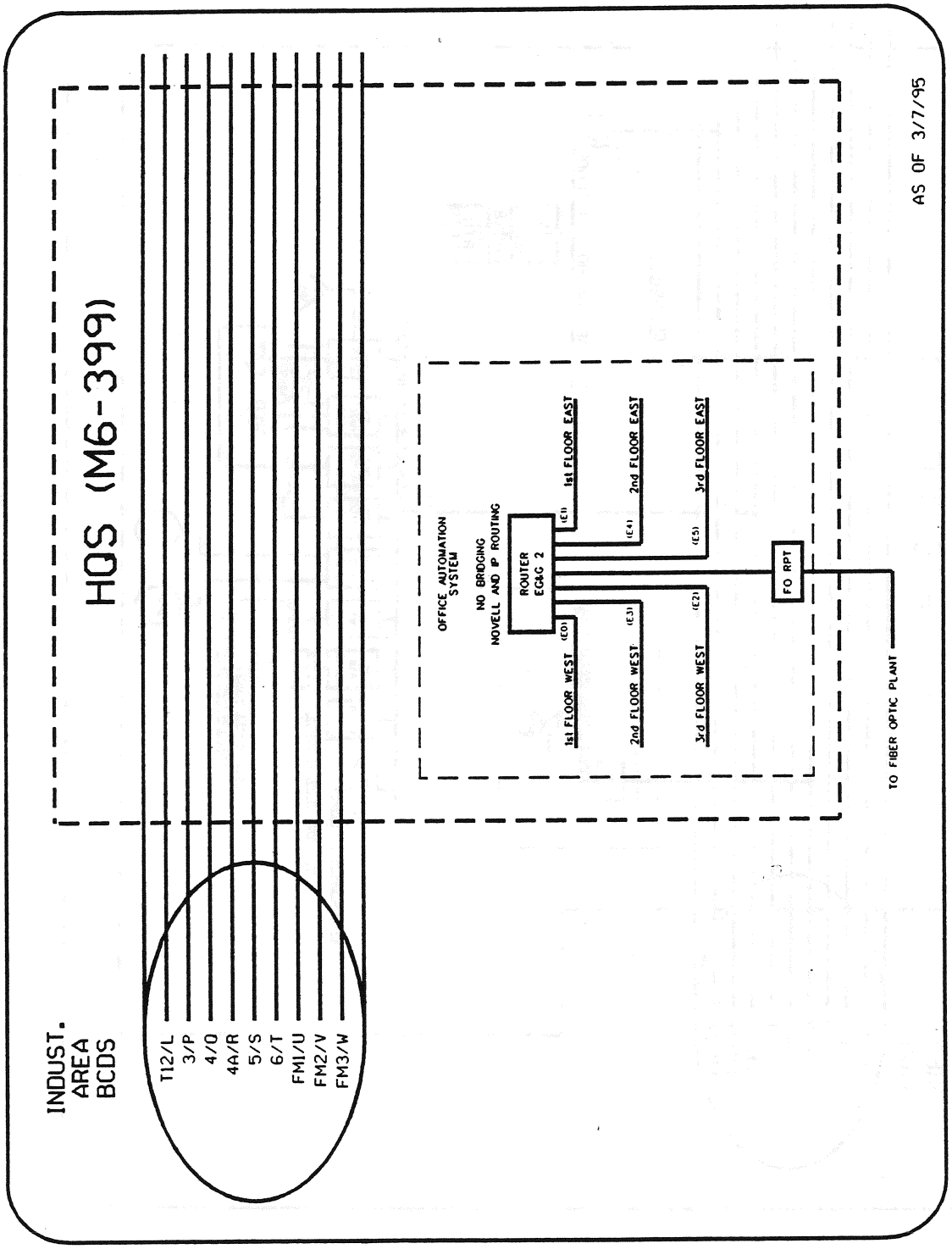


Figure 12a. HQS Bldg. Broadband Connections

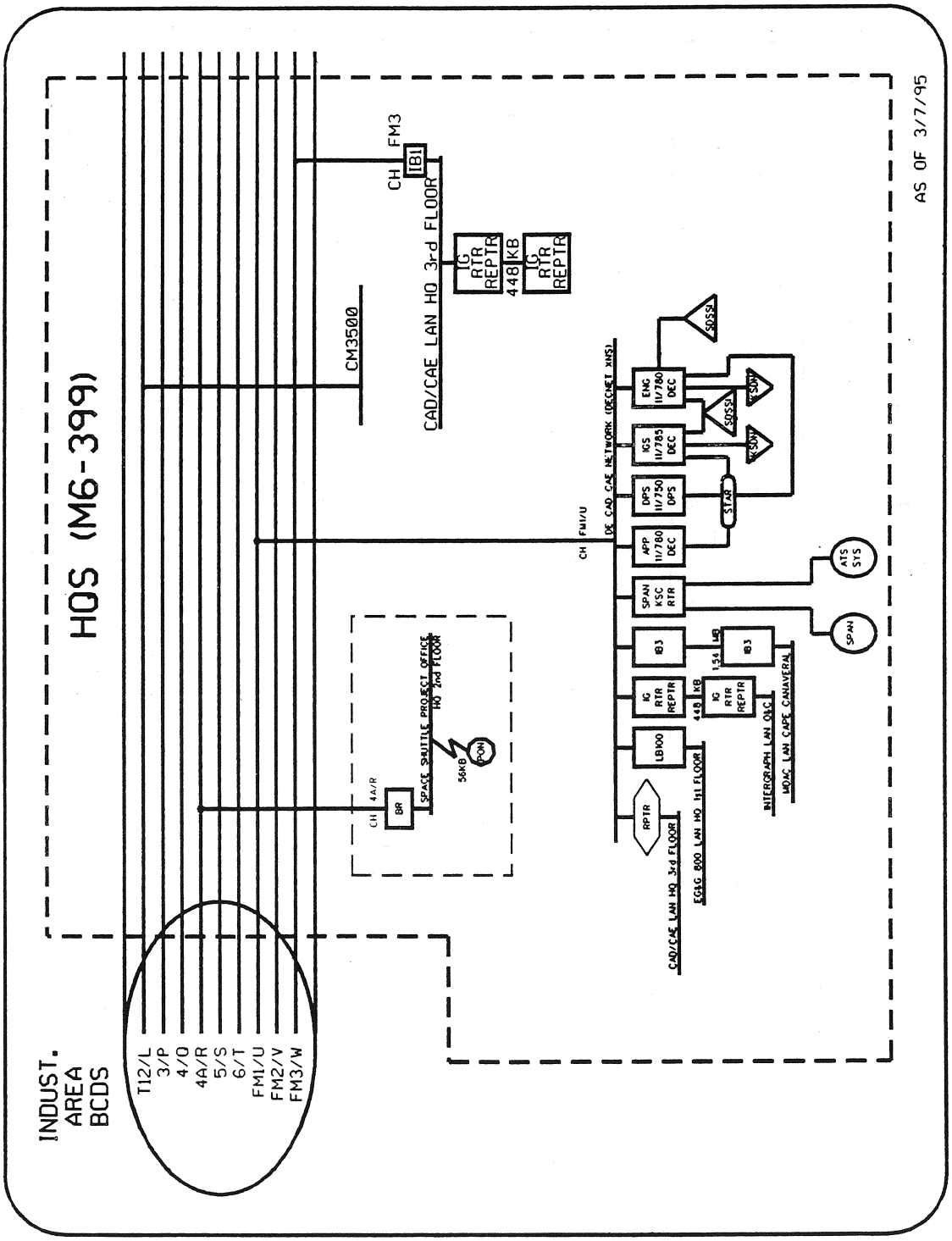


Figure 12b. HQS Bldg. Broadband Connections

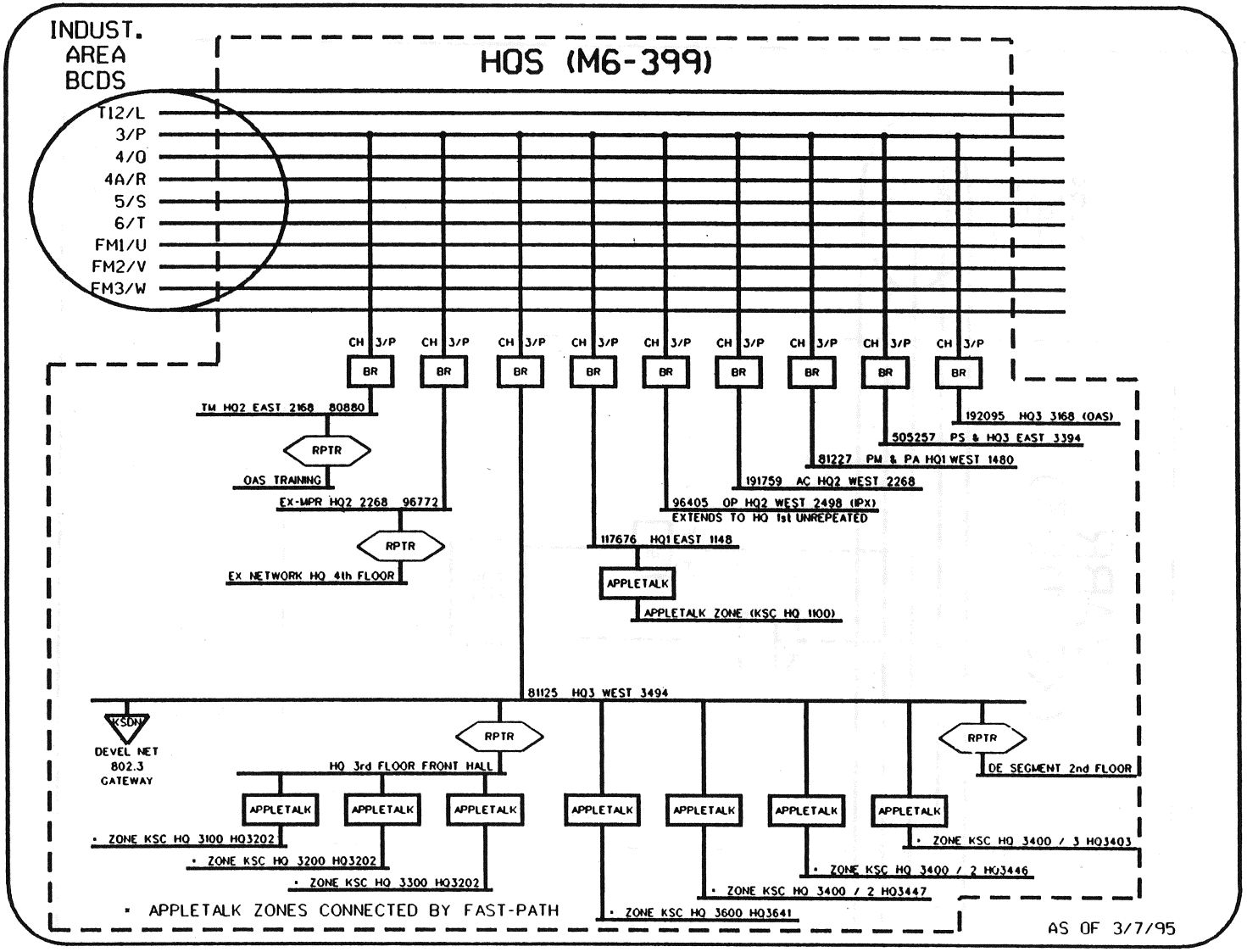


Figure 12c. HQS Bldg. Broadband Connections

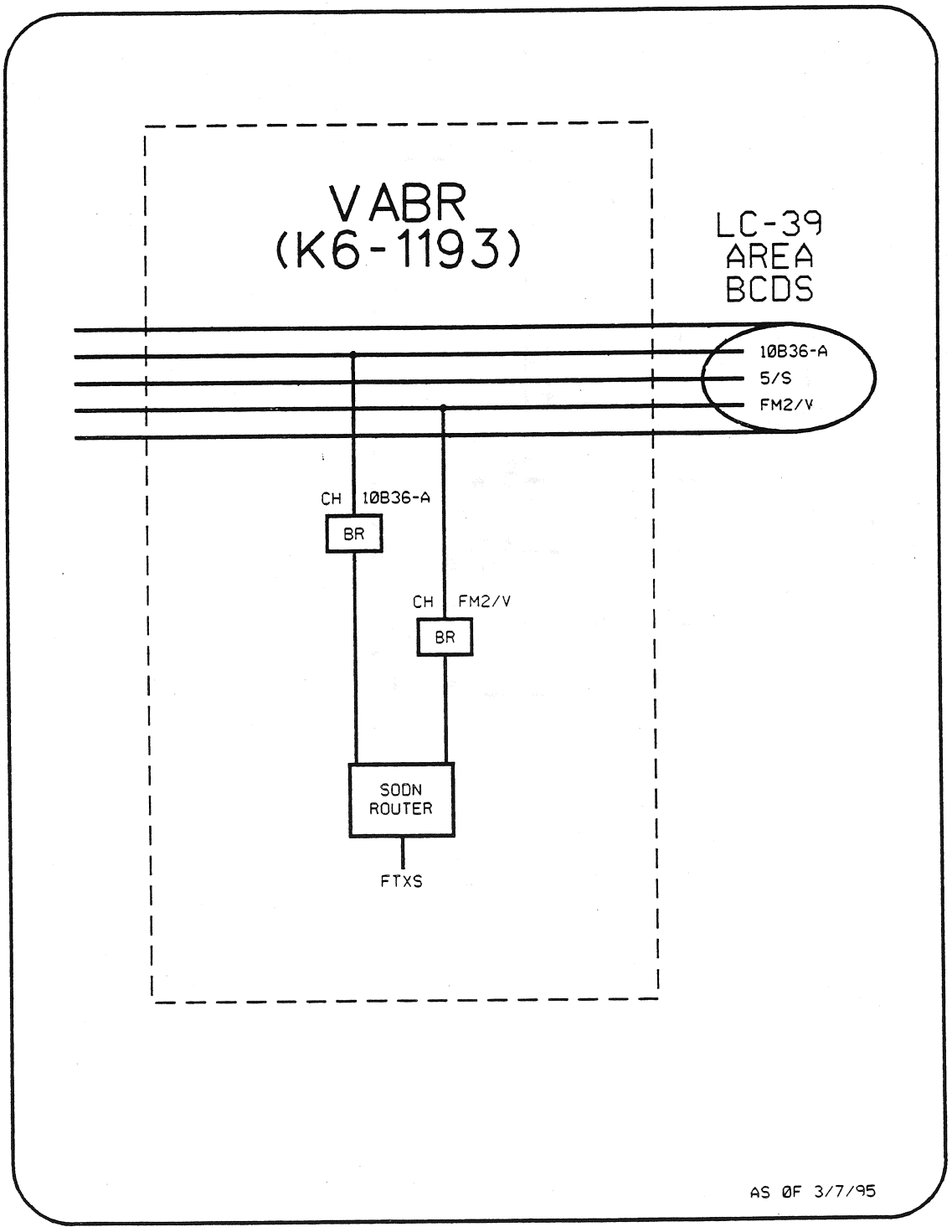


Figure 13. VAB Repeater Bldg. Broadband Connections

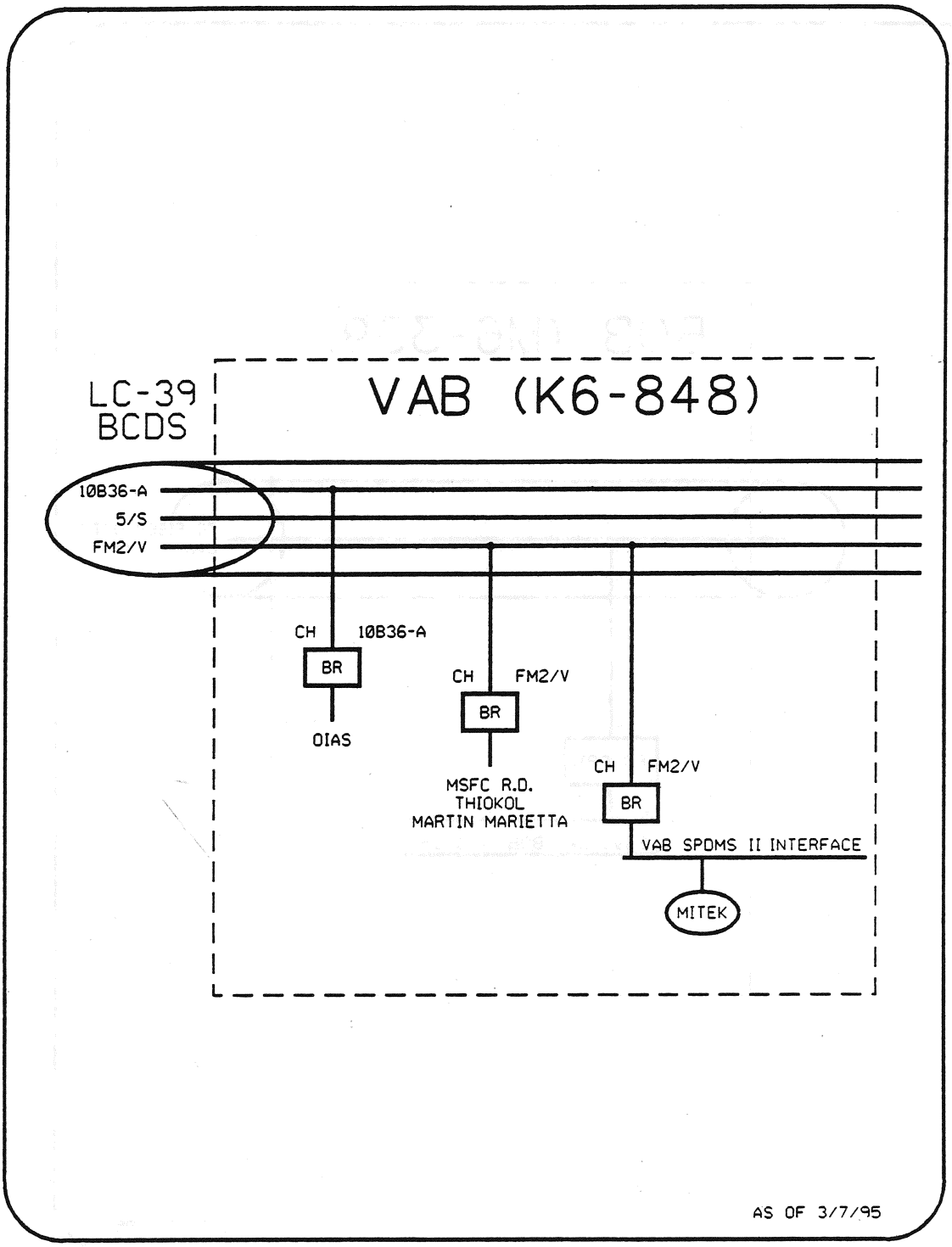


Figure 14. VAB Broadband Connections

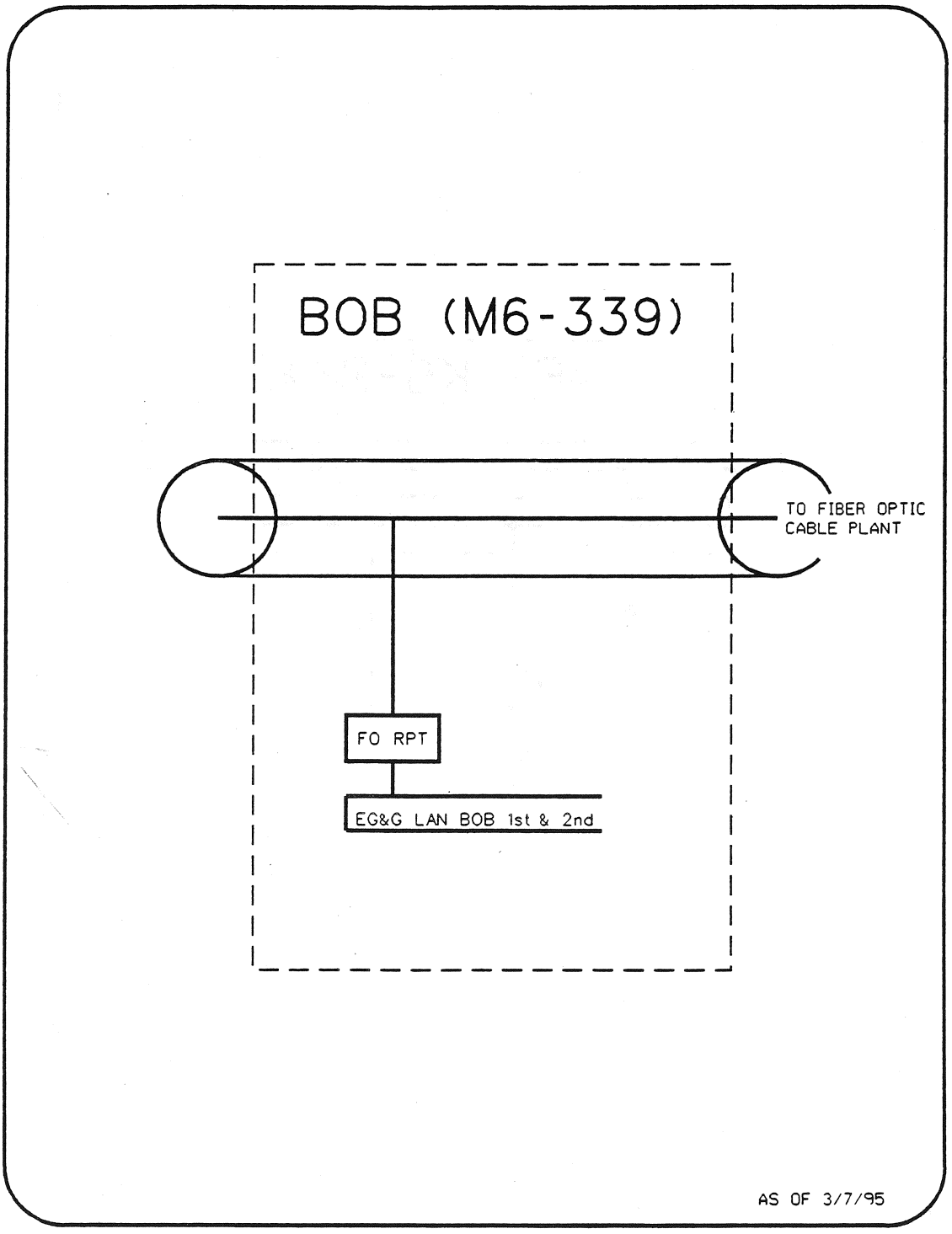


Figure 15. Base Operations Bldg. Fiber Optics Connections

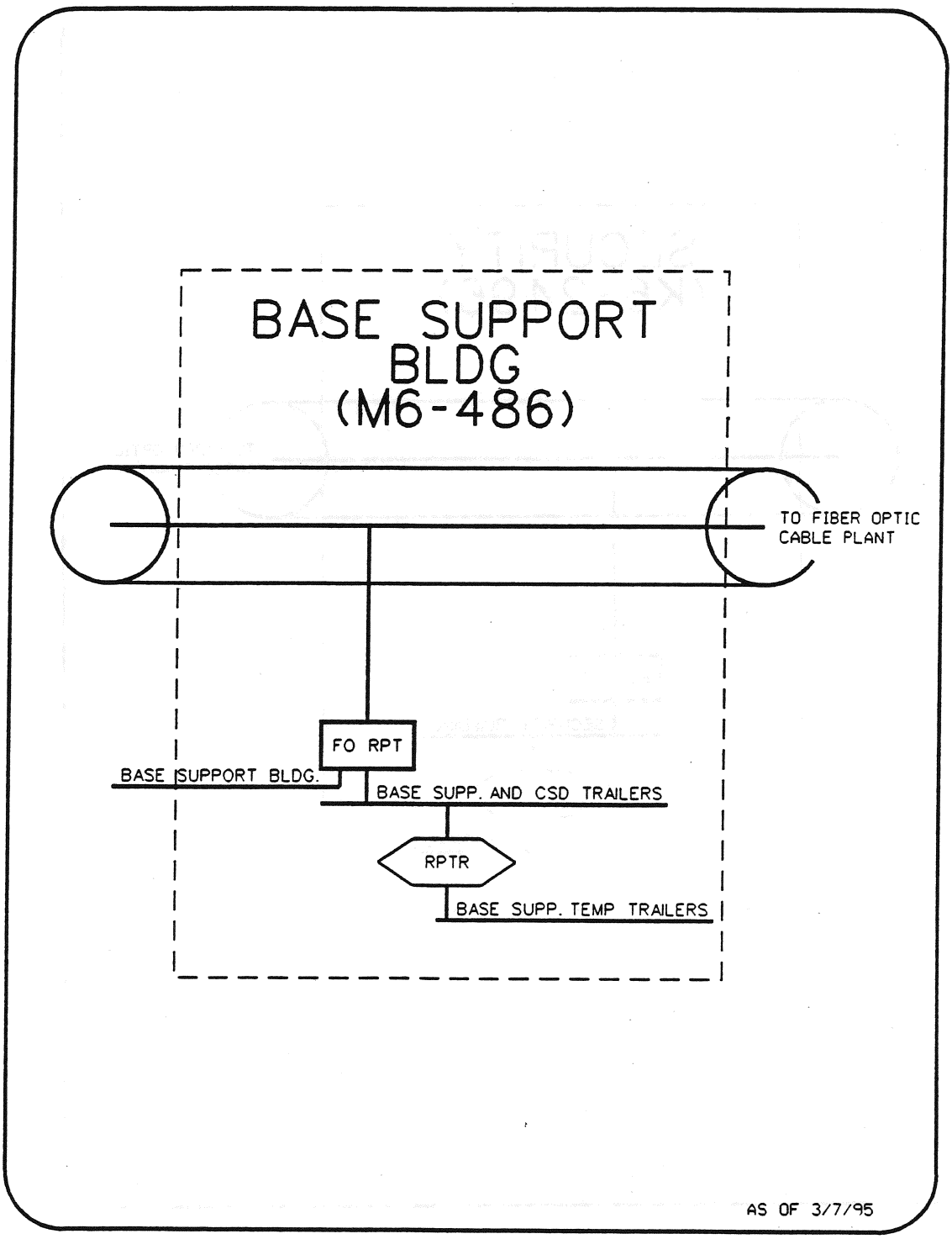


Figure 16. Base Support Bldg. Fiber Optics Connections

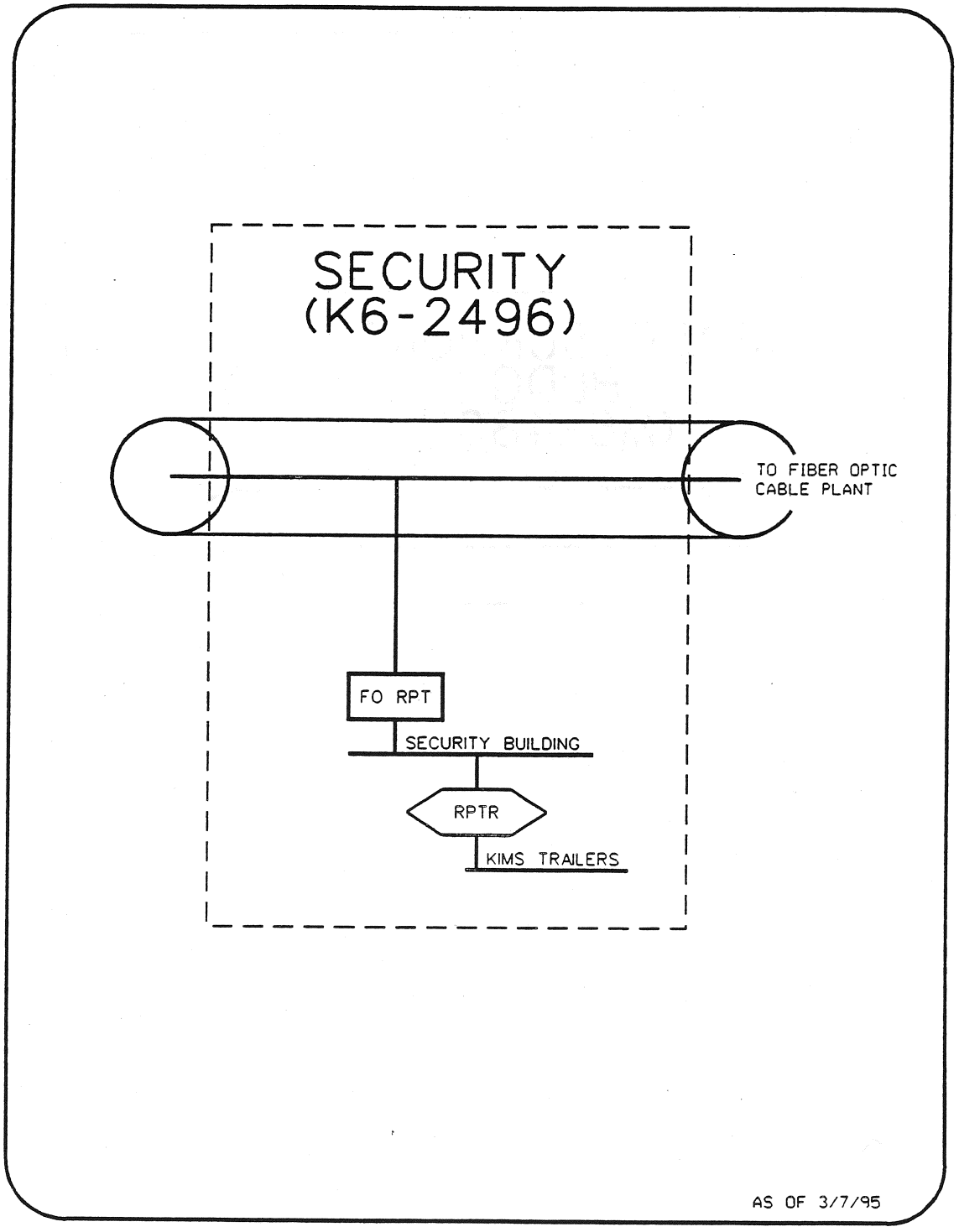


Figure 17. Security Bldg. Fiber Optics Connections

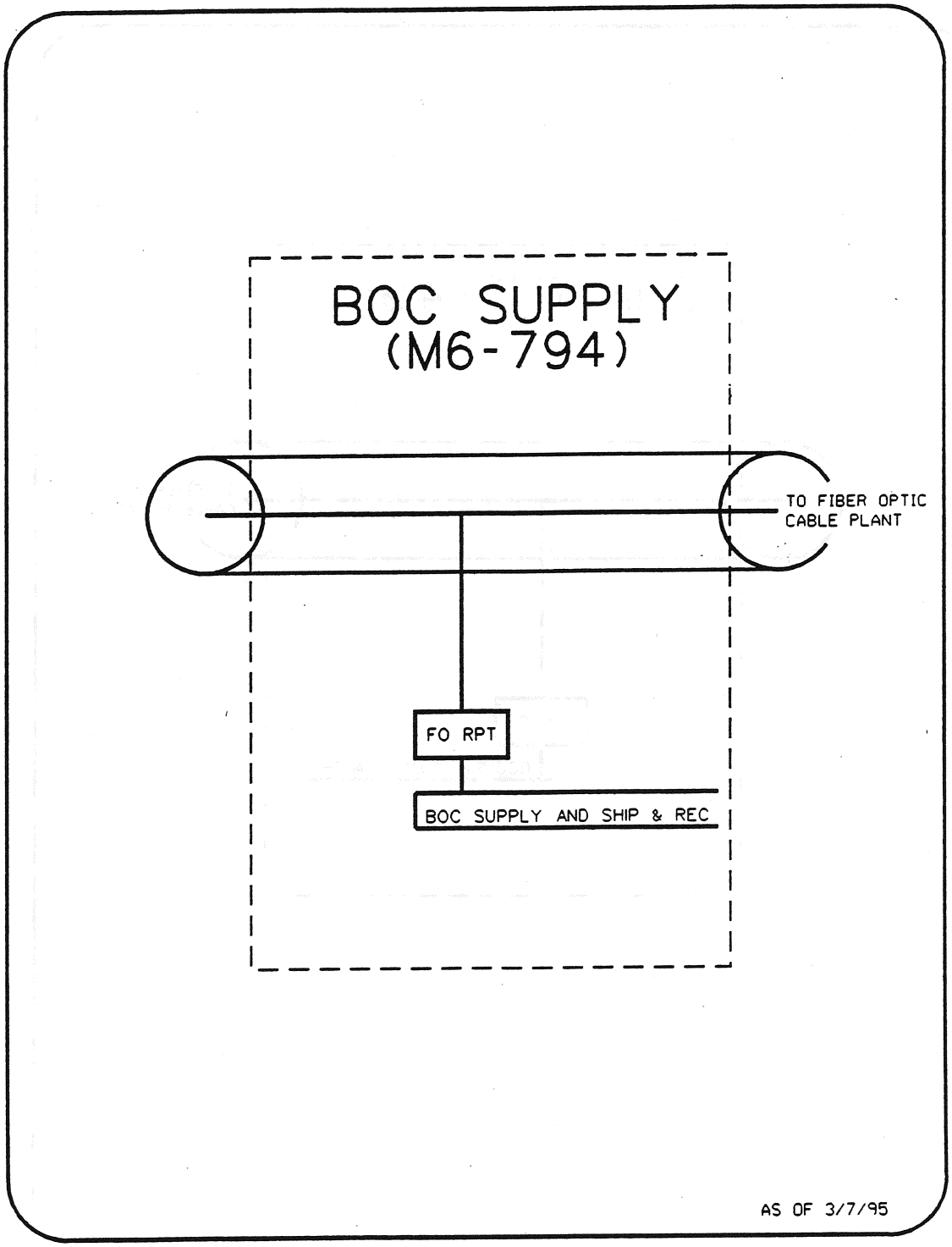


Figure 18. Base Operations Supply Building Fiber Optic Connections

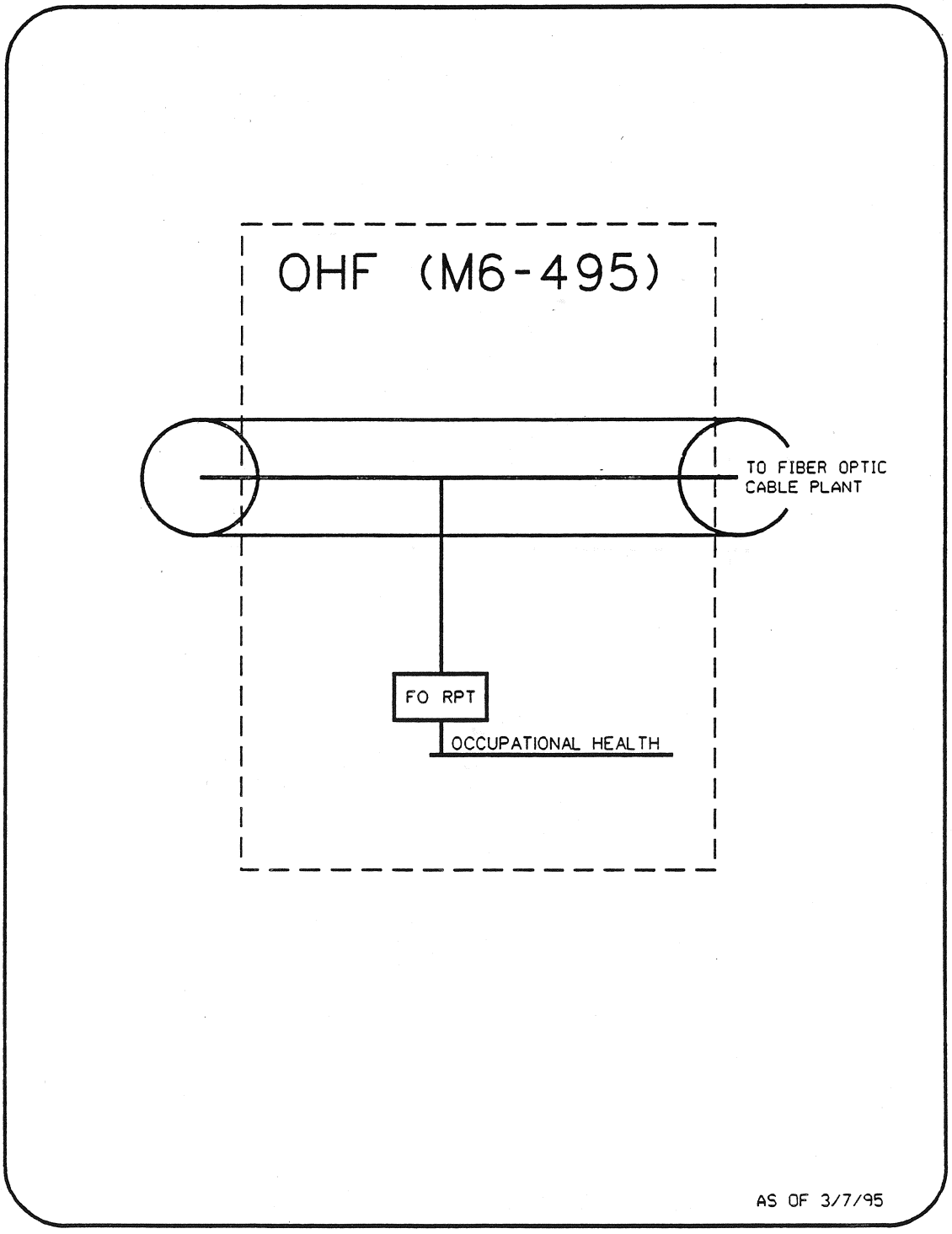


Figure 19. Occupational Health Facility Fiber Optic Connections

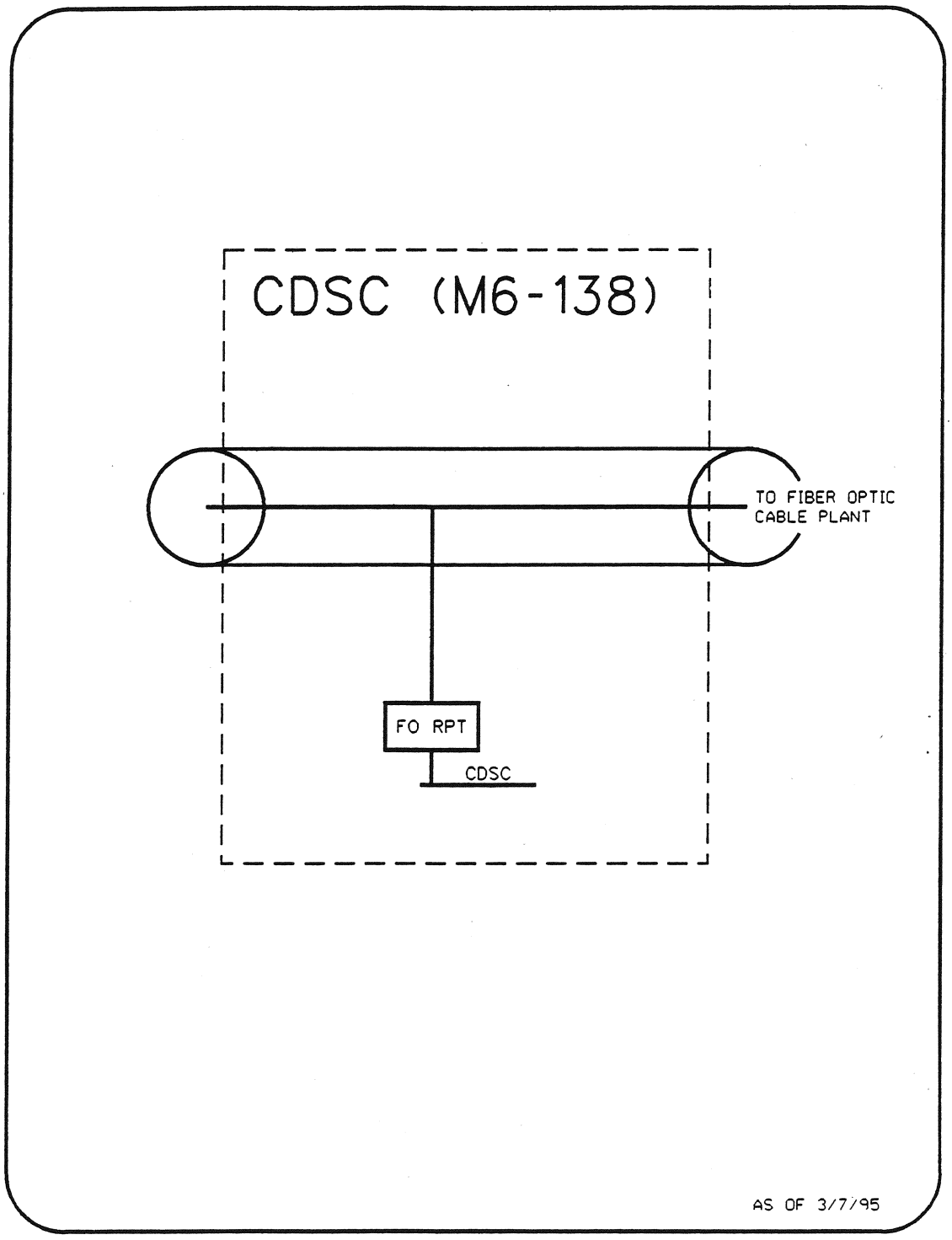


Figure 20. CDSC Fiber Optic Connections

APPENDIX D: NETWORK USER HELP GUIDE

I. Contact the following personnel to help with your network problems:

1. AppleTalk Network Support

Contact
Individual Networks and Apple Computer Support Desk, I-NET, 867-2334

2. Bionetics Work Order Tracking Network

Contact
C. Tintera, BICO/RIVETS ADP, 853-5673

3. Central Data System (CDS) Network

Contact
Glenn Seaton, TE-ISD-3, 861-7336
R. Miller, GTS-683, 861-6994
S. Kerney, LSO-073, 861-0836

4. KMail

Contact
Stephanie Sowards, IM-FCC-A, 867-4756
Linda Myers, DL-DSD-24, 867-4430

5. Kennedy Data Network (KDN) Support

Contact
C. Sims, IM-FCC-B, 867-7040
Waddy Blackmon, BOC-074, 867-3127

6. Kennedy Inventory Management System (KIMS)

Contact
Laddie Frye, BOC-140, 867-1602

7. **Kennedy Switched Data Network (KSDN)**

   Contact
   Michael Seay, TE-COM-2, 867-3180
   Anthony Valenti, LSO-110, 867-2023

8. **Launch Processing System (LPS) Office Network**

   Contact
   Glenn Seaton, TE-ISD-3, 861-7336

9. **LPS Operational Network (LON)**

   Contact
   Glenn Seaton, TE-ISD-3, 861-7336
   S. Kerney, LSO-073, 861-0836
   R. Miller, GTS-683, 861-6994

10. **Launch Processing System Software Development (LSDN) Network**

    Contact
    Steve Stover, TE-ISD-2, 861-7278
    David R. Slaiman, LSO-394, 861-7917

11. **NASA DE CAD/CAE Network**

    Contact
    Shawn Riley, BOC-139, 867-7007

12. **Network Documentation System (NDS)**

    Contact
    Felix A. Soto Toro, DL-CMD-N, 867-2228
    Bill Lohne, INI-18, 867-4847

13. **Network News Bulletin Board System**

    Contact
    Jim Dumoulin, CS-GSD-33, 867-3686
    Sam Rushing, CS-GSD-33, 867-3686

14. Payload Operations Network (PON)

Contact
J. Shaver, CG-ESD-1, 867-3731
Steve DeWitt, MDSS, 867-2826
Theresa Perkins, MDSS, 867-2826
Hours - (M-F, 7:00-4:30)

15. Payload Data Management System (PDMS)

Contact
Jim Dumoulin, CS-GSD-33, 867-3686
K. Mathews, MDSS, 867-8741
Joe Prevo, DEC, 867-1489

16. Program Support Communications Network (PSCN)

Contact
Darwin Brown, HM-INF, 867-7293
Milo Burgess, I-NET/PRISMS, PSC-01, 867-7726

17. Shuttle Processing Data Management System (SPDMS)

Contact
IPS Operations System/Network Control Center, LSO-184, 861-HELP

18. Shuttle Operations Data Network (SODN)

Contact
Michael Seay, TE-COM-2, 867-3180
Charles Gebelein, LSO-115, 867-2023

19. Space Shuttle Program Network (SSPN)

Contact
Chuck Ellis, Rockwell, ZK 06, 861-2671

20. KSC Wide Area Network (KWAN)

Contact
John Schnitzius, DL-CMD-N, 867-7278

21. **45th Space Wing Network**

    Contact
    Paul Dassing and John Gleason, CSR, 494-6689

22. **DE Integrated Engineering Computer System (IECS)**

    Contact
    J. Barnes, DL-CMD-N, 867-7278
    B. Boatright, DL-CMD-N, 867-7278
    Don Philp, INI-11, 867-2334

II. Contact the following personnel to help with your transmission problems:

1. **Broadband Communication Data System (BCDS)**

   Contact
   Gerald Talley, TE-CID-2, 867-3180
   Michael Springer, LSO-115, 867-8024

2. **Data Voice Communications System (DVCS) Transmission**

   Contact
   Rich Nelson DL-CMD-R, 867-1391

3. **Fiber Distributed Data Interface (FDDI)**

   Contact
   Victor Gonzalez, TE-COM-2, 867-3180
   Matthew Guessetto, LSO-111, 867-4704
   Bryan Boatright, DL-CMD-N, 867-7278

4. **Multiplexed Data Transmission System, fiber based**

   Contact
   Bill Toler, TE-CID-2, 867-3180
   Walt Bridges, LSO-110, 867-2023

5. **T-Carrier/SONET Transmission System, fiber-based**

   Contact
   Victor Gonzalez, TE-CID-2, 867-3180
   Dennis Weatherby, LSO-110, 867-2023

6. Wideband Transmission Systems, Copper-based

Contact
Bill Toler, TE-CID-2, 867-3180
Walt Bridges, LSO-110, 867-2023

7. Wideband Transmission System, fiber-based

Contact
Bill Toler, TE-CID-2, 867-3180
Walt Bridges, LSO-110, 867-2023

APPENDIX E

KSC NETWORK SERVICE REQUEST FORMS

This appendix contains these forms:

- SODN Service Request - New Service
- SODN Service Request - Relocation/Deletion
- SODN Network/Subnet Address Request
- SODN Domain Name Service (DNS) Request
- KSDN Service Request - New Service
- KSDN Service Request - Relocation
- Support Request
- Engineering Support Request
- McDonnell Douglas Customer Service Request
- Avoid Verbal Orders Form 1-14
- KSC Access Via WAN Request Form
- Payload Data Management Systems Access Request Form
- Shuttle Processing Data Management System ID Support Request Form
- Memorandum of Understanding - SPDMS II Personal User ID
- T-1 Service Request Form
- DE IECS Support Request Form

SODN Service Request

- New Service -

Fill out, attach to an ESR or SR, and forward to the appropriate agency for processing.

Customer Information

1. Customer Identification
   Name | Org. | Mail code | Phone No.
2. Equipment Type
   Mfr. Name | Model No. | Qty.
3. Equipment Location
   Building No. | Room No.
4. Equipment Layout (Include Sketch)

Existing Local Area Network (LAN)

To be filled out by the responsible LAN administrator and/or LAN manager if the requested service requires connection to an existing local area network, i.e., Ethernet or Token Ring.

5. Type of LAN (Specify Cable Type(s))
6. Location of LAN (Include Drawing or Sketch)
7. Type of Network Operating System
8. Network Address/Subnet Address (If Applicable)
9. Network Protocols
10. Applications
11. File/Print Servers
    Number | Bldg./Rm. Locations
12. Users
    Number | Bldg./Rm. Locations

LAN Information

To be filled in by the responsible LAN administrator and/or LAN manager.

13. LAN Administrator/Manager Information
    Name | Org. | Mail Code | Phone No.
14. Type of Service
    Ethernet | Token Ring | Other
15. Type of Network Operating System
16. Approximate Number of Users
17. Network Address/Subnet Address Required
    Yes _____ No _____ (If Yes, Fill Out KSC Form 29-783)
18. Network Protocols
19. Applications
20. Domain Name Service Required
    Yes _____ No _____ (If Yes, Fill Out KSC Form 29-786)
21. Mail Host Name (If Applicable)
22. Network Adapter
    Mfr. | Model No. | Interface
23. Communications Required
    Name _____ Org. _____ Ph. No. _____ Type of LAN _____ Network Address _____
    Name _____ Org. _____ Ph. No. _____ Type of LAN _____ Network Address _____
    Name _____ Org. _____ Ph. No. _____ Type of LAN _____ Network Address _____
24. Lan Manager/Administrator Concurrence (Signature)

KSC FORM 29-784 (12/92)

SODN Service Request - New Service

SODN Service Request

- Relocation/Deletion -

Fill out, attach to an ESR or SR, and forward to the appropriate agency for processing.

Customer Information

1. Customer Identification
   Name | Org. | Mail code | Phone No.
2. Equipment Type
   Mfr. Name | Model No. | Qty.
3. Equipment Location
   Building No. | Room No.

Check One:

4. Relocation _____ 5. Deletion _____

Existing Local Area Network (LAN)

If this is a service deletion, fill out block 6 and skip to line 25. This section to be filled out by the responsible LAN administrator and/or LAN manager if the requested service requires connection to an existing local area network, i.e., Ethernet or Token Ring.

6. Present SODN Circuit Number
7. Location of New Requirement (Include Drawing or Sketch)
8. Type of Network Operating System
9. Network Address/Subnet Address (If Applicable)
10. Network Protocols
11. Applications
12. File/Print Servers
    Number | Bldg./Rm. Locations
13. Users
    Number | Bldg./Rm. Location

LAN Information

To be filled in by the responsible LAN administrator and/or LAN manager.

14. LAN Administrator/Manager Information
    Name | Org. | Mail Code | Phone No.
15. Type of Service
    Ethernet | Token Ring | Other
16. Type of Network Operating System
17. Approximate Number of Users
18. Network Address/Subnet Address Required
    Yes _____ No _____ (If Yes, Fill Out KSC Form 29-783)
19. Network Protocols
20. Applications
21. Domain Name Service Required
    Yes _____ No _____ (If Yes, Fill Out KSC Form 29-786)
22. Mail Host Name (If Applicable)
23. Network Adapter
    Mfr. | Model No. | Interface
24. Communications Required
    Name _____ Org. _____ Ph. No. _____ Type of LAN _____ Network Address _____
    Name _____ Org. _____ Ph. No. _____ Type of LAN _____ Network Address _____
    Name _____ Org. _____ Ph. No. _____ Type of LAN _____ Network Address _____
25. Lan Manager/Administrator Concurrence (Signature)

KSC FORM 29-785 (12/92)

SODN Service Request - Relocation/Deletion

SODN Network/Subnet Address Request

Fill out, attach to an ESR or SR, and forward to the appropriate agency for processing.

Customer Information

1. Customer Identification
   Name | Org. | Mail code | Phone No.
2. Equipment Type
   Mfr. Name | Model No. | Qty.
3. Equipment Location
   Building No. | Room No.
4. Equipment Layout (Include Sketch)

LAN Information

To be filled in by the responsible LAN administrator and/or LAN manager.

5. LAN Administrator/Manager Information
   Name | Org. | Mail Code | Phone No.
6. Type of LAN
   Ethernet | Token Ring | Other
7. Location of LAN (Include Drawing or Sketch)
8. Type of Network Operating System
9. Users (Approximate)
   Number | Bldg./Rm. Locations
10. File/Print Servers
    Number | Bldg./Rm. Locations
11. Network Protocols
12. Applications
13. Domain Name Service Required
    Yes _____ No _____ (If Yes, Fill Out KSC Form 29-786)
14. Mail Host Name (If Applicable)
15. Lan Manager/Administrator Concurrence (Signature)

LAN Information

To be filled in by LSOC Communications personnel. A copy of the request will be returned to the requester.

16. Network Connected to SODN?
    Yes _____ No _____ (If No, Explain Off-Site Connectivity, Including Sketch or Drawing)
17. Network Address Class
    A _____ B _____ C _____ D _____ E _____
18. IP Subnet Assignment
    _____ To _____

KSC FORM 29-783 (12/92)

SODN Network/Subnet Address Request

SODN Domain Name Service (DNS) Request

Fill out, attach to an ESR or AVO, and forward to the appropriate agency for processing.
Customer must complete an SODN Services Request, KSC Form 29-784 and/or an SODN Network/Subnet Address Request form, KSC Form 29-783.

Customer Information

1. Customer Identification

Name | Org. | Mail code | Phone No.

LAN Information

To be filled in by the responsible LAN administrator and/or LAN manager.

2. LAN Manager/Administrator Concurrence (Signature)

Host Information

List host name and associated IP address. Attach hard copy of hosts if applicable.

Host Name	IP Address

KSC FORM 29-786 (12/92)

KSDN SERVICE REQUEST
— NEW SERVICE —

This Form, when properly filled out, will be attached to an ESR and forwarded to the appropriate agency for processing and implementation.

NOTES:

1. *See completion instructions for clarification.*
2. *Hayes SMART modems or equivalent are not compatible with the KSDN system.*

Originating Equipment: (Terminal/Printer, CPU Etc.)

1. Type Of Service: Synchronous _____ Asynchronous _____
2. Speed Required: BIT/BAUD rate _____
3. Equipment type: Mfg. Name _____ Model No. _____ Unit Type _____
4. Equipment Location: Building No. _____ Room No. _____
5. Equipment Layout: _____
6. Customer Identification:

   Name: _____ Mailcode: _____ Phone No. _____

7. Communications With:

   _____ _____ _____ _____

   _____ _____ _____ _____

NOTE:
Lines 8 thru 11 are not required to be filled in unless the requested service requires direct access to a mainframe computer, another terminal or a printer.

Terminating Equipment:

8. Equipment Type: Mfg. Name _____ Model No. _____ Unit Type _____
9. Equipment Location: Building No. _____ Room No. _____
10. Equipment Layout: _____
11. Customer Identification:

    Name: _____ Mailcode: _____ Phone No. _____

12. Need Date: Desired _____ Required _____
13. Requestor Responsibilities:

    A. Insure that adequate AC power receptacles are available to power up the equipment. One AC outlet is required for each terminal, printer, CPU and modem.

    B. To provide any RS-232 cables. If the short RS-232 pigtail that comes with the modem is not adequate.

    C. To provide any fallback switches that may be required.

    D. To provide the telephone number(s) associated with accoustic couplers being replaced with hardline data circuits.

KSC FORM 29–248 (REV. 1/86)

KSDN Service Request - New Service

KSDN SERVICE REQUEST
— RELOCATION —

This Form, when properly filled out, will be attached to an ESR and forwarded to the appropriate agency.

NOTE:

See completion instructions for clarification.

1. Circuit Number _____

2. Existing Equipment Location: Building No. _____ Room No. _____

3. New Equipment Location: Building No. _____ Room No. _____

4. Equipment Layout: _____

5. Customer Identification:

   Name: _____ Mailcode: _____ Phone No. _____

6. Need Date: Desired _____ Required _____

7. Communications With:

   _____ _____ _____ _____

   _____ _____ _____ _____

8. Requestor's Responsibilities:

   A. Insure that adequate AC power receptacles are available to power up the equipment at the new location. One (1) AC outlet is required for each terminal, printer, modem.

   B. For relocation of RS-232 cables and fallback switches.

KSC FORM 29—247 (REV. 1/86)

KSDN Service Request - Relocation

1 W.O. NO.	SUPPORT REQUEST					2. CONTROL NO.
REQUESTING OFFICE COMPLETES BLOCKS 3.23	3 REQUESTER (NAME, SYMBOL, PHONE NO.)		4 TECHNICAL CONTACT (NAME, SYMBOL, PHONE NO.)		5. REQ. OFFICE AUTHORIZATION (SIGNATURE & DATE) (SYMBOL, PHONE NO.)	
	6 PROGRAM	7. VEHICLE	8. EVENT	9. CAT.	10. DATE SUBMITTED	11. DUE DATE
12. ECP NO./FEC NO	13. CCBD NO.	14. CR NO.	15. O&M RESP.	16. NASA SYS. ENG.	17. MATERIAL SOURCE (CONTACT & PHONE NO.) AVAILABILITY DATE:	
18 SUPPORT DESCRIPTION (A. JOB DESCRIPTION, B. LOCATION OF COMPLETED WORK, C. JUSTIFICATION, D. EFFECT OF DELAY, E. POSSIBLE HAZARDS INVOLVED.) SAMPLE						19 WORK TYPE 20. RECOMMENDED SUPPORT AGENCY 21. REF. SR'S NO. _____ NO. _____ NO. _____ NO. _____ 22. ENCLOSURES SKETCH/DWGS. ☐ YES ☐ NO MOD INSTR PKG. ☐ YES ☐ NO MIP #
						23. QUALITY REQUIREMENT CONTR. QAL. INSPECTION ☐ YES ☐ NO GOV'T SOURCE INSPECTION ☐ YES ☐ NO QAL SIGNATURE
24 AREA FACILITY AUTHORIZATION (SIGNATURE & DATE)	25 PERFORMING ACTIVITY	26 ESTIMATED HOURS	ACTUAL HOURS	MATERIAL COSTS		
27 PERFORMING ACTIVITY COMPLETION (SIGNATURE & DATE)	28 INSPECTED BY (SIGNATURE & DATE)		29 ACCEPTED BY (SIGNATURE & DATE)			

KSC FORM 10-15 (REV. 3/80)

Support Request

ENGINEERING SUPPORT REQUEST	1. DATE	2. PROGRAM NO.	3. ESR NO. REV.	4. SHEET _____ OF _____
5. LOCATION	6. EFFECTIVITY	7. EVENT REQ'D BY	8. USER NEED DATE	9. CATEGORY
10. FACILITY/SYSTEM/EQUIPMENT	11. PART	12. PART NO.	13. REF. DES/FIND	14. LEVEL INTERFACE AFFECTED
15. TITLE				17. MANUFACTURER
16. DESCRIPTION OF REQUIREMENT/CONDITION/EVENT				18. TYPE OF ACTION
				19. SCHEDULE IMPACT
20. ACTION REQUESTED				
21. JUSTIFICATION				
22. COMMENTS AND ACTION ITEMS				

23. TECHNICAL CONTACT			24. APPROVAL			25. DE APPROVAL		
NAME	ORG.	PHONE	SIGNATURE	ORG.	DATE	SIGNATURE	ORG.	DATE

SAMPLE

KSC FORM 21-318 (MAY 8/77)

Engineering Support Request

McDonnell Douglas Space Systems Company
Kennedy Space Center

Customer Service Request

Request No.

Requestor Information

Name _____ Employee No. _____ Mail Code _____
Phone No. _____ Company _____
Date of Request _____ Bldg./Room No. _____

Authorization

Senior Manager Signature _____ Date Required _____
Material Cost Charge No. _____ WBS _____ Property Cust. ____

Service Information

CPU Tag No.: NASA/MDSSC _____
Hardware Manufacturer _____ Model No. _____ CPU Serial No. _____
Operating System: MS DOS/UNIX/OS2/Finder/Other _____

One CSR Per PC **Type of Service Requested** *One CSR Per PC*

☐ New Circuit (One per request)*
New Location Site/Bldg. _____ Rm. _____

☐ Relocate Existing Circuit: (One per request)*
Old Location Site/Bldg. _____ Rm. _____
New Location Site/Bldg. _____ Rm. _____

☐ Additional Connections on Existing Line
New Location Site/Bldg. _____ Rm. _____

SAMPLE

☐ Payload Television Systems (VRSS Connectivity)

☐ Hardware/Software Request

☐ Application Access

☐ Other

*Note: Drawing of Existing/Desired Circuit Location Required!

A. Description **B. Justification** **C. Effect of Delay**

A. _____

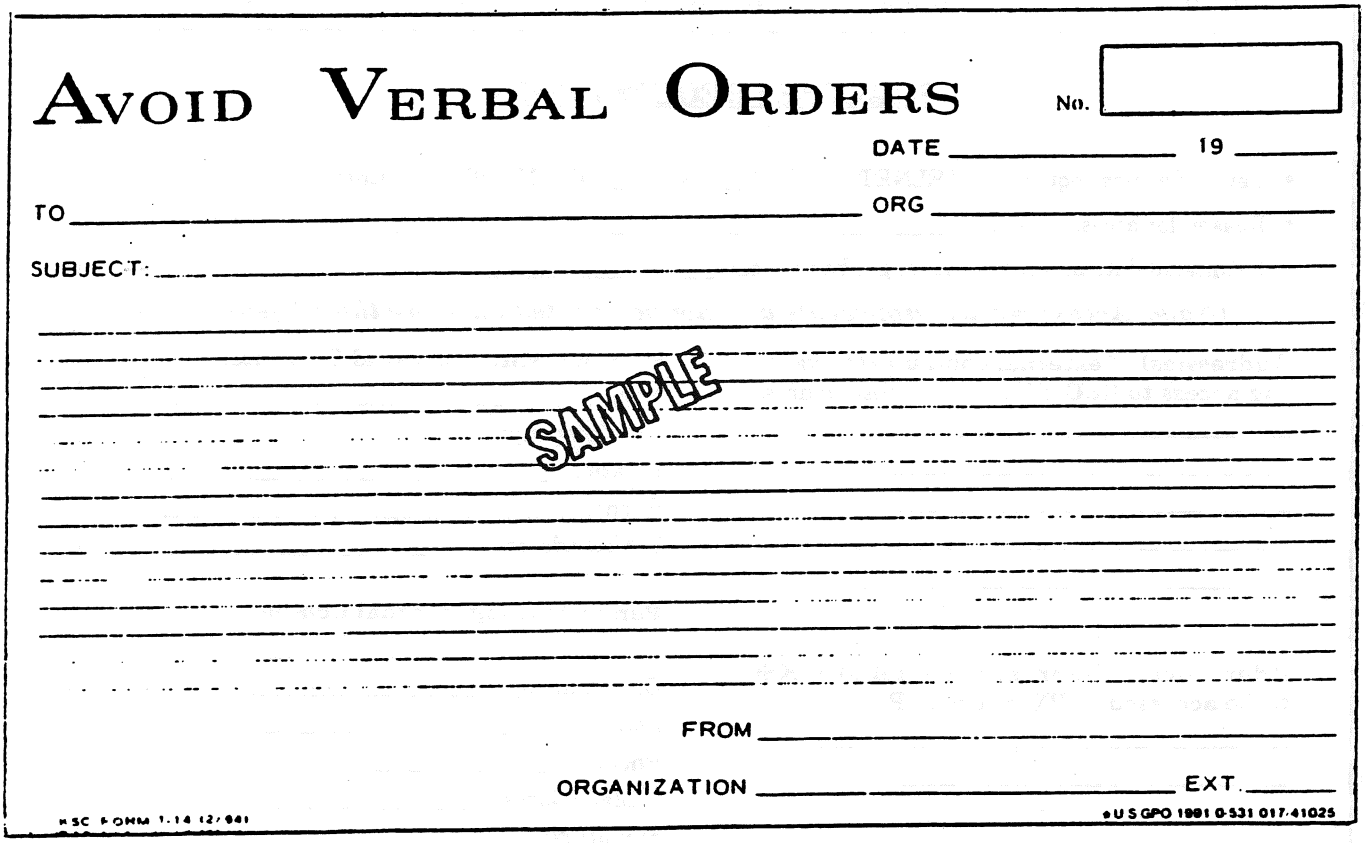
B. _____

C. _____

Return Form To: Help Desk

KSC FORM 31-136 (6/92)

McDonnell Douglas Customer Service Request



AVOID VERBAL ORDERS

No.

DATE _____ 19 _____

TO _____ ORG _____

SUBJECT: _____

SAMPLE

FROM _____

ORGANIZATION _____ EXT. _____

NSC FORM 1-14 12/981

USGPO 1981 0-531 017-41025

Avoid Verbal Orders Form 1-14

ACCESS TO KSC VIA WAN

Access OUT OF KSC is unrestricted, and electronic mail delivery is unrestricted into or out of KSC. TCP/IP Accesses INTO KSC is controlled. SAP advertisements into and out of KSC are controlled. Persons requiring TCP/IP or IPX connectivity to a host within KSC from the outside must obtain the approval of the KSC representative for the area the local host is in. Contacts are:

Network	Form	Network Contact	Mail Code	Phone
PON	CSR	Kevin Billings	F432	867-7302
SODN	KSC Access Request	Michael Seay	TE-COM-2	867-3180
KDN	KSC Access Request	Clark Sims	IM-FCC-B	867-7040
SPDMS II	Support Request	Ken Taylor	LSO-431	861-5405

KSC ACCESS REQUEST FORM

- Level of access requested: TELNET ___ FTP ___ NFS ___ IPX(Novell) ___ Other(list) _____
- Reason for access request: _____
- Estimated date access will no longer be needed: _____

(Note: Access request approvals will not be granted for more than 1 year)

Address(es) of external computer(s) wanting access to KSC if IPX include SAP address

_____
_____
_____
_____
_____
_____

Address(es) of internal computer(s) at KSC to be accessed if IPX include SAP address

_____
_____
_____
_____
_____
_____

Network Contact (from above)

Name: _____
Org/Company: _____
Phone: _____
Signature: _____

M3/PageMaker/usr/customer/T.Gould/KSC Access WAN form

Person Owning External Computer:

Name: _____
Org/Company: _____
Location: _____
Phone: _____
E-Mail address: _____

Person Owning Internal Computer:

Name: _____
Org/Company: _____
Location: _____
Phone: _____
E-Mail address: _____
Signature: _____

COMMENTS:

KSC Access Via WAN Request Form

PLEASE PRINT

PAYLOAD DATA MANAGEMENT SYSTEMS ACCESS REQUEST FORM

1. ☐ NEW USER ☐ ADDITIONAL PRIVILEGES ☐ CHANGE ☐ DELETION

2. USER NAME (LAST, FIRST (NICKNAME)):	3. PHONE: ( )	4. EMPLOYEE NO.:

5. ORIG. DATE:	6. NEED DATE:	7. COMPANY:	8. MAIL STOP / DEPT:

9. BLDG / RM #:	10. CITY, STATE, ZIP (COMPLETE IF NOT ON KSC):

11. CHECK THE APPLICATION REQUESTED:

☐ ADPI	☐ DR LOG 5	☐ LSGMS	☐ OWS	☐ SS ISDB
☐ ALSTAR	☐ EIIS	☐ LSA	☐ PPF	☐ SSMFA
☐ CE	☐ EMPRESS	☐ MFA	☐ POSSE	☐ STMS
☐ CONTRACTS	☐ FAB	☐ MM	☐ POSSP	☐ STS MFA
☐ CABS	☐ GSA/DLA	☐ MMAP	☐ PRACA	☐ TARS
☐ CCN/WRO	☐ IDS	☐ MMC	☐ PROLL/LABOR	☐ TD
☐ CMTS	☐ ISDB	☐ MPA	☐ PRRSS	☐ TTSS
☐ COPA	☐ ISS	☐ NETS	☐ QA	☐ WAD
☐ CPCA	☐ KAPD	☐ OMI	☐ RMRS	☐ WIT
☐ CRAR	☐ LIV	☐ OTS	☐ SI	☐ OTHER _____

12. DESCRIBE FUNCTION YOU NEED TO SUPPORT (REFER TO INSTRUCTION SHEET):

SAMPLE

13. RESPONSIBILITY AGREEMENT:

As a computer user on the computer systems at Kennedy Space Center, I will abide by the following:

1. I will be responsible for my USERID and confidential PASSWORD. This includes setting a unique password that will not be found in a dictionary or that cannot be easily guessed, or that is not personally related to me (make of car or boat, name of family or pets, old addresses, etc...).
2. I will notify Help Desk immediately at 867-1709 if I suspect unauthorized use of my USERID.
3. I will only use my USERID for valid work and required tasks associated with my job.
4. My signature below acknowledges agreement to the above terms.

USER SIGNATURE: _____

14. USER'S SUPERVISOR / MANAGEMENT APPROVAL:	15. PRINT LAST NAME:	16. MAIL STOP	17. USER'S SUPV PHONE: ( )

RETURN FORM TO HELP DESK, F424, Kennedy Space Center, FL 32815 Questions? Call the Help Desk 407-867-1709 BASIC (11/91)

Payload Data Management Systems Access Request Form

USER DO NOT WRITE ON THIS PAGE.

USER SERVICES USE

18. CSR NO.:	19. DATE:

USER ADVOCATE USE

20. USER ADVOCATE SIGNATURE/DATE:	21. PRINT LAST NAME:	22. MAIL STOP:	23. PHONE: ( )
24. DISPOSITION / DATE:			

SYSTEM MANAGER USE

25. USER NAME:	26. INITIAL PASSWORD:	27. DATE/INITIAL
28. ACCOUNT GROUP:	29. UIC:	30. DISK QUOTA:
31. PATHWORK FILE SERVICES:		
32. IDENTIFIERS:		

DATA CUSTODIAN USE

33. SCREENS AVAILABLE/PERMISSION GRANTED

SAMPLE

34. DATE/INITIALS

PV&CC USE

35. SYSTEM: ☐ VAX ☐ MDAC ARTEMIS ☐ SYMBOLICS ☐ SATURN ☐ MARS ☐ CM ARTEMIS ☐ PM ☐ OTHER

36. LIST DESTINATION, USERID, ACCOUNT (HP, ART, SYM, ETC):

DESTINATION	USERID	ACCOUNT

37. MDSSC SESSION NO.:

38. CONTRACTOR / NASA ID:

39. ADMINISTRATION SIGNATURE/DATE:	40. ADMINISTRATION SIGNATURE/DATE:

41. COMMENTS:

Payload Data Management Systems Access Request Form (cont)

PDMS USER ACCESS instructions:
Please print all information except for signatures

#1 - Indicate the type of request. For example, if you are already a user and need access to other applications, check additional privileges. For name changes or transfers, check the change box.

#2.- Enter your last and first name.

#3.- Enter your telephone number - include area code.

#4.- Employee number (McDonnell Douglas only - all others use your company name).

#5.- Today's date.

#6.- Need date. Enter date that you require access to PDMS data.

#7.- Your company name, MDSSC, NASA, etc.

#8.- Your mail stop or mail code.

#9.- Building identifier and your room number.

#10.-Your location.

#11.-Check the application(s) for which you need access.

#12.-Provide a brief description of your job responsibilities;i.e., will your need to read or modify data.

#13.-Please read the agreement and sign as indicated.

#14.-Signature approval from your supervisor or manager.

#15.-Print last name of supervisor or manager.

#16.-Supervisor's or manager's mail stop or mail code.

#17.-Supervisor's or manager's telephone number. If not located at Kennedy Space Center, please include area code.

Forward the form to Technical Support, User Services Help Desk, F424. The form is then approved by the application user advocate and upon approval is processed by Technical Support.

If you need to request hardware, software or other technical support to provide connectivity, please complete the attached Communcations Service Request (CSR) and submit it with the access form to User Services.

Payload Data Management Systems Access Request Form (cont)

SHUTTLE PROCESSING DATA MANAGEMENT SYSTEM
ID SUPPORT REQUEST FORM

SECTION 1. USER INFORMATION

___New Userid Request ___Modify Existing Userid Request

Date:_____ Userid To Be Modified_____
(Applicable Only If Box 2 Selected)

First Name | MI | Last Name

Preferred 1st Name | Lockheed Employee Number | Agency /CO

Department | Mail Stop | Telephone Number | Extension

NASA Center | Building | Room

Business Address

City | State | Zip

SECTION 2. SYSTEM PROFILE INFORMATION

Userid_____ (Applicable Only If This Is Not A New Request)

Individual_____ Center_____ (Check One Only)

ONG CODE_____ CIR CODE_____

ACTION (A.M.D.)	MODE	USER CLASS	VIRTUAL STORAGE	DASD MEGABYTES REQUIRED	VIRTUAL ADDRESS

CHECK LIST: MOU COMPLETED____ TRAINING COMPLETION CERTIFICATE____

SECTION 3. APPROVAL SIGNATURES

CENTER LEAD | DATE | SYSTEM ADMINISTRATOR | DATE

RESOURCE COORDINATOR | DATE | SECURITY ADMINISTRATOR | DATE

DO NOT WRITE IN THIS SPACE

USERID | PROFS NICKNAME | CONTROL NO.

USER NOTIFIED_____DATE_____WORK COMPLETE_____DATE_____

Shuttle Processing Data Management System ID Support Request Form

MEMORANDUM OF UNDERSTANDING
SFDMS II PERSONAL USER ID

To: Shuttle Data Systems Security Administrator

Subject: Personal User ID

I am requesting a personal user ID to access the SFDMS II computer system.

I understand that this is a personal user ID for my use exclusively. I accept responsibility for security of the ID and password and I will be accountable for all use of my user ID.

I understand that the computer resources I will have access to are provided to support my Government and/or contractor job function only. Any use of these computer resources unrelated to my job function is a violation of Federal Statutes.

THESE COMPUTERS ARE OPERATED BY/FOR THE UNITED STATES GOVERNMENT. UNAUTHORIZED ACCESS TO AND/OR USE OF THESE COMPUTER SYSTEMS IS A VIOLATION OF LAW AND PUNISHABLE UNDER THE PROVISIONS OF 18 USC 1029, 18 USC 1030 AND OTHER APPLICABLE STATUTES.

SAMPLE

_____
Requester Name (please print)

_____ _____
Requester Signature Date

_____
Resource Coordinator Name (please Print)

_____ _____
Resource Coordinator Signature Date

T-1 Service Request

Fill out, attach to a Support Request, and forward to Mail Stop: LSO-095 for processing and implementation.
(See reverse side for instructions.)

Originating Equipment

1. Equipment Type

Mfg. Name | Unit Type | Model No.

2. Equipment Location | 3. Equipment Layout (attach sketch)

Building No. | Room No.

4. Customer Identification

Name | Org. | Mail Code | Phone No.

5. Communications With:

SAMPLE

6. Bit Rate Required

7. Timing Required
☐ Network (default) ☐ DTE

8. Electrical Interface Required
☐ V.35 ☐ RS-449 ☐ DS-1

9. If DS-1, Line Code Required
☐ B8ZS (Default) ☐ AMI

10. If DS-1, Framing Required
☐ ESF (Default) ☐ SF ☐ Proprietary ☐ Unframed

Terminating Equipment

11 Equipment Type

Mfg. Name | Unit Type | Model No.

12. Equipment Location | 13. Equipment Layout (attach sketch)

Building No. | Room No.

14. Customer Identification

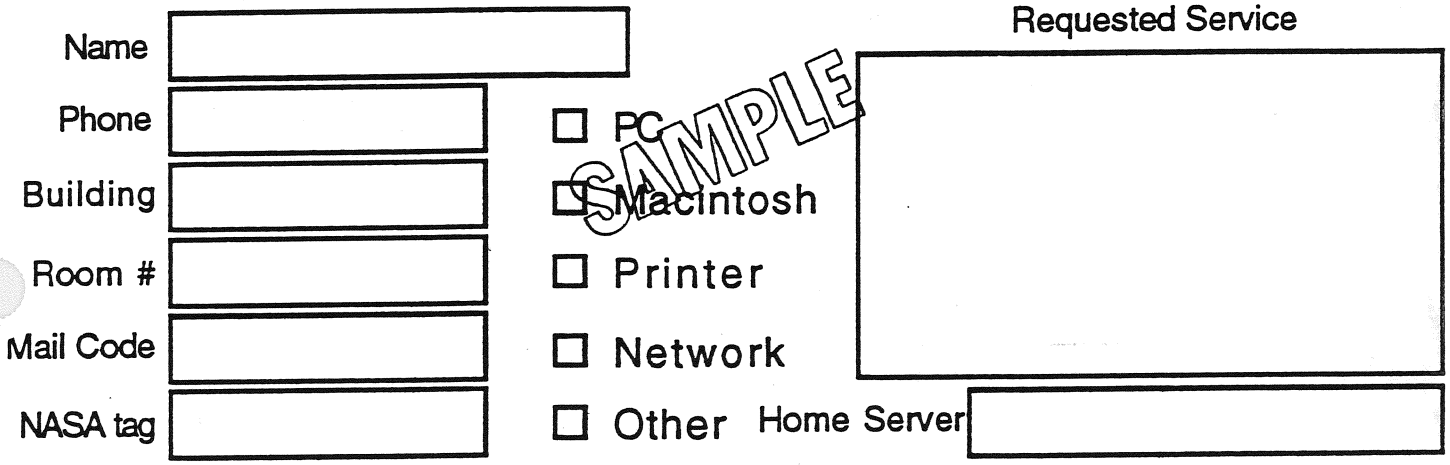
Name | Org. | Mail Code | Phone No.

Requestor Responsibilities

1. Ensure that adequate AC power receptacles are available to power up the equipment.
2. Provide cables from equipment to the CSU or CSU/DSU (LSOC Communications will provide the CSU/DSU or CSU for customer T-1 connection). Note: The cable end interfacing the CSU/DSU or CSU must have a male connector.
3. Reference OMRSD 80K55452 for a description of the T-Carrier System and its performance specifications.

KSC FORM 29-617 NS (6/93)

T-1 Service Request Form



Please Email form to User Help as found in your ElectronicMail address book. If someone has not been in touch about this call within 24 hours please call 7-2334.

DE-IECS Support Request Form