

AD-A173 472

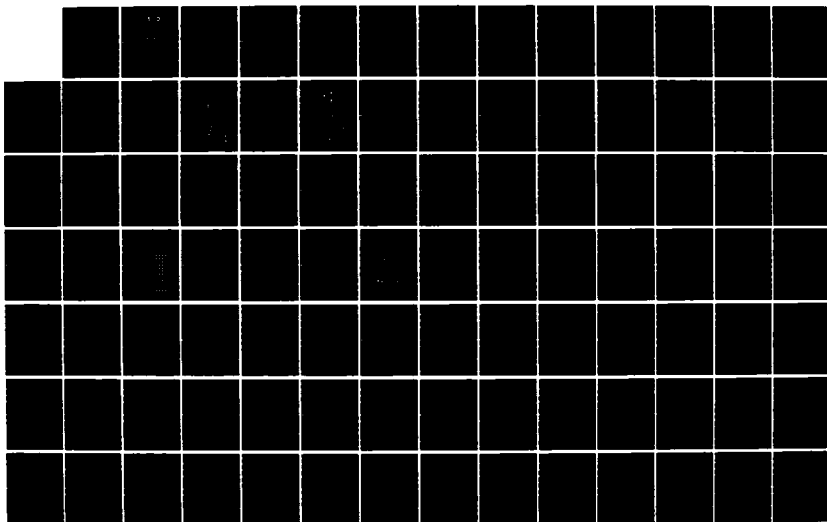
THE DDN (DEFENSE DATA NETWORK) COURSE(U) NETWORK
STRATEGIES INC FAIRFAX VA R DE VERE ET AL. APR 86
DCA100-83-C-0062

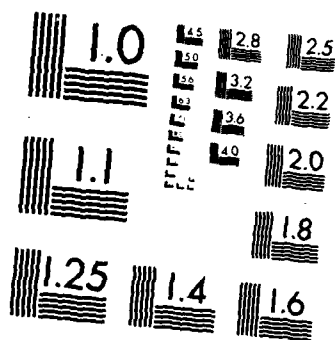
1/4

UNCLASSIFIED

F/B 17/2

NL





MICROCOPY RESOLUTION TEST CHART
NATIONAL BUREAU OF STANDARDS-1963-A

AD-A173 472

1

DTIC
ELECTE
OCT 20 1986

S D

THE

DDN

COURSE

Contract DCA-100-83-C-0062

Network Strategies, Inc.
10201 Lee Highway
Fairfax, Virginia 22030

Approved for Public Release, Distribution
Unlimited.
Per Mr. John Jasper, DCA/Code B630

DTIC FILE COPY

APRIL 1986

86 10 15 008

THE DDN COURSE

Prepared for:

Defense Data Network
Program Management Office
Defense Communications Agency

April 1986



Prepared by:

Network Strategies, Inc.
10201 Lee Highway
Fairfax, Virginia 22030

This document has been approved
for public release and sale; its
distribution is unlimited.

Accession For	
NTIS CRA&I	☒
DTIC TAB	☐
Unannounced	☐
Justification	
By <i>per phone call</i>	
Distribution	
Availability Codes	
Dist	Availability or Special
<i>A-1</i>	

TABLE OF CONTENTS

PURPOSE, OBJECTIVES, OVERVIEW OF COURSE

I. FUNCTIONAL REQUIREMENTS FOR DATA COMMUNICATIONS

1.	Historical Perspective: Data Networks	1-1
A.	Early Networks	1-1
B.	Switched Telephone Network	1-1
C.	Evolution of Computer Communication Networks ...	1-2
D.	Components of Typical Data Communication Systems	1-4
E.	Local Area Networks - LANs	1-7
F.	Switched Network Services	1-8
2.	Switching Techniques	2-1
A.	Circuit Switching	2-1
B.	Message Switching	2-3
C.	Packet Switching	2-5
D.	Basics of Packet Switching Networks	2-7
E.	Packet Switching Services	2-11

II. COMPUTER NETWORK ARCHITECTURES

3.	Introduction and Concepts	3-1
A.	The Need for Network Architectures	3-1
B.	A Natural Layering of Network Functions	3-2
C.	Definition of a Computer Architecture	3-4
4.	Description and Comparison of Major Network Architectures	4-1
A.	SNA	4-1
B.	DECnet (DNA)	4-5

C.	OSI	4-10
E.	The DoD Approach to Internetworking	4-15
F.	Comparison of the Major Computer Network Architectures	4-18
G.	The Future of Computer Network Architectures	4-19

III. THE DEFENSE DATA NETWORK AND THE DoD PROTOCOL SUITE

5.	The Defense Data Network - Overview	5-1
A.	Introduction to the DDN	5-1
B.	DDN Packet Routing Technique	5-5
C.	DDN Packet Switching Devices	5-10
D.	Network Access Devices for the DDN	5-16
E.	Network Monitoring	5-24
6.	DDN System Performance	6-1
A.	Survivability	6-1
B.	Availability	6-2
C.	Transmission Quality and Bit Error Rate	6-3
D.	Network Delay	6-3
7.	Security	7-1
A.	Security Services	7-1
B.	DDN Security Mechanisms.....	7-2
8.	The DoD Protocol Suite	8-1
A.	DDN Access Protocols - Layers 1 through 3	8-1
B.	Internet Protocol (IP).....	8-10
C.	Internet Control Message Protocol (ICMP)	8-14
D.	Transmission Control Protocol (TCP).....	8-16
E.	Telnet Protocol	8-19
F.	File Transfer Protocol (FTP).....	8-22
G.	Simple Mail Transfer Protocol (SMTP).....	8-25
H.	Gateway Protocols	8-27

IV. THE DDN: STRATEGIES FOR SUBSCRIBERS

9.	Levels of DDN Interoperability	9-1
A.	Definitions	9-1
B.	DDN Host Interfaces.....	9-2
10.	Special Topics in DDN Interconnection	10-1
A.	Polled Terminal Protocols and Full Screen Applications on the DDN	10-1
B.	Connecting Subscriber Local Area Networks to the DDN	10-6
C.	Personal Computers on the DDN	10-10
D.	Subscriber Network Monitoring Systems on the DDN	10-14
11.	Administrative Issues for DDN Subscribers	11-1
A.	Qualification Testing	11-1
B.	Host Site Responsibilities	11-2
C.	Node Site Responsibilities	11-3
D.	Ordering DDN Service	11-7
E.	Using the NIC	11-13

APPENDIXES

DDN Interface Vendor Summaries	A-1
Protocol Headers	B-1
Glossary	C-1

Daily Course Schedule

	Day 1	Day 2	Day 3
9:00-10:00	1	5 6	11
10:00-11:00	2	7	
11:00-12:00	3	8	
12:00-13:00	Lunch Break	Lunch Break	Lunch Break
13:00-14:00	3	8	Discussion
14:00-15:00	4	9	
15:00-16:00	5	10	

The Instructors

Rosemary De Vere

Ms. De Vere, Staff Consultant, Network Strategies, Inc., has expertise in the design, implementation and technical support of data communications networks. Currently, she provides host systems support to subscribers transitioning onto the DDN. She previously held positions at Tymnet, Inc. where she provided technical support for a multi-million dollar private data network for a major Federal government agency and at SESA-Honeywell Communications, Inc. where she was involved in telecommunications documentation development. Ms. De Vere holds a B.A. in French from the City University of New York and an M.A. in Intercultural Communications from the Monterey Institute of International Studies.

Mark S. LaRow

Mr. LaRow, Consultant, Network Strategies, Inc. specializes in the areas of communications network design and management. He has recently been involved in the design and implementation of a nationwide voice/data T1 network and has extensive experience in the implementation of X.25 packet switching networks and DTS systems. Previously, he was a systems engineer with the Hughes Aircraft Company where he was involved in the design of communication satellite systems. Mr. LaRow is an instructor for a the Systems Technology Forum seminar company, teaching courses on T1 Networking and Introduction to Data Communications. He is also a frequent speaker at national conferences on Network Design and Network Management. Mr. LaRow received his MS and BS degrees in electrical engineering from MIT.

Kenneth A. Napier

Mr. Napier, Staff Consultant, Networks Strategies, Inc. provides network design, implementation, and technical evaluation to the Defense Communications Agency Defense Communications System Data Systems. His experience includes network modeling and the design and implementation of a major microcomputer based Local Area Network. Previously, he was a systems analyst with the Sperry Computer Systems Company where he assisted in the design, test and implementation of a large secure data communications network including network load modeling, evaluation and problem analysis. While assigned at a DoD agency he has taught network operations and programming languages to clients. Mr. Napier has completed course work towards a Bachelor of Science degree in Computer Science.

L. David Passmore

Mr. Passmore, Group Manager Network Architectures and Protocols, Network Strategies, Inc., provides consulting assistance to commercial and government clients in network design, computer network architectural issues, networking standards, and strategies for integration of corporate network facilities. He has previously held positions with Deal and Associates and the Mitre Corporation. Mr. Passmore is an instructor for the Systems Technology Forum seminar company, teaching courses on IBM's SNA, Network Protocols and Standards, and X.25. He holds both BS and MS degrees in Computer Science and Engineering from the Massachusetts Institute of Technology.

OVERVIEW OF COURSE

A. Purpose

- ✓ The purpose of this course is to provide the DDN user community with sufficient technical and program information to enable the users to obtain effective data communications service through the DDN and to meet DoD interoperability requirements.

B. Objectives

The specific objectives which have been established to accomplish this purpose are to instruct the student in:

- 1) The technical evolution of data communication networking from simple data networks up to the level of modern integrated computer network architectures so that he will be able to take full advantage of the services offered by the DDN.
- 2) The characteristics of the DoD network architecture and several major commercial network architectures so that the student has a consistent framework with which to determine the architectural changes required by connection to the DDN and DoD interoperability.
- 3) The level of computer interoperability required by the DoD and the importance of the DoD protocol suite in achieving interoperability, so that the student can implement systems which meet these requirements.
- 4) The importance of the DDN in providing communication services to the DoD community and providing cost savings of communications lines.
- 5) The importance of the DDN dynamic routing algorithm in providing survivability of the network, particularly during conditions of stress.

- 6) Network components, their functions, and the monitoring capabilities provided by the network Monitoring Center so that the student knows the equipment the network provides, how that equipment is monitored, and procedures to follow for getting network related problems resolved.
- 7) Performance objectives of the DDN architecture to enable the subscriber to configure his network connection to meet his system's requirements.
- 8) Levels of security which will be provided by the DDN and the time frame for their implementation so that the student can begin planning the migration of his secure network to the DDN.
- 9) The key functional aspects of the DoD protocol suite so that the student will understand the implications of his alternatives in terms of the software needed to connect his system to the DDN and to make it interoperable with other systems on the DDN.
- 10) Major interfacing issues concerned with connecting DoD systems to the DDN such as:
 - The different levels of interoperability obtainable through the DDN
 - Accommodating Local Area Networks and personal computers on the DDN and into the DoD architectureso that the student will be able to chose the best interface for his system.
- 11) The procedures and time frame required to obtain DDN service to enable the student to initiate each step at the appropriate time so that all parties are prepared to complete the connection.
- 12) Using the Network Information Center so that the subscriber can make effective use of this network resource.

C. Course Organization:

1) Overall Course Organization

The Course is organized into four sections:

- I. Functional Requirements for Data Communications ;
- II. Introduction to Computer Network Architectures ;
- III. The Defense Data Network and the DoD Protocol Suite ;
- IV. The DDN: Strategies for Subscribers .

2) Section I - Functional Requirements for Data Communications

Chapter 1 — Describe the background of the use of communications by computing devices — starting with simple host to host batch transmission and leading to interactive transactions between terminals and hosts.

Chapter 2 — Describe the three basic switching techniques employed in communications networks — circuit switching, message switching, and packet switching. Describe the special characteristics and advanced features available with packet switching networks.

3) Section II - Computer Network Architectures

Chapter 3 — Introduce the concept of a computer network architecture and describe the layered approach for defining an architecture.

Chapter 4 — Describe and compare several major network architectures used in industry and in the DoD. Describe the future directions of these major network architectures. Describe the technique used to support internetworking in the DDN.

4) Section III - The Defense Data Network and the DoD Protocol Suite

- Chapter 5 — Describe the mission of the Defense Data Network and its general hardware architecture and packet routing technique.
- Chapter 6 — Describe the DDN's network performance objectives.
- Chapter 7 — Describe the security architecture of the DDN.
- Chapter 8 — Introduce and describe the functionality of each element of the DoD protocol suite.

5) Section IV - The DDN: Strategies for Subscribers

- Chapter 9 — Describe the levels of interoperability obtainable through the DDN and the DoD protocol suite.
- Chapter 10 — Address special topics concerning "polling terminal protocols", local area networks, the use of personal computers, electronic mail, and subscriber network monitoring systems on the DDN.
- Chapter 11 — Describe the process through which a potential subscriber obtains service on the DDN.

SECTION I

FUNCTIONAL REQUIREMENTS FOR DATA COMMUNICATIONS

OBJECTIVES
OF
FUNCTIONAL REQUIREMENTS FOR DATA COMMUNICATIONS

- **To understand the technical evolution of data communication networking from simple data networks up to the level of modern integrated computer network architectures so that the student will be able to take full advantage of the services offered by the DDN.**

1. Historical Perspective: Data Networks

A. Early Networks

Two of the earliest American data communications networks were:

- 1) Pony Express
- 2) Telegraph lines

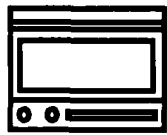
These are examples of message switched networks. Message switching and switching in general will be discussed in a later chapter of this Section.

B. Switched Telephone Network

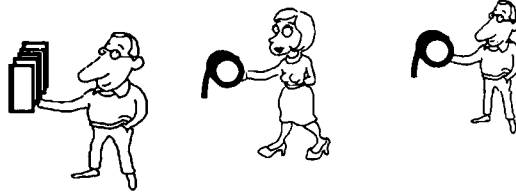
The first telephone networks were ones in which each telephone set was connected to all other telephone sets via a pair of wires. It quickly became apparent to early telephone users that these direct connections between phones were impractical as $n \cdot (n-1)/2$ lines are required to interconnect n phones. Hence, a telephone network based on phone company switching centers evolved:

- 1) A.G. Bell invents the telephone - 1876.
- 2) Installation of first switching office in New Haven, CT - 1878.
- 3) Interconnection of the local switching offices with each other provides the any-phone to any-phone connectivity we have today.

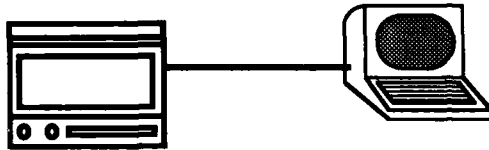
Computer Network Evolution



Host
Computer

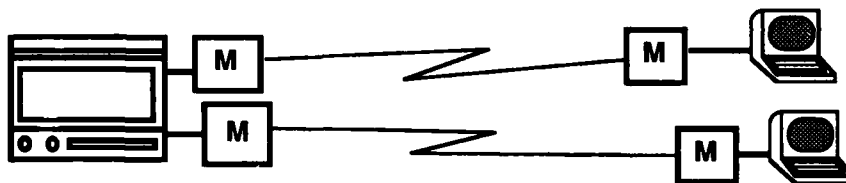


50's
Batch



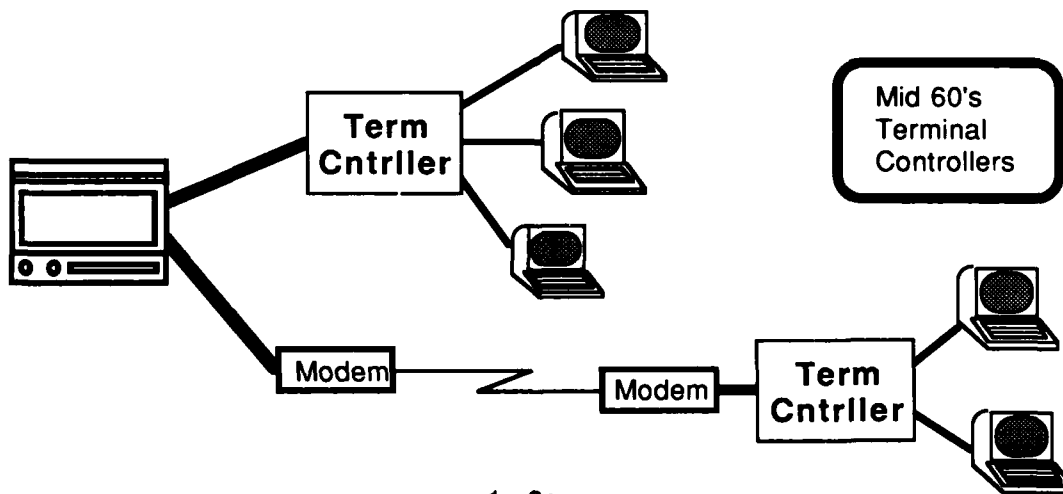
Host
Computer

Early 60's
Interactive



Host
Computer

Mid 60's
AT&T's 103 modem



Mid 60's
Terminal
Controllers

C. Evolution of Computer Communication Networks

Initially, nearly all communications systems were developed to support the growing demand for *voice communications*. As such, networks and transmission facilities were not available to support the specific needs of computer communications. Instead, *computer communications had to be adapted* to be compatible with the characteristics of voice communications.

Beginning in the 1960's computer communications became an important factor in many organizations which then spurred the common carriers and other vendors to develop *specialized communications services and networks designed specifically for data communications*. Nowadays, computer networks need not be constrained by the limitations caused by use of existing voice networks.

1) 1950's

The first computers operate in local "batch job" environment utilizing punch cards, magnetic tape, or paper tape to input data from a user. Interactive communications is not yet widely used and so there is not a great demand for data communications.

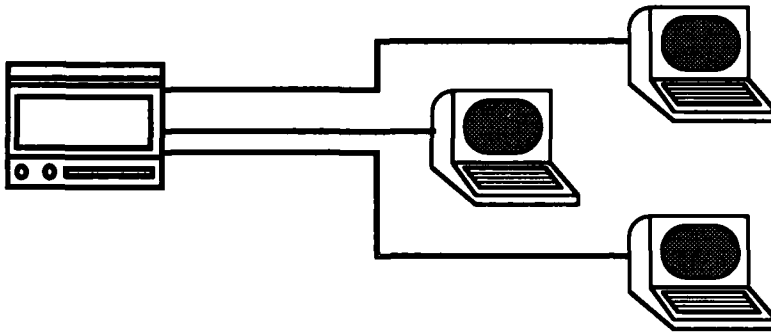
2) Early 1960's

Local interactive communication between terminals and computers come into much greater usage, but the number of terminals that can be connected to a computer is limited and thus there still is not a great demand for data communications.

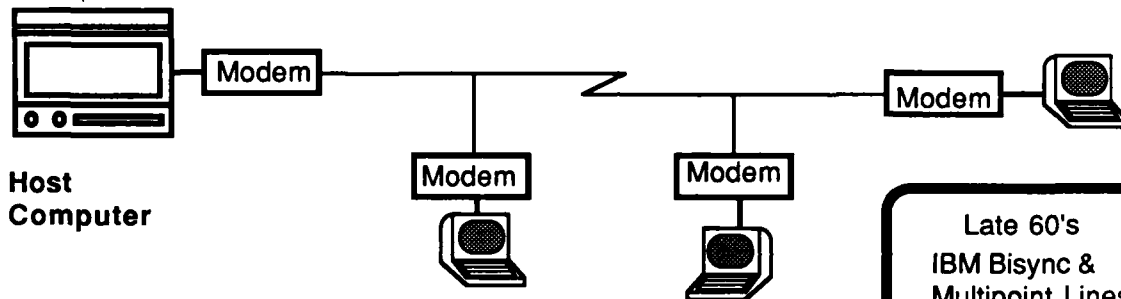
3) Mid 1960's

- a) AT&T introduces the AT&T 103 modem, providing low speed dial-up connections for data communication.
- b) With the development of synchronous terminals, computer vendors develop terminal controller devices that allow a greater number of terminals to access the computer through fewer communications ports. These terminal controllers can be used as "communications concentrators", which allow many terminals to use the same communication circuit.

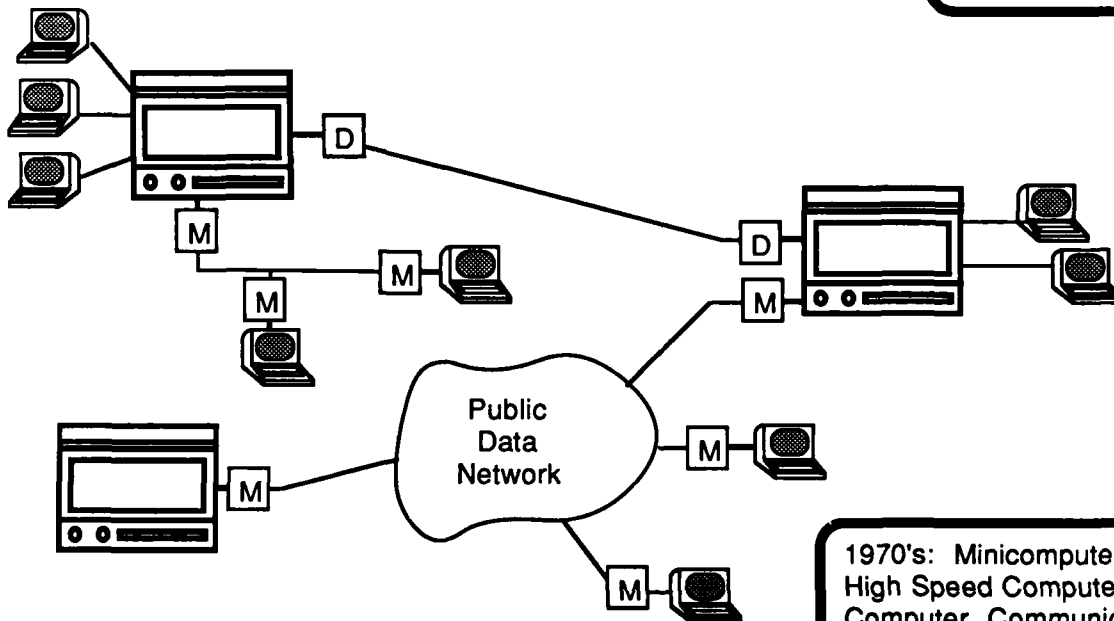
Computer Network Evolution



Late 60's
Timesharing



Late 60's
IBM Bisync &
Multipoint Lines



1970's: Minicomputers
High Speed Computer -
Computer Communication

4) Late 1960's

- a) Low speed time-sharing interactions between simple interactive terminals and host computers becomes widely available to many computer systems. The ability to connect a large number of terminals to a computer spurs a large demand for remote access capabilities, and thus telecommunications vendors begin introducing products to allow this access.
- b) IBM introduces the Binary Synchronous Communication protocol (Bisync or BSC). Multipoint connections become possible, thus making data communications between a computer and many terminals more cost effective.

5) 1970's

Localized use of versatile and inexpensive minicomputers becomes widespread. The desire to share files and processing power between many computers within an organization drives the development of *high speed computer to computer communications* networks utilizing new all-digital communication facilities and specialized data networks.

D. Components of Typical Data Communication Systems

There are three basic component groups in typical data communications systems:

- Transmission Facilities
- Data Circuit-Terminating Equipment - DCE
- Data Terminating Equipment - DTE

The DTE are the devices which generate or terminate data. The transmission facilities transport the data from one location to another, and the DCE provide the interface between the DTE and the transmission facilities.

1) Transmission Facilities (Circuits)

a) Switched Circuits or Dedicated Circuits

- Switched circuits are those which require the dialing of a telephone number in order to establish a connection.
- Switched circuits allow a user to establish connections to many different locations just as telephones can be connected to any other telephone in the telephone network.
- Dedicated circuits are *always* connected and thus never require the dialing of a telephone number.
- Dedicated circuits generally provide a higher quality transmission path and thus higher data rates can be supported than with switched circuits.
- Dedicated circuits can be point-to-point or multipoint

b) Analog and Digital Circuits

- Analog Circuits are designed to transmit analog signals such as voice conversations.

- The majority of data networks in CONUS are comprised of analog circuits since they are so widely available and relatively inexpensive.
- Data can be transmitted over an analog facility by first converting the data into an "equivalent" analog signal through a process called **modulation**.
- Digital circuits are special communications circuits which can transmit data in digital form. This eliminates the need to convert the data to an equivalent analog signal.
- Most common carrier digital circuits require a circuit interfacing device to adjust the data signal into the correct format for transmission.
- Digital circuits generally provide a *higher quality transmission* path for data than analog circuits.
- The DDN uses 56 Kbps digital circuits to provide very high speed data transport between subscribers' host systems and their DDN access points.

c) Transmission Media

- Twisted Pair
- Coaxial Cable
- Satellite Circuit
- Fiber Optics
- Microwave Radio

2) Data Circuit-Terminating Equipment

- **Modem** (MOdulator - DEModulator) This device converts *digital signals* to analog form suitable for transmission over *analog circuits*, and reconverts them back to digital form at the destination.

A modem is required at each end of an analog communications circuit.

- **DSU / CSU** (Data Service Unit / Channel Service Unit) This device converts *digital signals* to the proper format for transmission over *digital circuits*.

DSU's are required at each end of a digital communications circuit.

3) Data Terminal Equipment (DTE)

Any digital device where data is generated or terminated.

a) Host computers

b) Terminals

c) Front End Processor (FEP)

- Specialized computer used to offload communication duties from host processor(s).
- Provides speed buffering, serial / parallel conversions, circuit handling, and implements the communication protocols.
- Often performs network control.

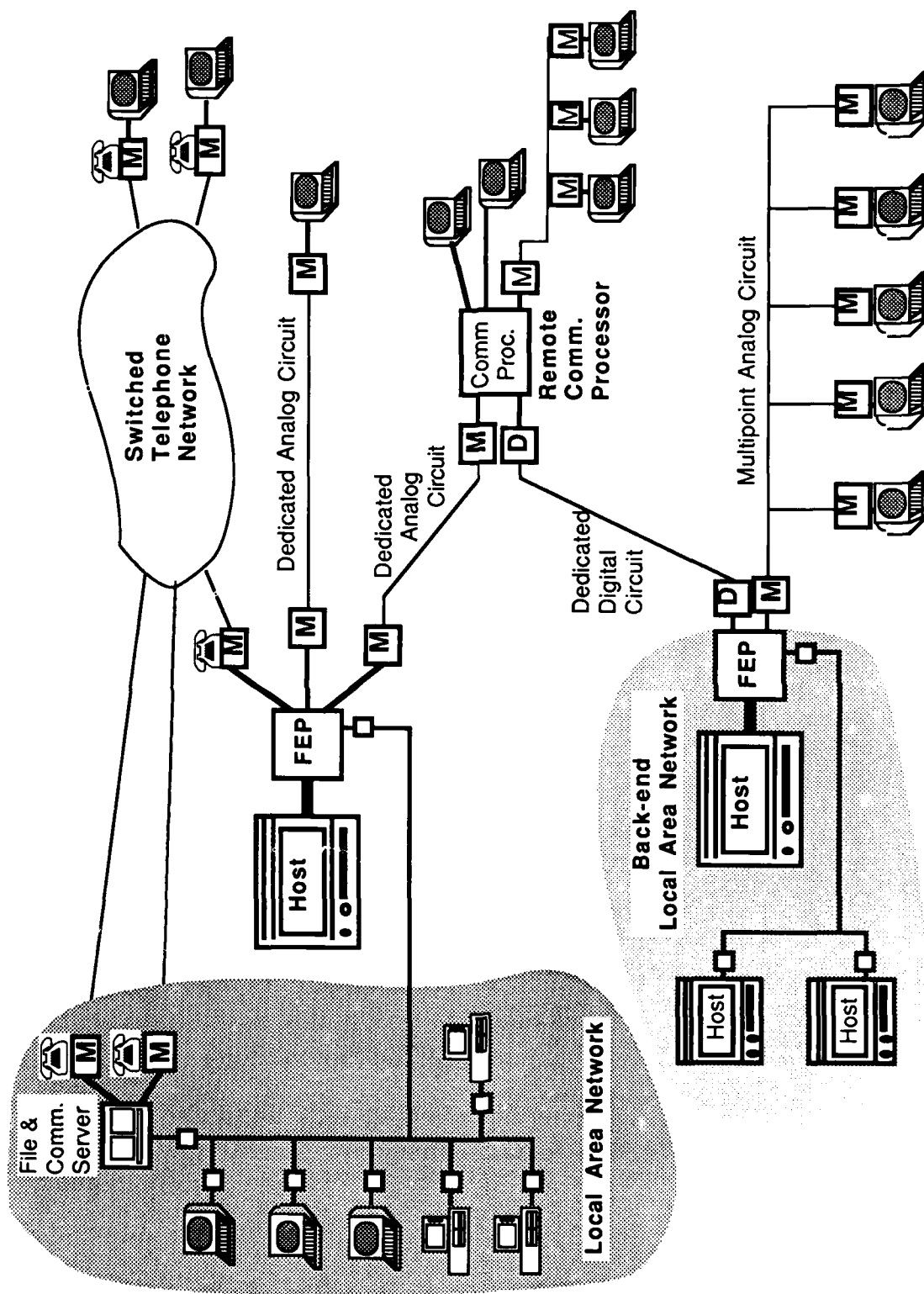
d) Multiplexers

These devices combine several low-speed communication channels onto one high-speed channel. Multiplexers decrease the number of communications circuits required to connect a given number of terminals to the host.

e) Remote Communication Processor (Concentrator)

This is a specialized computer dedicated to performing communication functions such as circuit, packet, or message switching and channel concentration remotely.

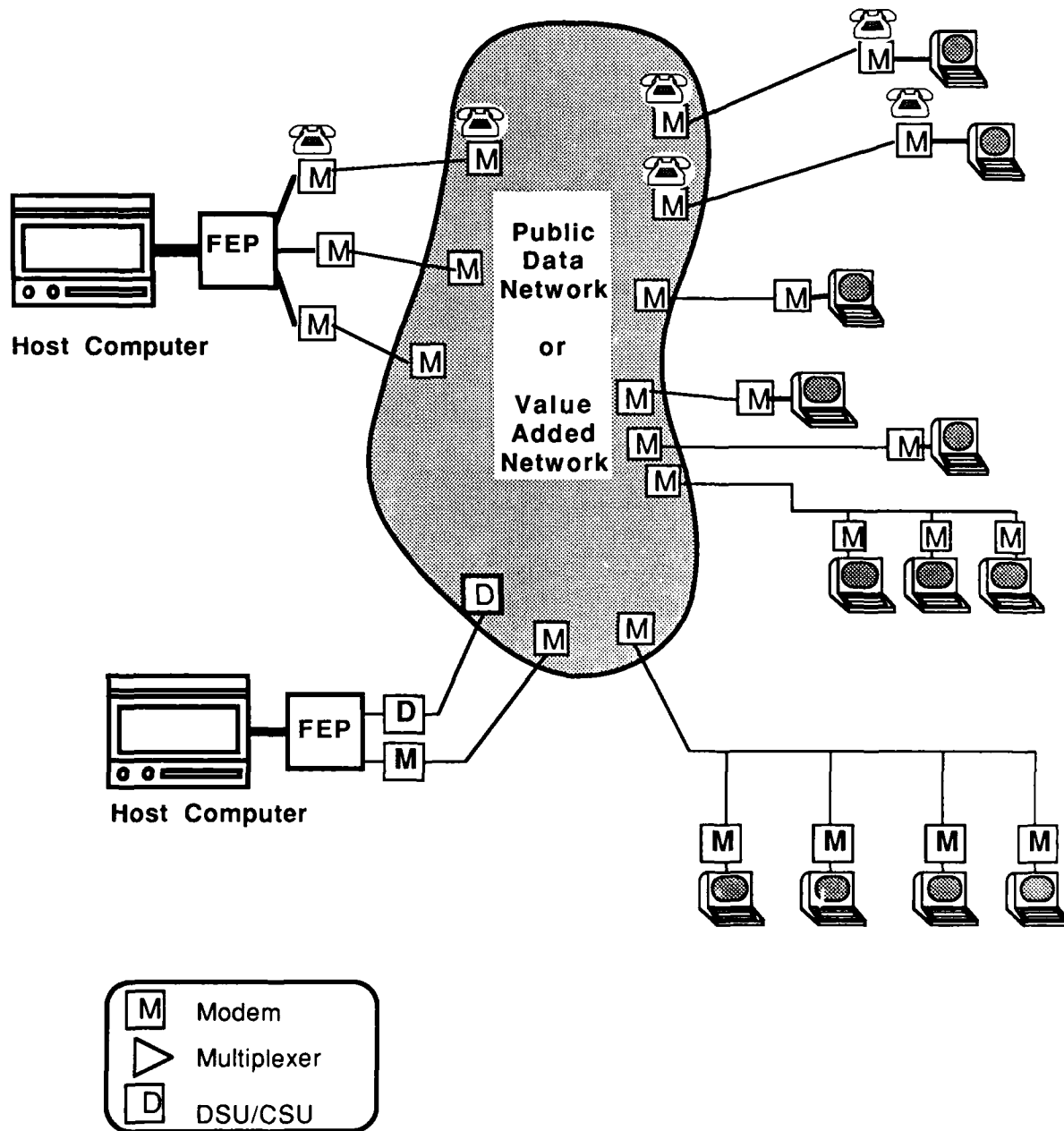
Data Communication System



E. Local Area Networks - LANs

- Used to connect many devices together which are separated by limited distances — typically within a building or within a campus area such as a military base.
- LANs reduce wiring and cabling by having the LAN be composed of a single transmission medium which all users share.
- LANs support high data rates - typically greater than 1 million bps.
- *Front-end LAN* used to connect many terminals to the host computer via a single communications medium.
- *Back-end LAN* used to connect several computers together
- *Office automation LANs* connect personal computers and word processors together so that they may exchange files, share communications circuits on a contention basis, and share high capacity disk drives.
- LANs are composed of:
 - Transmission medium — coaxial cable or twisted pair wires,
 - Access Devices — devices which allow DTE to access the shared communication medium.
- Devices on an LAN can be connected to a modem to dial out through the public switched network through use of a "communications server" on the LAN.
- Devices on an LAN can be made to look like devices on another network through use of *gateways*.

Data Communication System



F. Switched Network Services

1) Public Switched Telephone Network (PSN)

The switched telephone network has the ability to connect various data communicating equipment together through the standard telephone network just as it connects telephones together for voice transmission.

2) Public Data Networks and Value Added Networks (PDNs and VANs)

PDNs and VANs have the same *interconnectivity* capabilities as the switched telephone network with the *added benefits for data networking* in that they can provide error-free data transmission, faster data rates, as well as various other intelligence functionality for a lower cost than the switched telephone network.

A PDN/VAN can be used as an "extension cord replacement" for existing dedicated circuit networks since the performance and services available on PDN/VANs can exceed those of dedicated circuit networks.

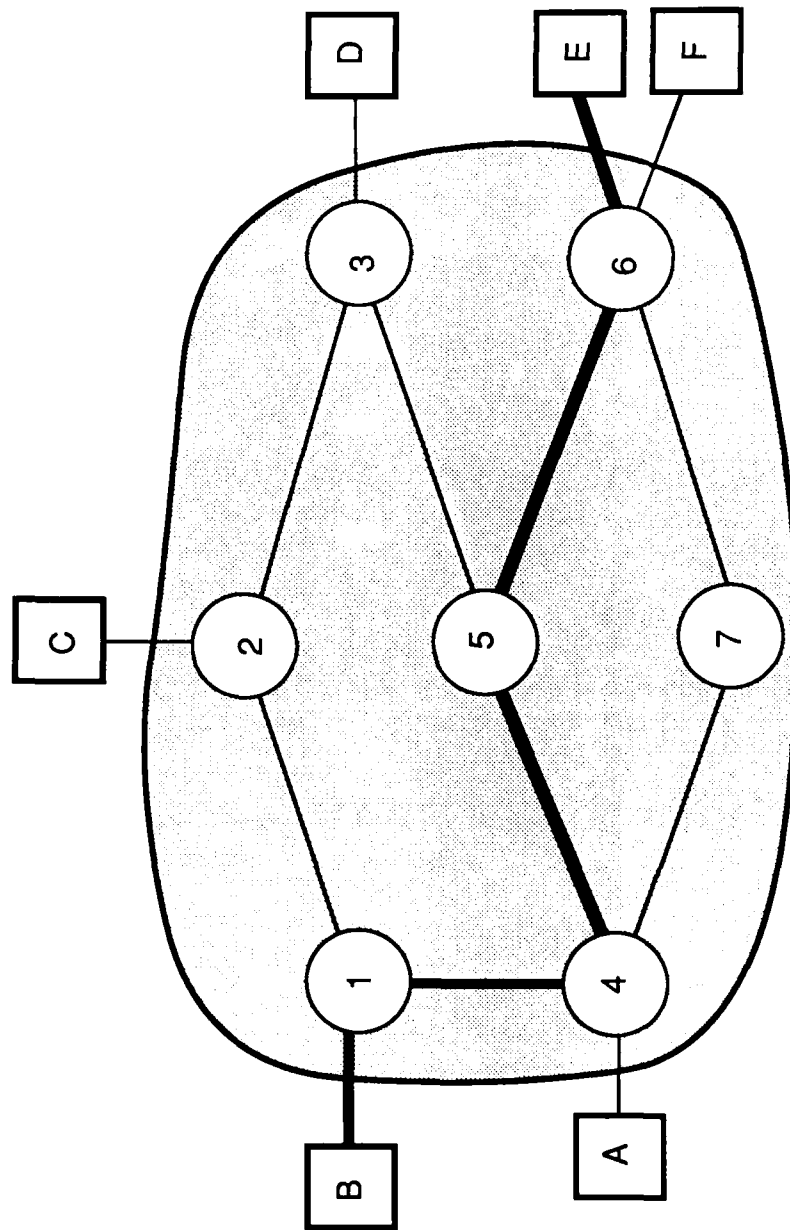
a) PDNs — Public Data Networks

- These networks are similar to the switched telephone network in functionality except that they are used to switch data "circuits" instead of voice circuits.
- Public "packet switching networks" and the european "X.21 circuit switched networks" networks are examples of PDNs.

b) VANs — Value Added Networks

- A VAN is considered to be any network (e.g. a packet switching network) that provides "added-value services" above and beyond "basic" data transportation.
- Added value services may include protocol conversion, code conversion, speed conversion, electronic mail, or security.
- Examples of packet switching Value Added Networks are: Tymnet, Telenet, and the DDN.

CIRCUIT SWITCHING



Call Connecting B to E

Note that A cannot call B, C, D or E until call is terminated

2. Switching Techniques

There are three commonly used techniques of switching that can be used to route information from one point to another. They are: Circuit Switching, Message Switching, and Packet Switching.

Each technique is suited for a particular type of communication.

A. Circuit switching

- Circuit switching is the oldest form of switching and is the method used in the public telephone network.
- Circuit switching entails the establishment of a temporary dedicated physical link (either physical wires or dedicated bandwidth on a multichannel communication link) between two communicating parties.
- Upon termination of the call the dedicated link is *dismantled* and the *resources are made available to other users*.
- Circuit switching is best suited to an environment of infrequent call establishment with short call hold times; e.g., a standard voice phone call.
- A data communications session is characterized by very long call hold times (i.e., terminals remain connected to a computer all day) and thus this technique is not cost effective for data communications.
- Switches are either electromechanical (e.g., Strowger switch, key system, Crossbar) or digital electronic (e.g., 4 ESS, 5 ESS)

1) Functionality of Circuit Switching Systems

- a) Call Establishment — Creation of the dedicated physical path from source to destination. Telephone number provides destination information to circuit switches.
- b) Transfer of Information — All information traverses the physical route that was set up during call establishment.
- c) Call Termination — All circuits freed upon call termination so that they can be used for other calls

2) Advantages of Circuit Switching Systems

- Simplest technique to implement in a switch
- Most cost effective switching technique for light, intermittent loads
- Least delay through the network once circuit established; fast enough for interactive use
- Transparent to data as no protocol or header format is required

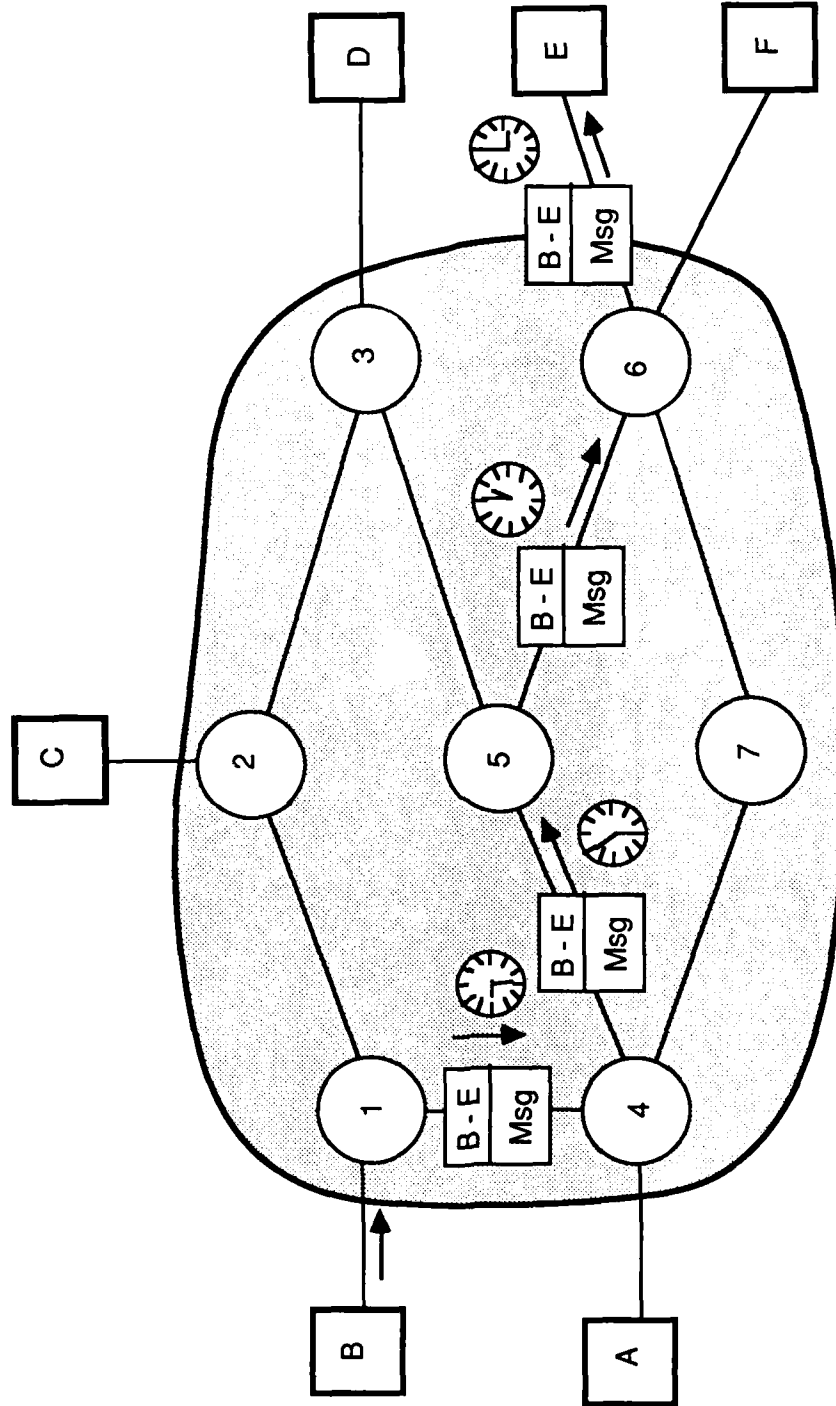
3) Disadvantages of Circuit Switching Systems

- Inefficient use of the network's available bandwidth as the entire capacity of the channel is dedicated for the duration of the call
- Fairly large setup delay

4) Examples

- Public Telephone Network
- Autovon

Message Switching



Message Sent from User B to User E

B. Message Switching

- Message switching came about as first type of communications specifically tailored to the needs of computer information transfer.
- It is well suited to batch job processing and electronic mail applications.
- Sometimes referred to as "**Store and Forward**" switching.
- This type of switching is used when *time is not a critical factor since transmission delays may be significant.*
- Message switches are usually general purpose minicomputers with a large amount of mass storage capability.

1) Functionality of Message Switching Systems

- a) An entire message is sent from the computer or terminal to its local message switching node. The message contains the address of the device which is to receive the message.
- b) The message switching node reads the address information and forwards the entire message on to the next node on its journey from source to destination.
 - The message may be stored for some period of time in a given node before it is forwarded to the next node if there are many messages ahead of it in the transmission queue.
 - Dedicated physical connections between source and destination are not required.
 - Routes are established dynamically by each switch on a hop-by-hop basis.
- c) The destination device is informed by its local node that a message has arrived for it.

2) Advantages of Message Switching Systems

- *Line efficiency* is much greater than that of circuit switching systems since messages from many devices will share the same node-to-node channels.
- *Simultaneous availability* of source and destination is not required.
- *Speed and code conversion* can be accomplished by the switches.
- *Robust network* architecture as switches can reroute subsequent messages avoiding failed network components
- Can address multiple addresses simultaneously

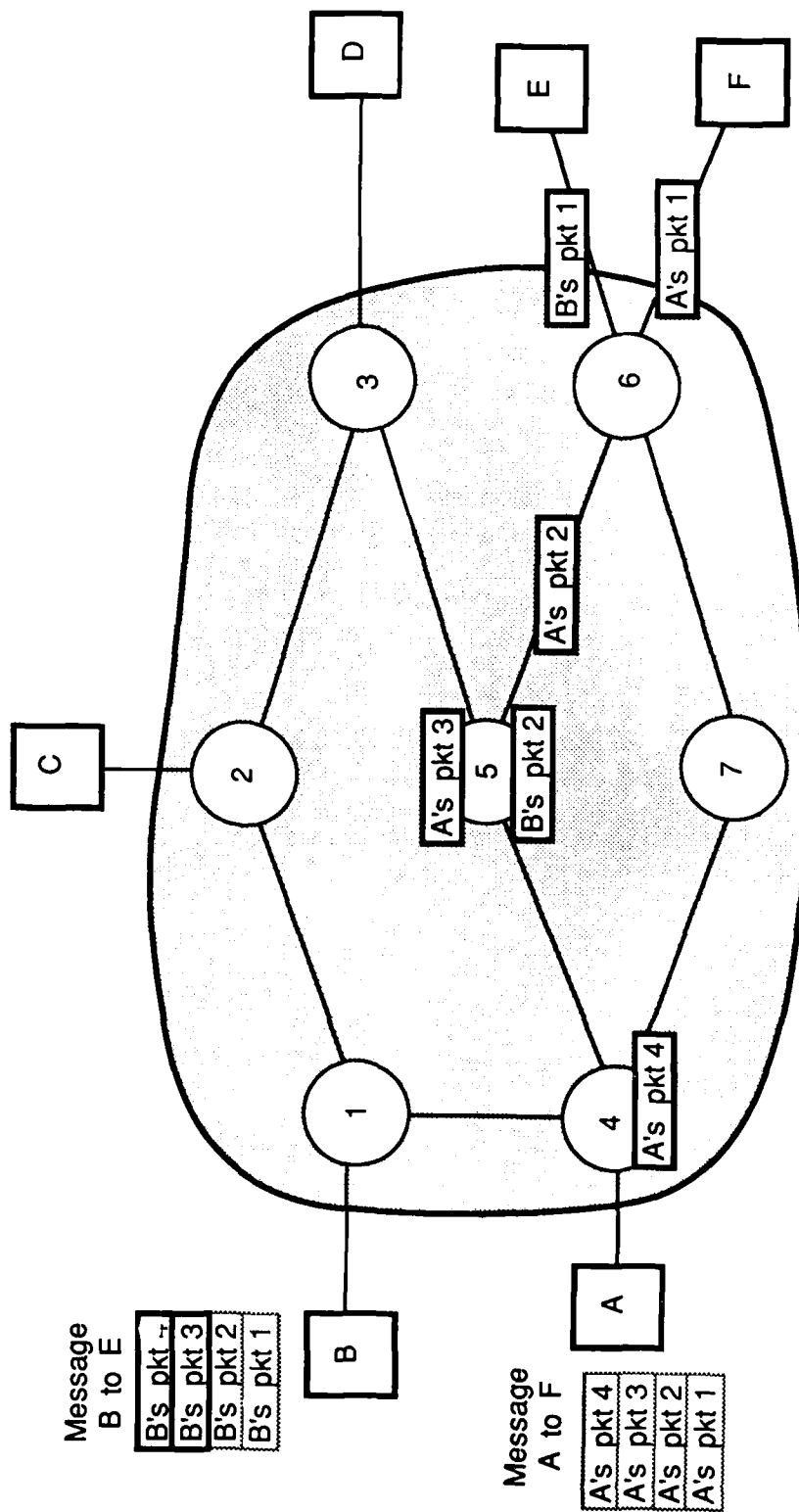
3) Disadvantages of Message Switching Systems

- Not suited to real time or interactive use
- Long and highly varying delays are possible

4) Examples

- Autodin
- Fedwire
- Bankwire

Packet Switching



Messages being sent from User B to User E, and
from User A to User F

C. Packet Switching

- Packet switching attempts to combine the advantages of circuit switching and message switching, while minimizing the inherent disadvantages of both.
- Packet switches are specialized digital devices.
- Messages are transmitted a piece at a time, rather than waiting for the entire message as in message switching systems. The "piece" is called a packet, and may vary in size from implementation to implementation.

1) Transferring Information Through Packet Switching Systems

- a) The computer or terminal breaks all messages into standard-size packets, attaches addressing information to each packet, and then sends the packet to its local packet switch.
 - A standard for the interconnection of computing devices to packet switching networks is *CCITT Recommendation X.25*. This is the principle access method supported by the DDN.
- b) Packets are held in the packet switching nodes' buffers just long enough for previous packets to be transmitted and error control/recovery processes to be completed.
- c) Each node forwards the packet to the next node on its route from source-node to destination-node.
 - The routing technique will vary between packet switching networks. The DDN has implemented a routing scheme which makes it *more survivable* than commercial packet networks.

2) Advantages of Packet Switching Systems

- a) Of the switching techniques presented, packet switching potentially provides the most efficient (cost effective) use of a network's bandwidth.
- b) Packet switched networks are fast enough for interactive communication usage.
- c) Error free communication through the packet network is possible due to internal error checking and correction.
- d) Speed and code conversion and other value-added features are possible with packet networks.

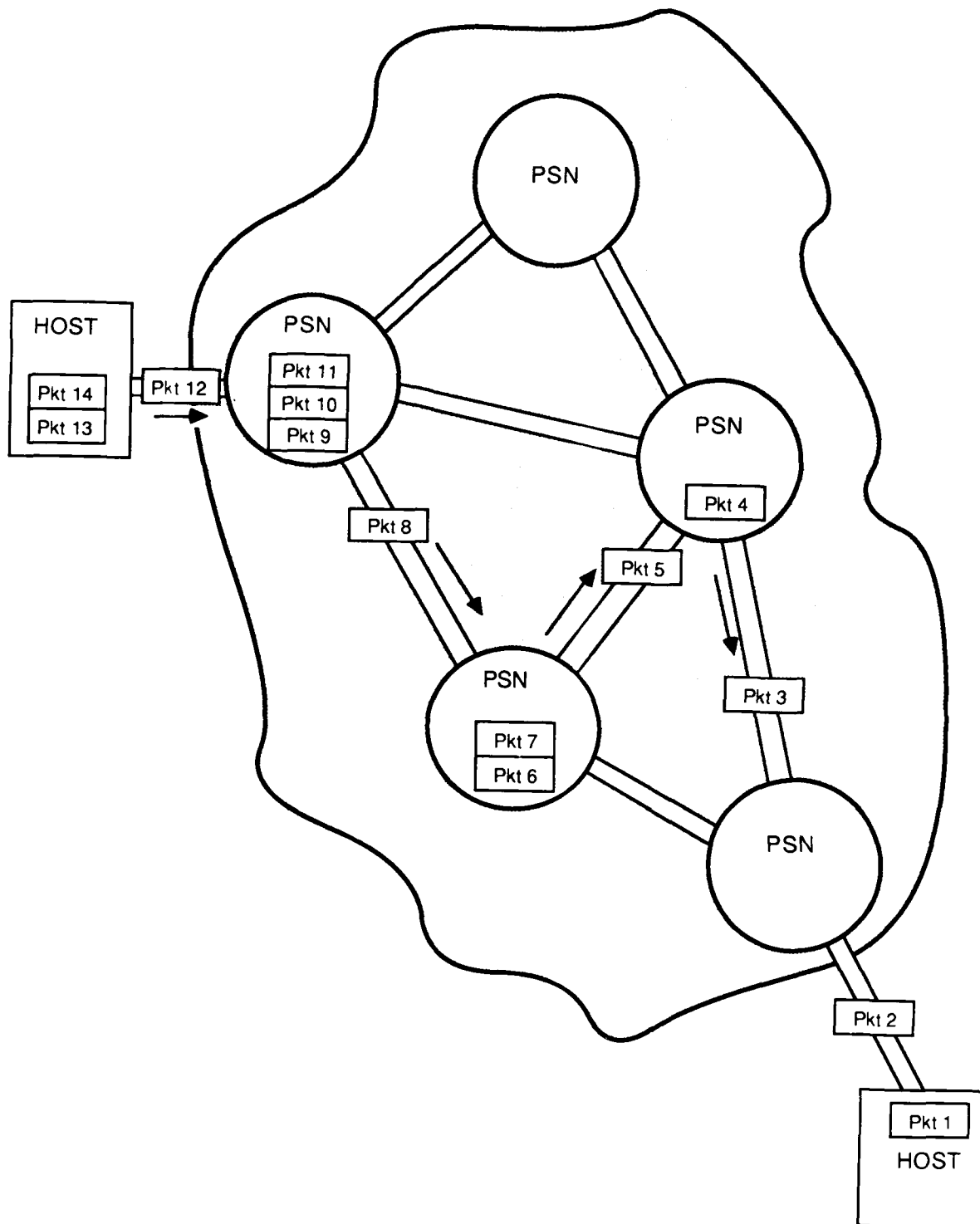
3) Disadvantages of Packet Switching Systems

- a) Slightly greater delay than with circuit switched transmission
- b) Unlike message switching, packet switching requires the simultaneous availability of source and destination.

4) Examples

- Defense Data Network
- Tymnet
- Telenet
- Uninet
- SNA networks
- DECnet

Static Routing



D. Basics of Packet Switching Networks

Basic packet switching networks are distinguished by their:

- Routing method
- Connection services supported
- Network control method

1) Packet Routing Methods

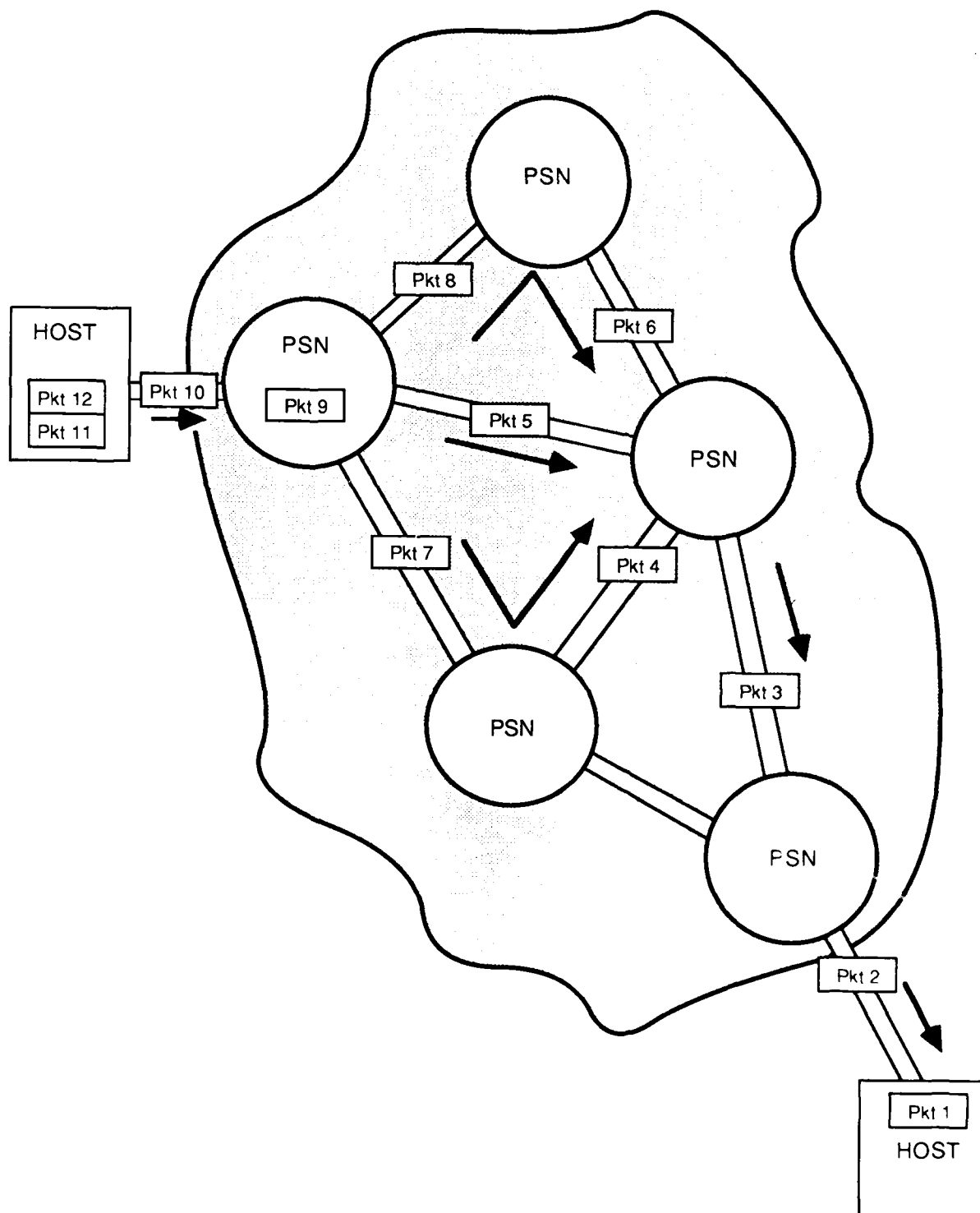
a) Static Routing

- Also referred to as **fixed path routing**. In this method, all packets follow the same physical route from source to destination.
- The route is *established at call setup time*.
- This is the method employed in virtually all public data networks since it is the *easiest to implement* and incurs the least "network overhead traffic".

b) Dynamic Routing

- Each packet may follow a *different route* from source to destination. The packets are thus able to be *routed over the optimum path* at any given time.
- Similar to message switching in that *each packet must contain all the addressing information* needed by a switch to route it to the destination.
- Upon receipt of a packet, the packet switch determines the next best path over which to route a packet so that it will arrive at the destination in the least amount of time and then forwards the packet over that route.
- Dynamic routing has been selected by the DoD to be used in the DDN because it provides the network with the *ability to re-constitute itself* in the event that one or many of the network components are damaged.

Dynamic Routing



c) Comparison Between Static and Dynamic Routing Packet Networks

- Dynamic routing *provides for a more robust network*. Packets will reach their destination by alternate means if a line or node suddenly fails.
- *Error detection / correction is simpler in statically routed systems* since correct packet sequencing is inherent to the system.

In a dynamically routed network, there is a possibility of packets arriving out of order. The reassembly process is complicated by the fact that the receiver doesn't know if a packet is missing or just delayed.

- *The possibility of oscillation* (a packet being routed over the same paths over and over again) exists in dynamically routed networks.
- *Dynamically routed systems will provide faster transmission* since each packet will be routed over the quickest path at any given time. Statically routed packets must traverse the same route for the entire duration of the call.

2) Types of Connection Service

There are two types of connection service obtainable in packet switched networks: Virtual Circuit Service and Connectionless Service (also called Datagram service).

a) Virtual Circuit Service

- Analogous to circuit switching in that a call is established, but the connection is logical, not physical, and bandwidth is not dedicated to a single user.
- Multi-Phase Connection Process:
 1. Call Request Used to establish availability of destination
 2. Call Accept Returned to source
 3. Communication
 4. Call Clear Sent by source after all messages have been sent; terminates virtual connection
 5. Clear Confirmation Sent by destination
- *This is the type of service provided by the DDN because it provides confirmed connections from source to destination.*

b) Connectionless Service

- Usually associated with the transmission of **Datagrams**.
- Each packet must contain source and destination addressing information because the packet network treats each packet as an individual message unto itself.
- A device communicating in datagram mode transmits without first establishing a call; i.e., there is no confirmed connection before the transmission begins.

3) Network Control

a) Centralized Network Control

- Control accomplished from central control computer
- Call set-ups and terminations are controlled by central computer
- Initial routing for each virtual circuit is determined by control computer
- Cannot be used with dynamic packet routing algorithms
- Provisions must be made to eliminate the possibility of the entire network failing in the event of a control computer failure.
- This is the type of control employed in commercial packet switching networks because it is the simplest to implement.

b) Decentralized Control

- Control functions are distributed throughout all switching nodes in the packet network.
- In the case of dynamic routing, decentralized control means that each node must determine the "next best hop" for a packet to traverse, in order to lead the packet to its destination in the quickest manner.
- Decentralized control is advantageous in that it provides for a robust network; multiple failures will not prevent the remaining nodes from completing their mission.
- Decentralized control is more complicated to implement since all nodes must have sufficient processing power and sufficient knowledge of the status of all other components in the network to determine the quickest route for a packet.

E. Packet Switching Services

1) Description

- A number of public data networks are available to obtain value added services; features include:
 - Error detection/correction
 - Speed, protocol, and code conversion
 - Electronic mail services
 - Timesharing access to applications and data bases of common interest to a specific user group
 - Security

2) Examples of Public VANs

- | | |
|------------|--|
| • Tymnet | McDonnell Douglas Network Systems Company |
| • Telenet | GTE |
| • Uninet | U. S. Telcom - to be merged with GTE-Telenet |
| • Accunet | AT&T |
| • Infonet | IBM SNA network |
| • MCI Mail | MCI electronic mail services |

Packet Switching Services

	Accunet Packet Switching Service	Compuserve	General Electric Marknet	GTE Telenet	TYMNET, Inc.	Uninet	DDN
Number of U.S. Cities (local dial)	11	250	600	350	516	332	131
Number of Foreign Countries (local dial)	0	0	25	54	64	33	14
Asynchronous/X.25		●	●	●	●	●	●
IBM 3270 Bisync		●	●	●	●		○
IBM SNA/SDLC			●		●	●	
IBM RJE/HASP				●	●	●	
Electronic Mail		●	●	●	●		●
Microcomputer (file transfer)			●	●	●	●	●
2400 bps Async Dial-up			●	●	●	●	
Async to 3270 BSC via network software			●		●		
Async to 3270 SDLC via network software					●		
Network-level Password Security		●	●	●	●		●
Link Encryption							●
OUTDIAL			●	●	●	●	

3) Comparison of Services Offered by the Major Packet Switching Services

- a) Number of US cities in which there are switching nodes
- b) Number of foreign countries included in the network
- c) Asynchronous terminal access to X.25 hosts
- d) Support for IBM 3270 Bisync protocol
- e) Support for IBM SDLC protocol
- f) Support for IBM RJE/HASP protocol for batch communication
- g) Electronic mail services
- h) Asynchronous file transfer protocols for microcomputers
- i) Support for 2400 bps dial-up access by async devices
- j) Async to 3270 BSC or 3270 SDLC conversion
- k) Network level password security
- l) Link encryption security
- m) Ability to dial out of the network over async dial-up modems

SECTION II

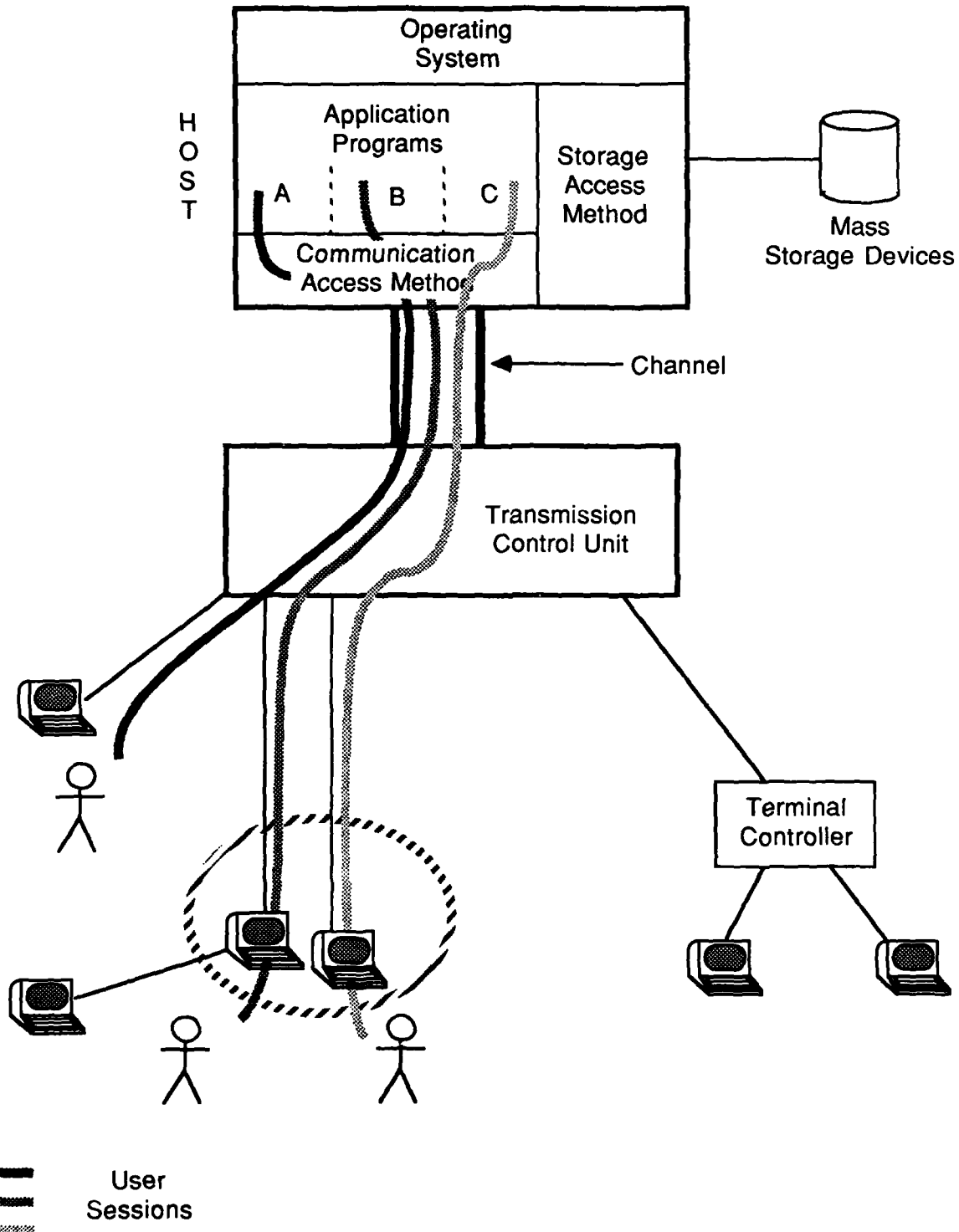
COMPUTER NETWORK ARCHITECTURES

**OBJECTIVES
OF
COMPUTER NETWORK ARCHITECTURES**

- **To understand the characteristics of the DoD network architecture and several major commercial network architectures so that the student has a consistent framework with which to determine the architectural changes required by connection to the DDN and DoD interoperability.**
- **To understand the level of computer interoperability required by the DoD and the importance of the DoD protocol suite in achieving interoperability, so that the student can implement systems which meet these requirements.**
- **To appreciate the importance of the DDN in providing communication services to the DoD community and providing cost savings of communications lines.**

A Remote Access System

Circa 1960 - 1970's

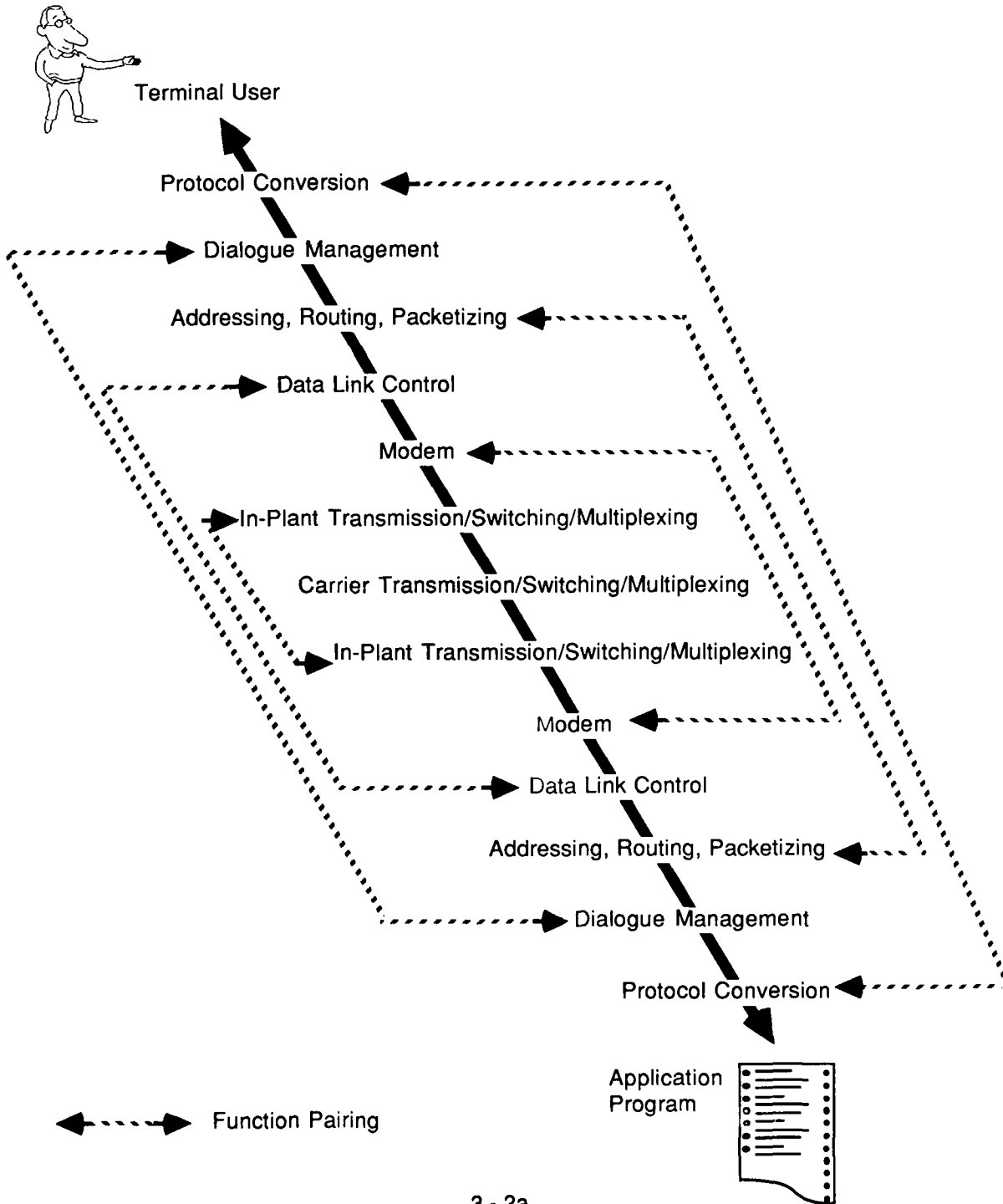


3. Introduction and Concepts

A. The Need for Network Architectures

- 1) In the 1960's and early 70's there were few standards for communications software.
- 2) If a user wanted to access an application program running on a remote host, he had to conform to that program's way of using the communication system of that host. This usually meant using a particular terminal, transmission speed, character code, etc.
- 3) These factors varied from program to program, so that it was very difficult for the user to switch from accessing one program to another. The user might need a different terminal.
- 4) The applications programmer had to have detailed knowledge of the host's communications system, and had to design and implement a separate access method for each program.
- 5) A small change in the host's communication facilities meant that all application programs using these facilities had to be changed.
- 6) It was very difficult to port such programs to hosts with different communications facilities.
- 7) What was needed was a *single communications system* that served all hosts, terminals and applications, with *standard interfaces* between these devices and the communication network.

Network Functions For End-to-end Communications

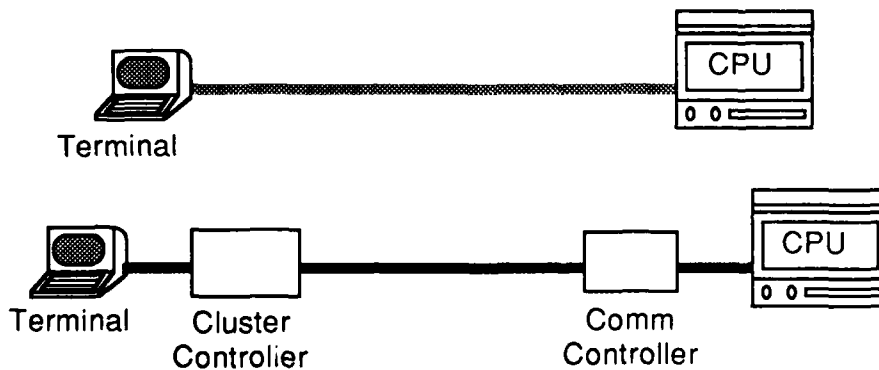
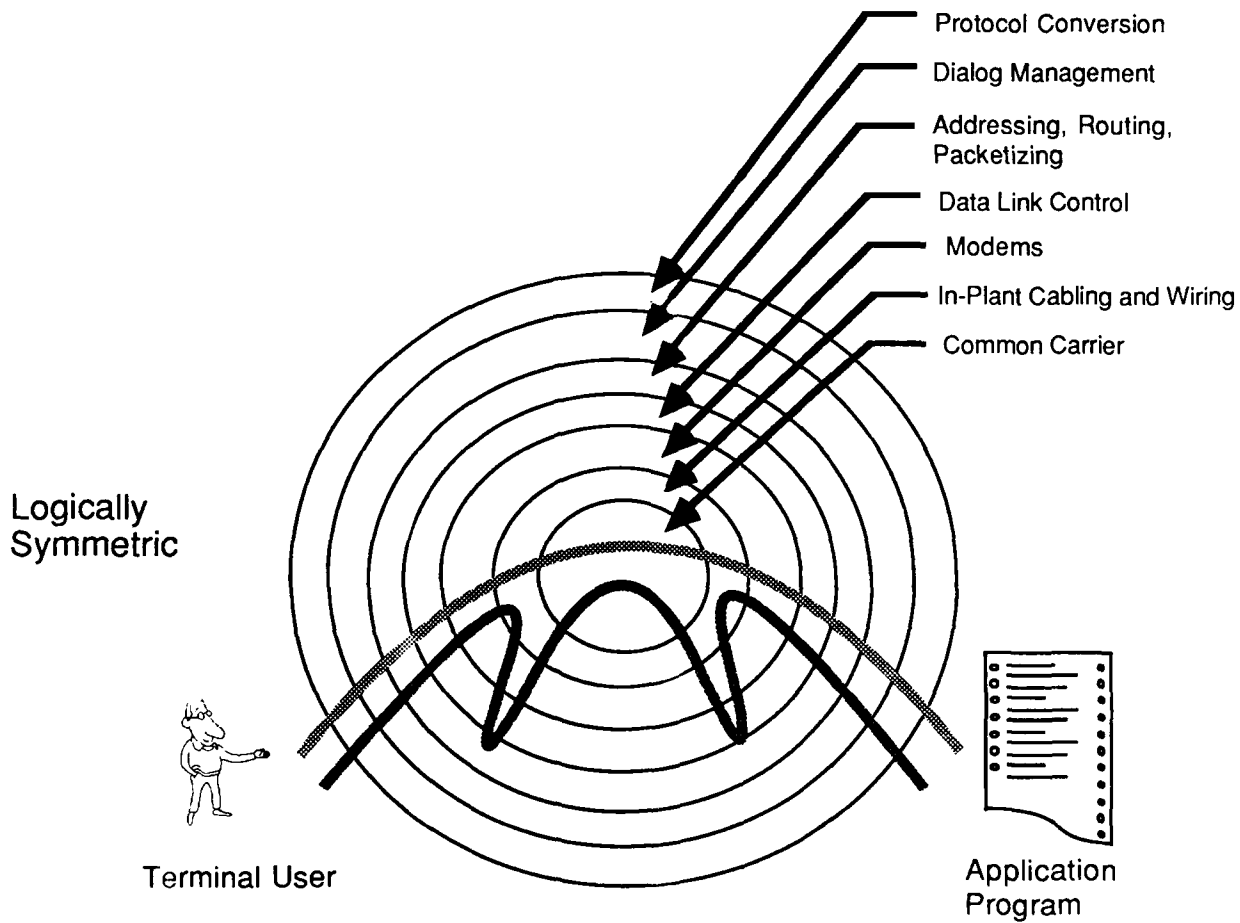


B. A Natural Layering of Network Functions

1) Some Necessary Functions for End-to-End Communications

- a) Provide a physical transmission path
 - Define what represents a 1 or a 0
 - Set transmission speed and synchronize clocks
 - Choose simplex, half or full duplex communication
 - Perform switching and multiplexing (in-plant and carrier)
- b) Provide digital to analog conversion (by modems) where necessary
- c) Provide error free transmission over the physical path
 - Send data in FRAMES, with special error checking patterns appended to the data
 - Send acknowledgements (ACKs) when a frame is received without error, and negative-acknowledgements (NAKs) when an error is detected
 - Provide TIMEOUTS for lost frames, ACKs or NAKs
 - Retransmit frames upon TIMEOUT or receipt of a NAK
 - Check for duplicate frames
- d) **Route** data through a network of physical paths
 - Segment source data into packets
 - Route packets through network as fast as possible, avoiding highly utilized links and nodes
 - Multiplex packets from different users together over the same physical links for efficiency
 - Reassemble data from packets at destination, in correct order
- e) Provide complete **end-to-end** service (source-to-destination)
 - Prepare data for presentation to the network
 - Provide end-to-end error checking (in case of node error)
 - Provide end-to-end **flow control**, if source and destination have different data flow rates
 - Provide end-to-end **addressing**, since source and/or destination might be hosts with multiple processes running or terminals attached

Hierarchical Pairing Of Network Functions



f) **Provide end-to-end dialog management**

- Establish and terminate a communication session (BIND and UNBIND two processes)
- Map logical addresses to physical addresses (figure out where another user is, or on what host an application is running)

g) **Accommodate format, code and language of end-user**

- Perhaps ASCII to EBCDIC conversion
- Text compression, data encryption
- Device management: interpretation of terminal control characters such as tabs, line feeds and carriage returns

2) **A Natural Grouping and Hierarchy of Functions**

a) Network functions depend on each other.

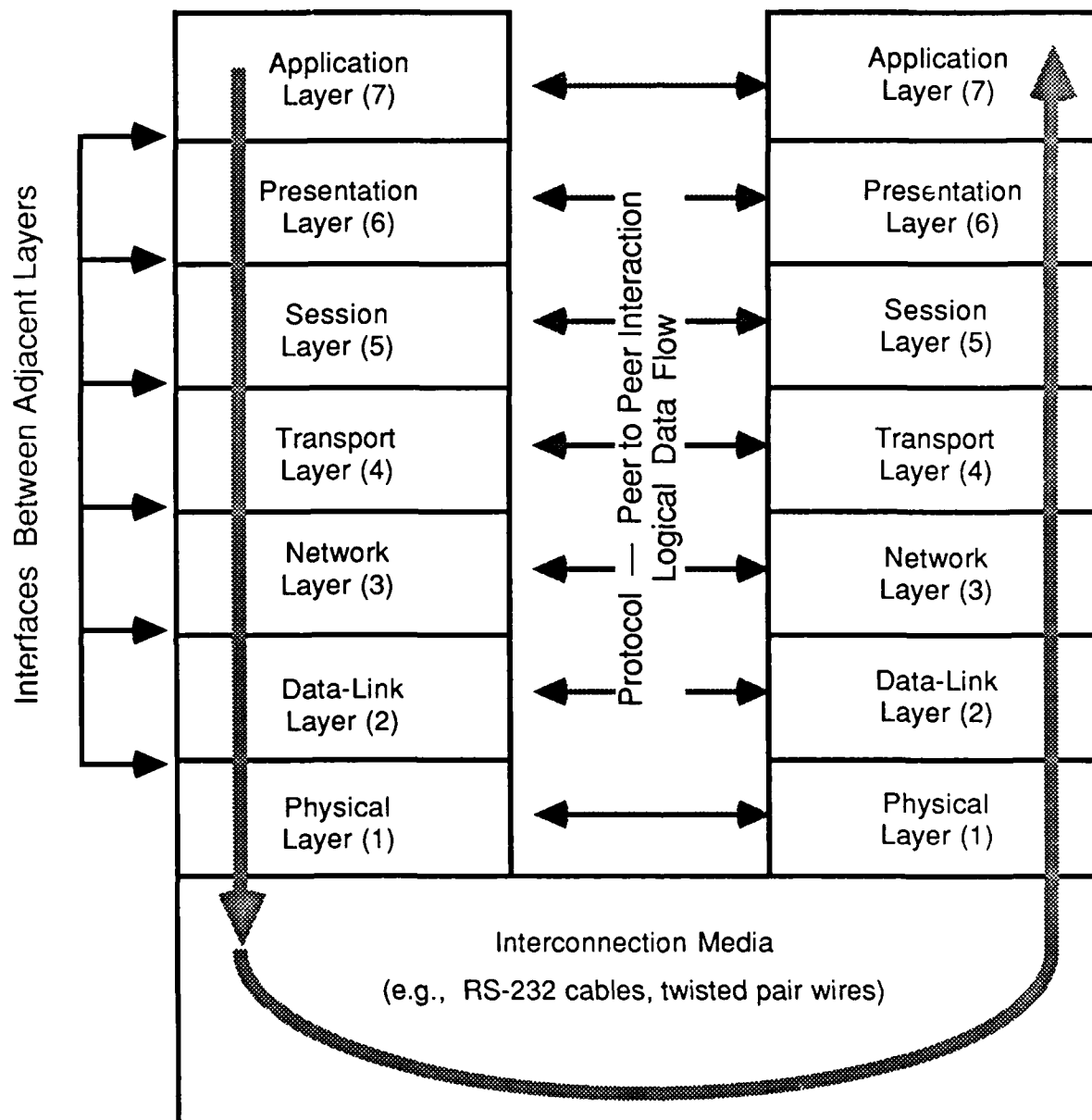
b) Functional dependency is a hierarchical relationship:

- Modems depend on the existence of a physical transmission path.
- Error checking and flow control depend on a digital transmission path (provided by modems where necessary).
- Network management and routing depend on flow controlled, error free links between nodes.
- End-to-end services need to have their data conducted successfully through the network for them.
- Dialog management assumes that end-to-end services will be provided once a dialog session is set up.

c) Data from a terminal user moves through the hierarchy as it moves through the network. Functions are performed sequentially.

- Data first undergoes format or code conversion (Protocol Conversion).
- Sequence numbers might be added by Dialog Management.
- Network routing and management then provides physical addresses and packetizes data.
- Data Link Control between nodes must add error checks and frame delimiters to data.
- Data is transmitted over the physical link.

Open System Interconnection (OSI) Reference Model



C. Definition of a Computer Network Architecture

1) The Concept of a Layer

- a) Similar network functions can be grouped into a logical layer.
- b) The layers are placed on top of each other in the same way network functions are performed in a sequential order.
- c) A layer's functions provide services to the layer immediately above, and utilize the services of the layer directly below.
- d) Layers are **modular**, so that a layer may have a protocol replaced without impact as long as it provides the same services as before.

2) Interfaces

- a) An interface is defined as the boundary between two adjacent layers.
- b) Thus when data and control information from layer N is passed to layer N-1 it passes through the interface between N and N-1.
- c) An interface defines the services that a lower layer offers the upper.
- d) Thus interfaces are concerned with the **physical** flow of user data and network control information.

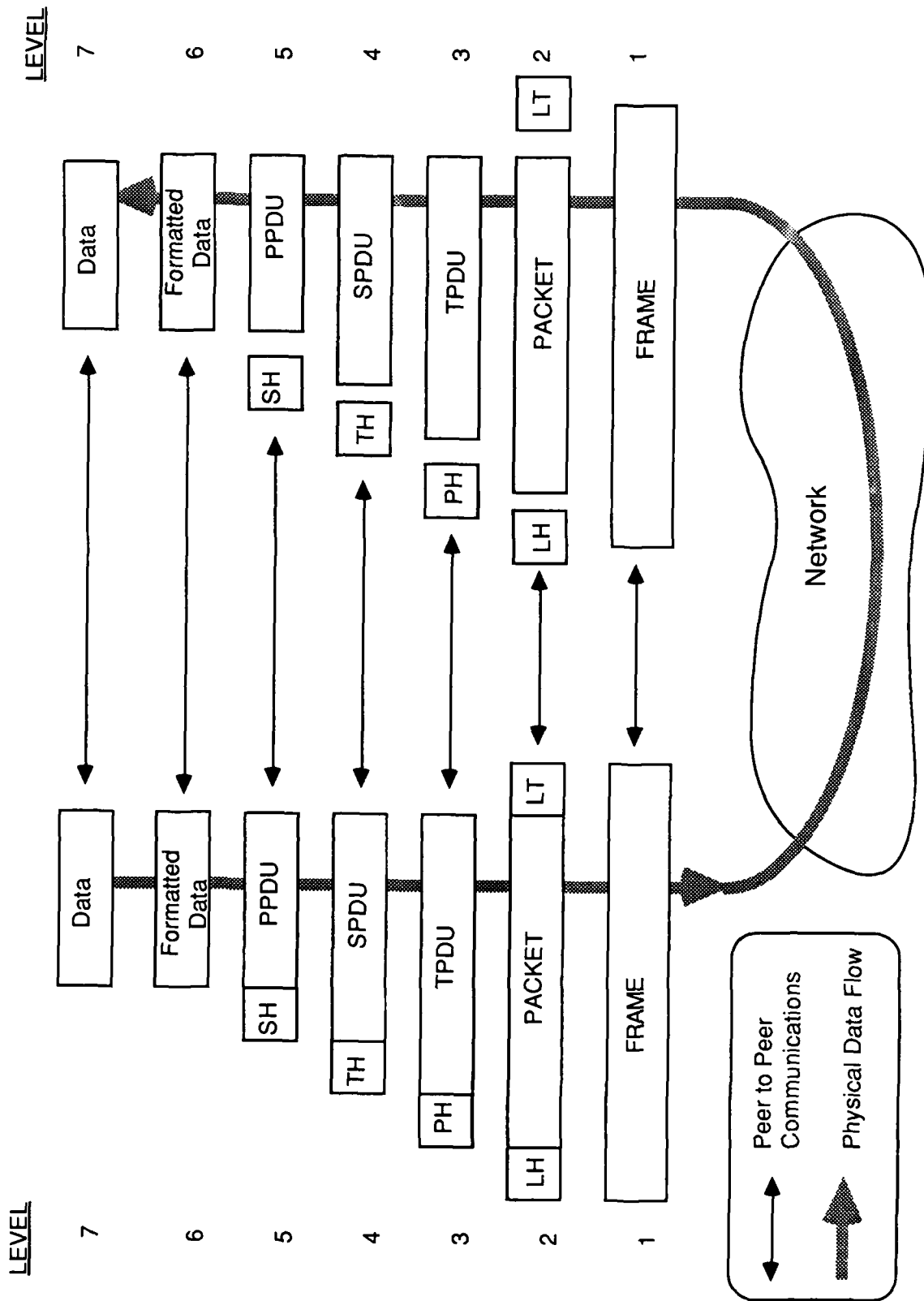
3) Protocols

- a) Peer layers at each end exchange control information with one another to perform the functions of that layer.
- b) *Logical flow* of control information is from peer layer to peer layer. *Physically*, the information flows through layer boundaries — from layer N to layer N-1.
- c) The *format* of control information (usually protocol headers) and the *sequence* of interaction between peer layers is defined by the protocol specification.

4) Computer Network Architecture

A computer network architecture is defined as a set of Protocols and Interfaces encompassing all layers.

OSI Data Flow



5) The Data Flow Model

- a) How an end-to-end message moves through a network architecture.

At the source:

1. Each layer receives data from the layer above and considers it a sealed package to be sent through the network without regard to its contents.
2. Each layer adds some control information such as an address, sequence number, byte count, error checking information, etc., by attaching a header and/or trailer to the data and passing this to the layer below. The layer below considers this to be a sealed package to be sent through the network.

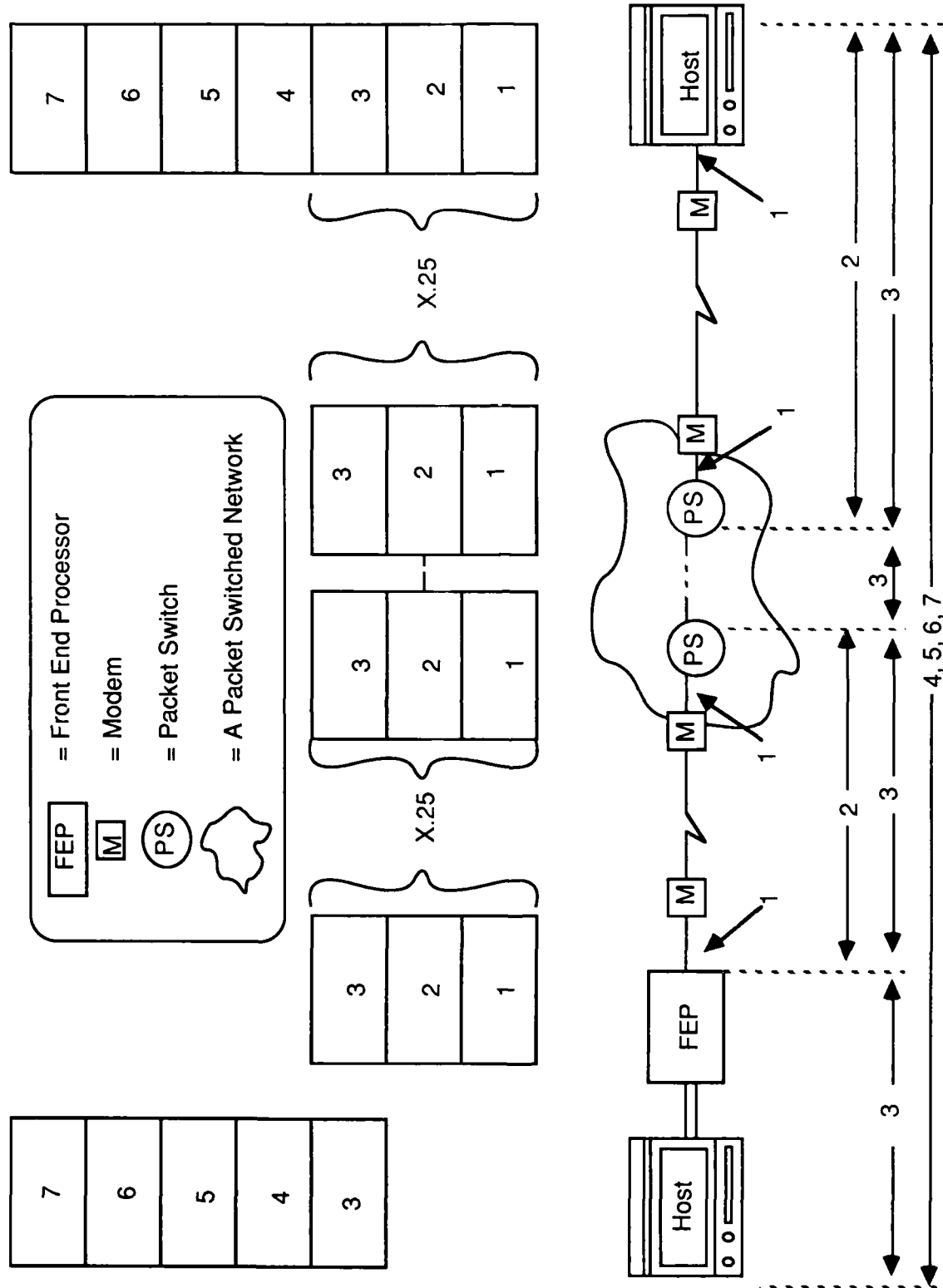
At the destination:

3. Each layer receives the sealed package of data from the layer below, strips off the header and /or trailer of control information sent to it by its peer layer at the source, and passes the rest of the data package to the layer above.
4. Thus two peer layers communicate by means of attached headers and trailers. The format and content of a header/trailer is specified by a layer's **protocol**.

- b) Example Data Flow (in OSI)

1. User DATA is passed from the Application Layer or to the Presentation Layer.
2. The Presentation Layer creates a Presentation Protocol Data Unit (PPDU) by reformatting data.
3. The Session Layer adds a Session Header (SH), thus creating a Session Protocol Data Unit (SPDU).
4. The Transport Layer creates Transport Protocol Data Unit (TPDU) by adding a Transport Header (TH).
5. The Network Layer adds a Packet Header (PH) to form a packet.
6. The Data Link Layer adds a Link Header (LH) and Link Trailer (LT) to the PACKET, thus making a FRAME.

Location Of Network Layers



6) Where Network Layers Reside

a) Implementation of the Layers

- Lower layers are usually implemented in hardware, higher levels in software.
- All of the layers may be implemented in a single device. This is the case with minicomputers such as VAXs.
- Layers may be divided among several devices such as in a mainframe host system where the lower layers are implemented in the Front End Processor, and the upper layers in the host itself.
- Intermediate nodes contain only the lower layers (Layers 1, 2 and 3 in the OSI model).
- End-to-end functions, those of the OSI Transport Layer and above, are handled by end nodes only (source/destination packet switches, hosts, terminals, etc.).

c) Example: The OSI Layers

1. PHYSICAL - is usually implemented in hardware such as physical DTE-DCE interfaces (e.g., RS-232C).
2. DATA LINK - is often performed by a mixture of hardware and software in a FEP, packet switch, intelligent terminal, host, or cluster controller line handler card.
3. NETWORK - routing and packetizing functions are implemented in software in hosts, FEPs, and packet switching node software.
4. TRANSPORT - end-to-end functions will be found mostly in hosts. The layer is often part of the operating system or part of the access method software.
5. SESSION - is sometimes merged with the Transport Layer, or included in the application software.
6. PRESENTATION - is implemented as host library routines, system macros, or in a mainframe application subsystem.
7. APPLICATION - is implemented as applications programs such as word processing, transaction processing, or database managers.

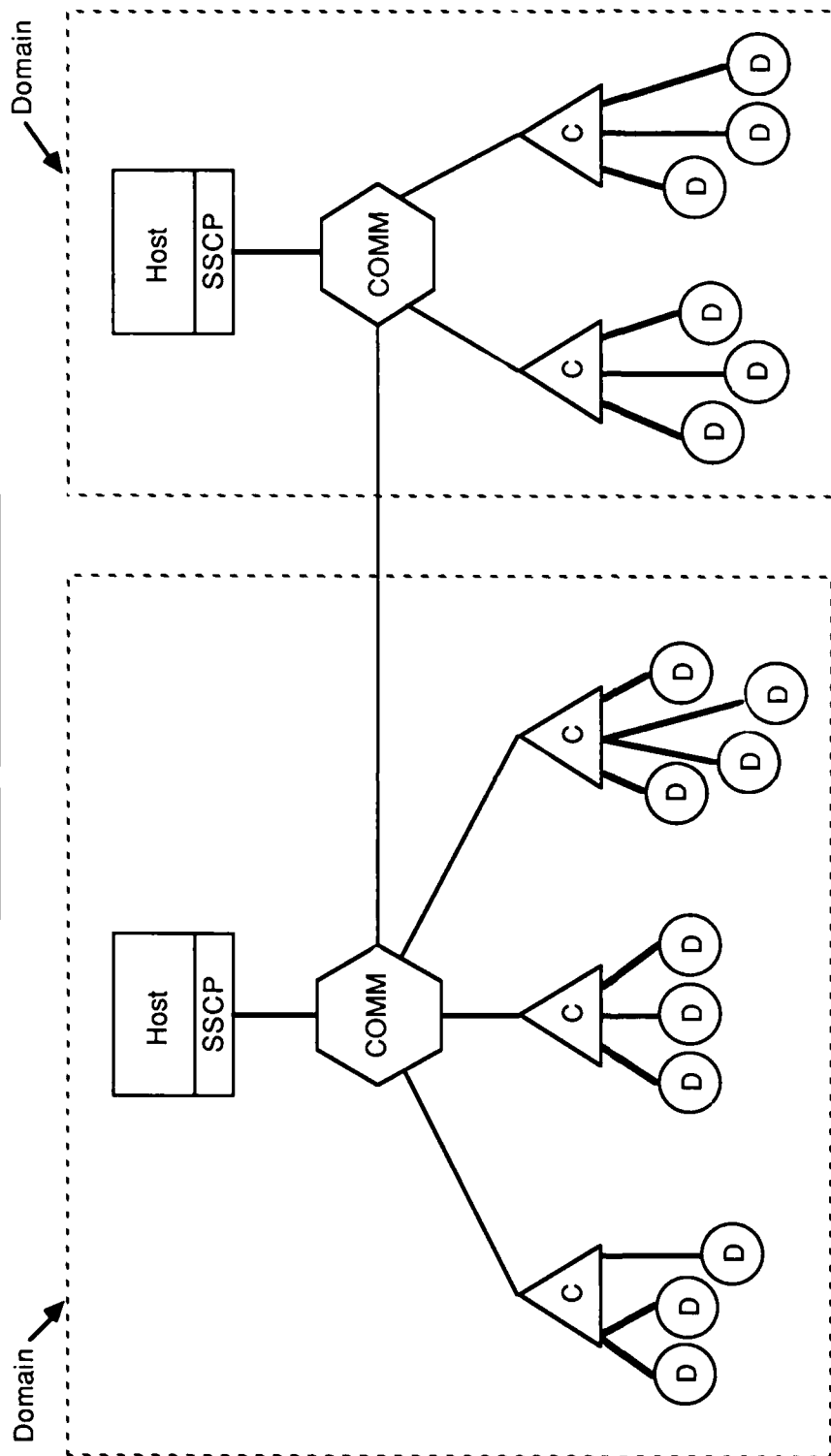
4. DESCRIPTION and COMPARISON of MAJOR NETWORK ARCHITECTURES

A. SNA

1) Background

- a) IBM's System Network Architecture
- b) Before 1974 IBM had hundreds of communications products, over 30 teleprocessing access methods, more than a dozen data link protocols.
- c) 1974 — First release of SNA, an architecture to be implemented by private networks of IBM products, allowed only hierarchical tree structured centralized networks (one host with attached terminals).
- d) 1978 — Advanced Communications Function (ACF) allowed connected tree structured networks with multiple hosts.
- e) 1981 — Latest releases of SNA products allow networks to be constructed in an arbitrary mesh topology and support packet switching across alternate routes, parallel links between adjacent nodes, and sessions of different priorities.
- f) As a result of trying to integrate so many different functions and applications from the multitude of IBM products, SNA is a large, complex, and comprehensive architecture.

A SNA Environment



	PU Type
Host SSCP	5
COMM	4
C	2
D	1

2) Key Concepts in SNA

a) 3 Kinds of NAUs (Network Addressable Units)

- Logical Units (LUs), which represent user ports into the network; usually one LU per terminal display and one per host application subsystem
- Physical Units (PUs), one for each node, used to address physical devices for network management and control purposes

4 Types of **NODES** (based upon PU type):

Devices : Terminal Displays (e.g., 3278) and Printers

PU type 2: Cluster Controllers (e.g., 3274, 3776)

PU type 4: Communications Controllers (e.g., 3705, 3725)

PU type 5: Hosts (e.g., 308X, 309X, 43XX mainframes)

- Systems Services Control Point (SSCP), a network supervisor resident in each host

b) Domains

- A domain is the collection of devices and nodes of PU types 2 and 4 which are controlled by a single host.
- The SSCP controls all network hardware and software within its domain.

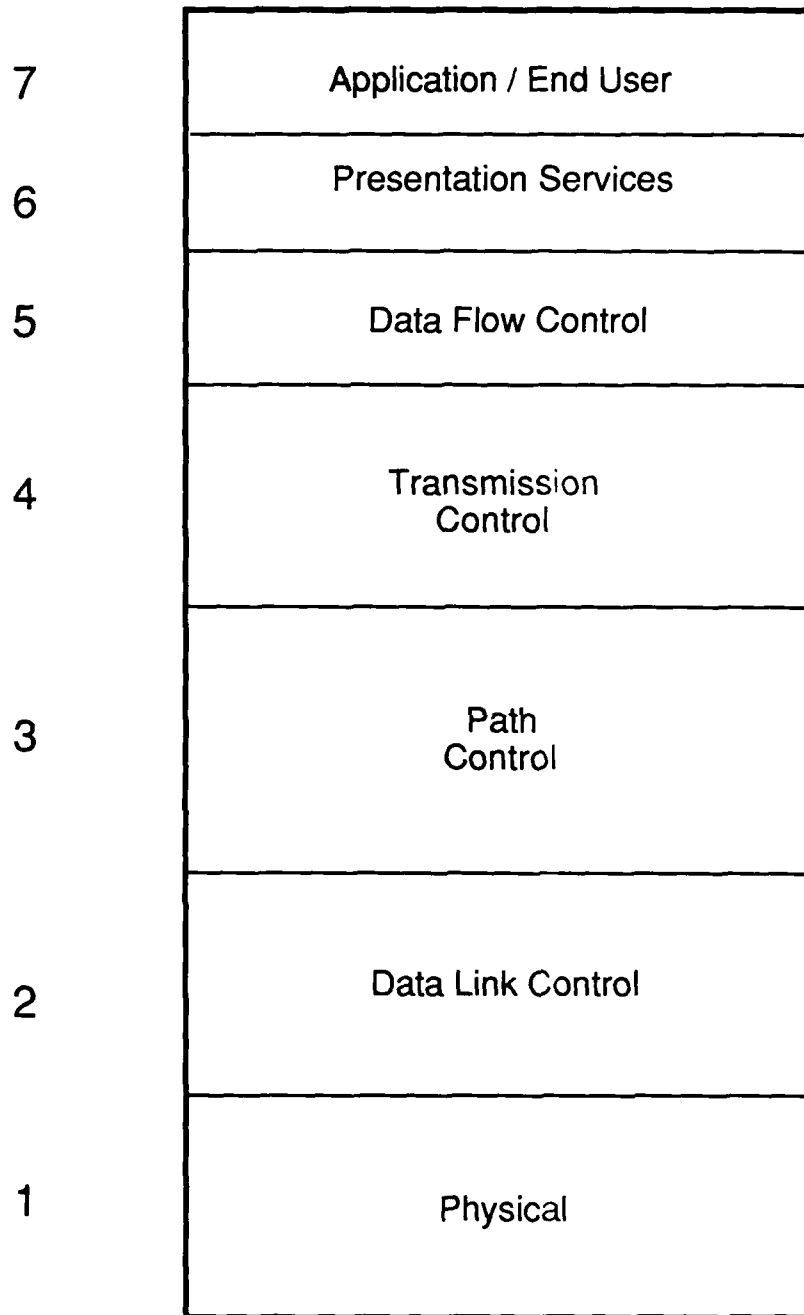
c) Sessions are managed by the SSCPs

- When one process wants to communicate with another, it must make a request to the SSCP controlling its domain, and ask that an LU-to-LU session be set up for them. (There is always a session between a process and its controlling SSCP).
- If the two processes are in different domains, the session must be set up by the two SSCPs governing those domains.

d) Sessions are ASYMMETRIC

- One process is the PRIMARY LU, the other is the SECONDARY LU.
- Primary LU has control and error recovery responsibility for the session.
- The host application is always the Primary LU while terminals are always Secondary LUs.

Layering In SNA



3) The Layers of SNA

- a) Physical — Usually RS-232 DTE-DCE interface
- b) Data link control — SNA uses bit-oriented SDLC (Synchronous Data Link Control) protocol
 - Normal Response Mode subset of HDLC
 - Requires one Primary station (responsible for polling and link control) and one or more Secondary link station(s)
 - Frames are delimited by a unique bit pattern, called a flag, at the beginning and end of each frame.
 - Handles half duplex, full duplex, multidrop and point-to-point lines
 - No explicit maximum frame size
- c) Path Control — Provides virtual circuit-type service and routing of SNA packets called Path Information Units (PIUs)
 - Performs functions of OSI NETWORK LAYER
 - Static Routing — routes are chosen from fixed tables which are determined manually at sysgen time. Each possible source-destination combination has a list of alternate routes to be chosen from depending on class of service selected.
 - Multiple sessions can use the same path.
 - Supports 3 priority levels for network traffic
 - Rate of data flow is controlled for all network traffic (sessions) on each path.

d) Transmission Control

- Provides end-to-end control of messages through the use of packet sequence numbers.
- Data flow rate is controlled in this layer for each session (analogous to a virtual circuit), as opposed to data flow rate in Path Control, which dictates the flow rate for all sessions on a particular path.
- Thus the Transmission Control Layer in SNA handles functions of the OSI TRANSPORT LAYER, by providing virtual circuit service.

e) Data Flow Control — Manages the **direction** of data flow between two processes

- Controls the send-receive state of a session, which can operate in half duplex flip-flop, half duplex contention, or full duplex mode
- Corresponds to the SESSION LAYER in the OSI model
- Controls arrival of messages to a process, assuring complete message integrity
- Does not control data flow rate. This is done in Transmission Control.

f) Presentation Services

- Text compression, compaction
- Terminal data streams:
 - Intermix data with control characters
 - Read, write, erase, intensity, etc.
- File management: create, destroy or update remote files
- Correspond to the functions of OSI's PRESENTATION LAYER.

g) Application of End-User

B. DECnet (DNA)

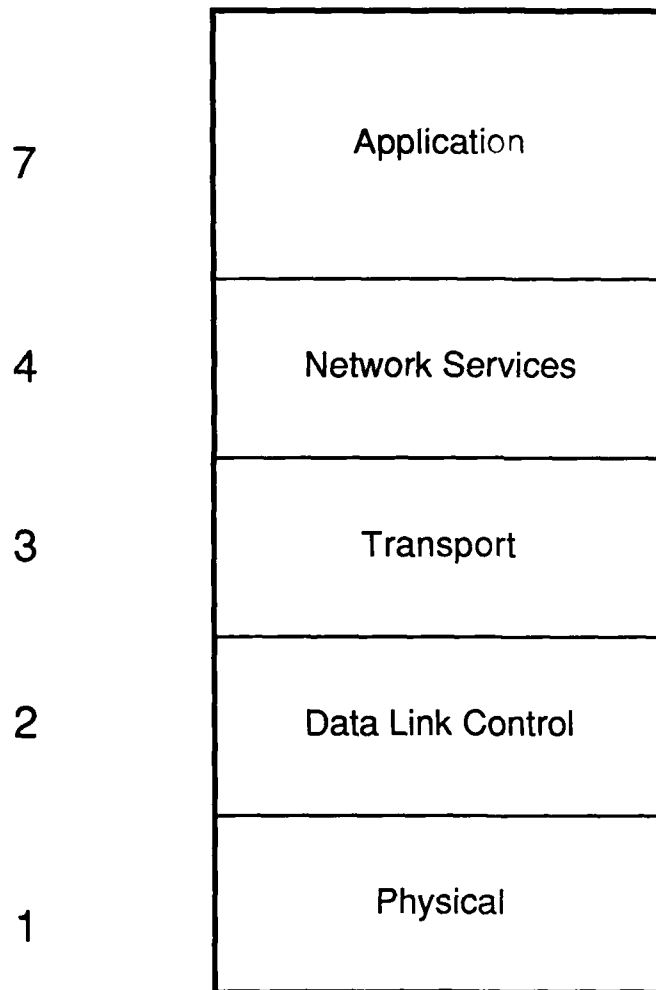
1) Background and Key Concepts

- a) Digital Equipment Corporation's Digital Network Architecture (DNA), implemented by software called DECnet, running in each networked computer.
- b) Early versions of DECnet did not allow indirect connection (i.e., two machines could only communicate if there was a direct link between them; communications through them could not go through a third machine).
- c) DNA today supports complete connectivity among mesh network nodes, and with DEC products connected via Ethernet LANs.
- d) DNA has a PEER style of interconnection, as opposed to host-centered like SNA. Because first DNA networks were composed of many minicomputers, there is no central network control in DNA.
- e) DEC is heavily involved with the ISO and so has committed itself to following existing OSI standards and adapting to new ones as they emerge, up to and including the OSI SESSION LAYER.

2) The Layers and Protocols of DNA

- a) Physical — Primarily RS-232 DTE-DCE interface

Layering In DNA



- b) Data Link Control — DNA uses character-oriented DDCMP (Digital Data Communications Message Protocol), but is beginning to incorporate HDLC, the OSI DATA LINK LAYER protocol, as well. Features of DDCMP:

- A **character count** in the frame header is used to keep track of frame length, rather than using frame delimiter patterns at the beginning and end of each frame.
- As a result, no bit-stuffing or character-stuffing is necessary.
- Because of the character count's importance, the frame header has its own checksum, separate from the data checksum.
- ACKs can be piggybacked on reverse traffic frames.
- Up to 255 frames can be unacknowledged before transmission must stop.
- Maximum packet size is fairly long: 16388 bytes.
- No preemption, so all traffic waits if a long frame is being sent.
- Can handle half and full duplex, multidrop and point-to-point lines.
- Multidrop lines require a master/slave relationship, with the master terminal doing the polling.

- c) Transport — Provides datagram service to the Network Services Layer

- Performs functions of ISO NETWORK LAYER
- Packets may be discarded, duplicated or delivered out of sequence.
- Routing tables are maintained at each packet switching node. The network manager assigns a cost to each link in the network. The nodes use these costs to calculate the least cost path from every source to every destination. These costs can be dynamically adjusted by the network manager in order to increase or decrease loads on certain links or nodes. Nodes will automatically detect link failures and adjust their routing tables. Any changes in one node's routing tables are eventually transmitted to all other nodes. Thus a DNA network adapts to changes in network topology (node and link failure), but needs human intervention to adjust to traffic fluctuations (fine tuning and congestion relief).
- This does not guarantee that node buffers will not fill up. If they do, packets are discarded.
- Packets are discarded if they have traversed more links than the longest path in the network. Thus packets may loop but not for a very long time.
- In the next few years the DEC Transport layer's packet format will include the ISO Internet Protocol (IS 8473) specification.

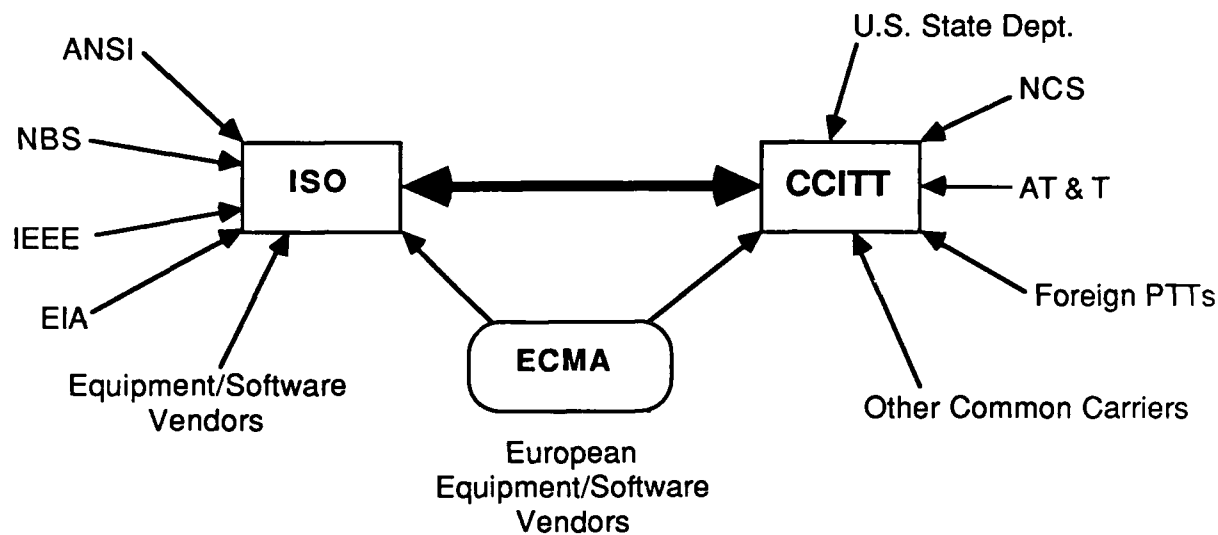
d) Network Services — Performs functions of the OSI TRANSPORT LAYER using Digital's proprietary Network Services Protocol (NSP).

- NSP commands are invoked as system calls or library routines and are **machine dependent**.
- Example NSP commands: CONNECT REQUEST, TRANSMIT, RECEIVE + parameters
- These commands are invoked directly by the user application. There is **no** Session Layer in DECnet. However, DEC plans to add a Session Layer as soon as the ISO standardizes one. In addition, NSP will be replaced by a future OSI Transport Protocol (TP).
- This layer must deal with the problems caused by an unreliable network (e.g., pure datagram service), such as discarded, duplicated or out of sequence packets. In an attempt to provide reliable transport service to the Application Layer, the NSP uses such techniques as **three way handshaking** (i.e., acknowledging acknowledgements).

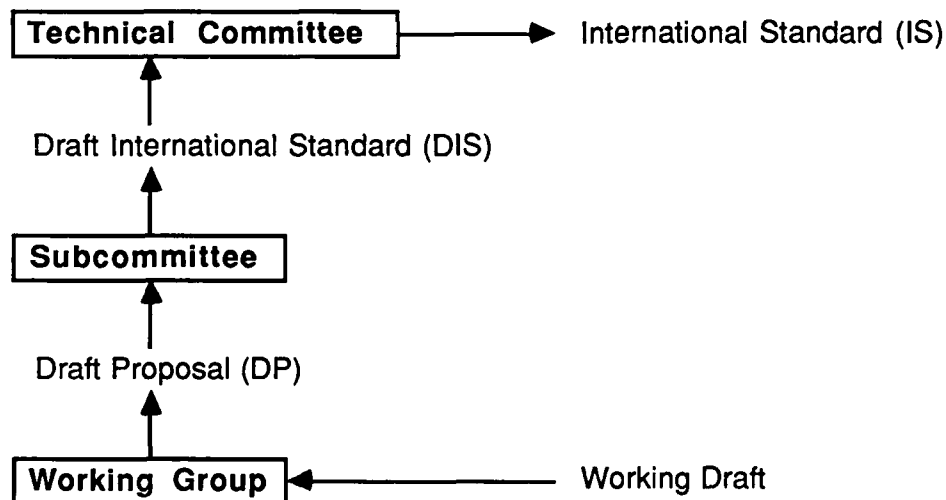
e) Application Layer

- Though it is a combination of the OSI PRESENTATION and APPLICATION Layers, the DNA Application Layer actually has minimal functions.
- Data Access Protocol (DAP) permits a user to access remote files:
 - Allows reading and writing of individual records, as well as entire files
 - Provides some conversion between different file formats, such as: different record delimiters, different carriage control characters

Standards Organizations



ISO Standardization Process



C. OSI

1) Background

- a) In 1977 the International Organization for Standardization (ISO) created the Open System Interconnection (OSI) subcommittee to develop a standard architecture.
- b) The abstract functional layering of this architecture, the current **OSI Reference Model** already described, was approved in 1982.
- c) It is a **framework** for the current and future development of complete service definitions for these layers, and the implementation of the services in standard protocols.
- d) The International Telegraph and Telephone Consultative Committee (CCITT) has adopted the OSI Reference Model and works closely with the ISO on service definitions and protocol development for each layer.
- e) Other standards organizations (such as IEEE, ANSI, EIA, and ECMA), are also developing, adopting, and supporting standard protocols and interfacing procedures that provide the services defined by the reference model.

2) Basic Concepts in International Standardization

a) The ISO Standardization Process

- **Working Draft** - Standard being developed by a Working Group (WG)
- **Draft Proposal (DP)** - Standard accepted by WG, submitted to Subcommittee (SC)
- **Draft International Standard (DIS)** - Standard approved by SC, submitted to Technical Committee (TC)
- **International Standard (IS)** - Standard approved by TC (Form: "IS ####")

b) The CCITT Standardization Process

- **Draft Recommendation**
- **Recommendation** - (Form: "X.##" or "V.##")

Current Status of OSI Reference Model Layer Standards

Layer	ISO			Representative Protocols		
	Services Definition	Protocol Specification	ISO	CCITT	Others	
1 Physical				V.24 V.35	EIA RS232 EIA RS 449	
2 Data Link	Draft Proposal	Draft Proposal	HDLC IS 8802	LAPB	IEEE 802.2	
3 Network	International Standard	International Standard	IS 8208	X.21, X.25		
4 Transport	International Standard	International Standard	TP IS 8073	X.214 (service) X.224 (protocol)		
5 Session	International Standard	International Standard	SP IS 8327	X.215 (service) X.225 (protocol)		
6 Presentation	Draft International Standard	Draft International Standard	SC21N897 SC21N898	(service) (protocol)		
7 Application	Draft Proposal	Draft Proposal	FTAM, VT	X.400		

d) Note that an ISO **IS** usually has a corresponding CCITT **Recommendation**.

c) General order of development of OSI layer standards

- Layer services definition
- Layer protocol specifications
- Specific layer protocols

3) Current Status of OSI Layer Standards

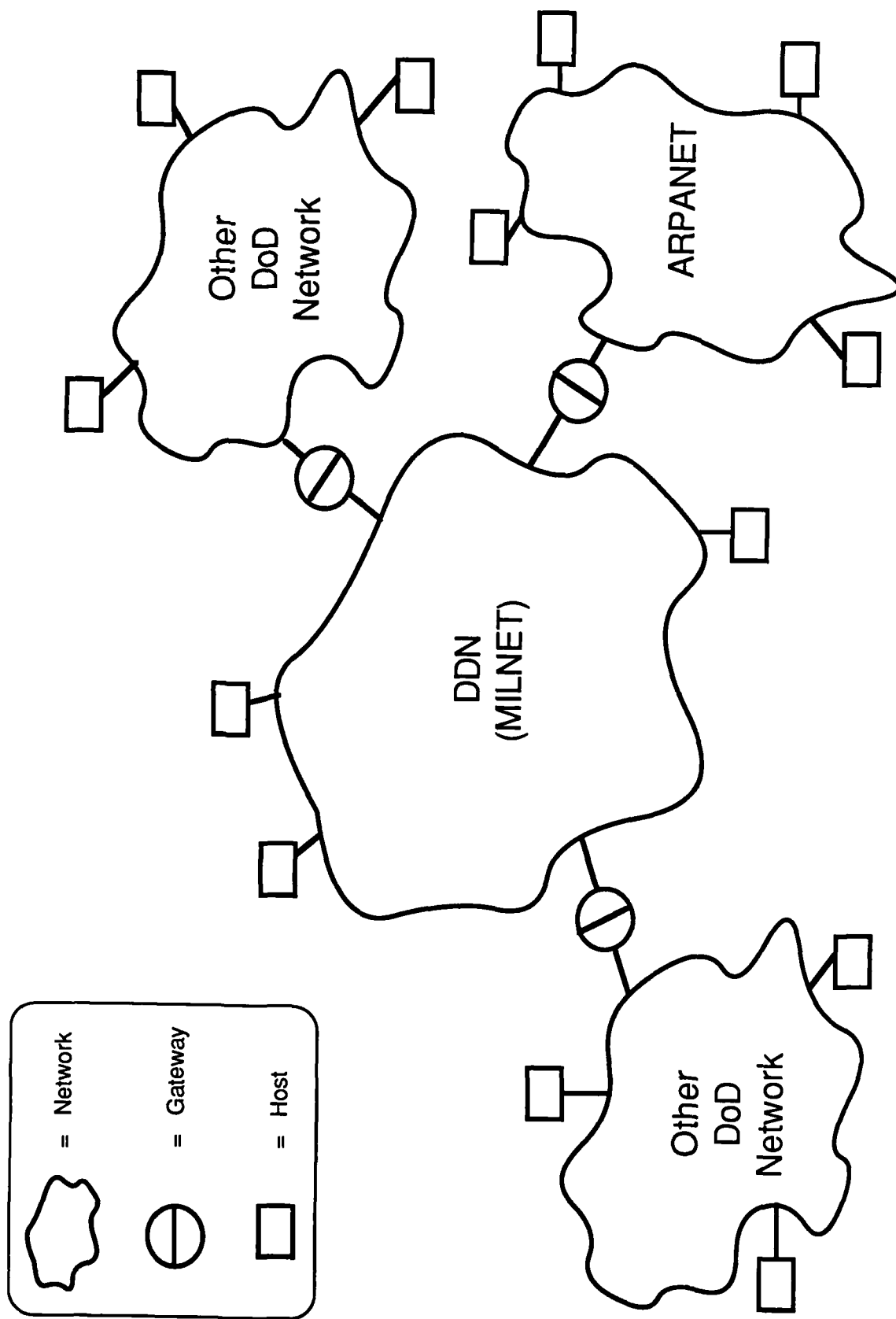
a) ISO

- The service definitions and protocol specifications for layers 3, 4 and 5 have been approved in final draft form (**DIS** and **IS**), though these are always subject to updates.
- The service definitions and protocol specifications for layers 1, 2, 6 and 7 are still in intermediate draft forms (**Working Draft** and **DP**).
- Note that representative protocols for layers 1 and 2 have preceded final approval of their layer service definitions and protocol specifications.
- Layer 3's services definition, already approved for **connection-oriented services**, is now being updated to include definitions for **connectionless services**.
- Layer 7 protocols, such as Virtual Terminal (VT); and File Transfer, Access, and Management (FTAM), are in **DP** form.

b) CCITT

- CCITT has adopted ISO's services definitions and protocol specs for layers 3, 4 and 5.
- CCITT has recently published the X.400 series of recommendations that define a standard electronic mail system, providing Application Layer functions.

The DoD Internetwork Environment



D. DoD Internet Protocol Suite

1) Background

- a) In 1969, the "grandfather" of all packet switching networks, the Arpanet, became operational.
- b) Research during the 1970's led to the Arpanet protocols, which were developed prior to any international or vendor standards.
- c) *These protocols have been changed relatively little in the past 10 years, other than the replacement of the Network Control Protocol (NCP) by the Transmission Control Protocol (TCP).*
- d) These Arpanet protocols, now referred to as the **DoD Internet Protocol Suite**, are used today by both the Arpanet community and the DDN communities.

2) Key Concepts

a) The DoD Internet Environment

- Within DoD, many computer networks are connected to form an **Internet** or **Catenet** (concatenated network).
- The individual networks are connected by **gateways**, which may reside in hosts but can be implemented by specialized processors.
- The largest network within the DoD Internet is known as the **MILNET**, and consists of over 100 packet switches.

DDN Dataflow Terminology

Data Unit

TELNET,
FTP
SMTP

MESSAGES

**TCP
SEGMENTS**

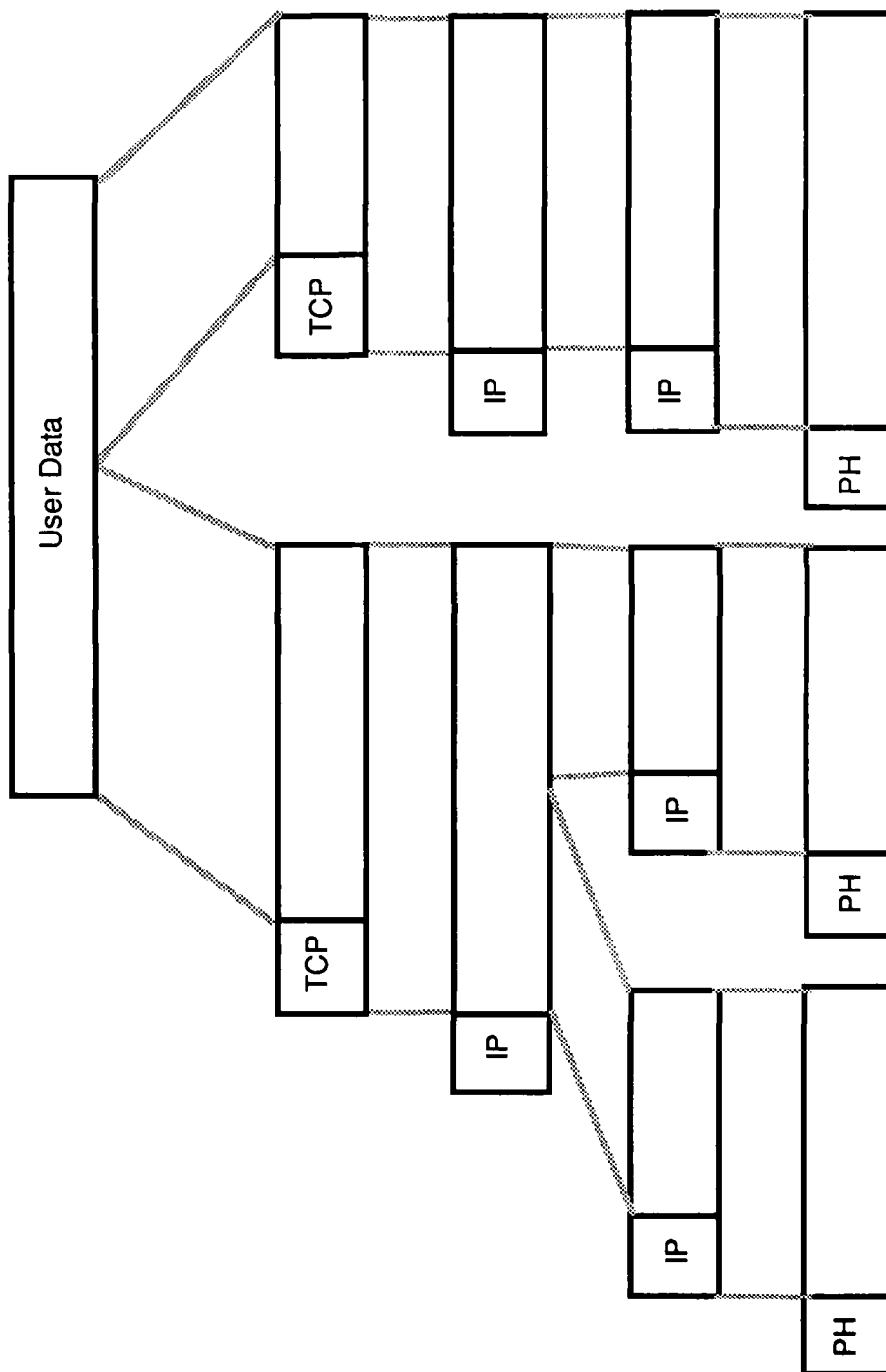
IP

DATAGRAMS

IP

FRAGMENTS

**X.25
PACKETS**



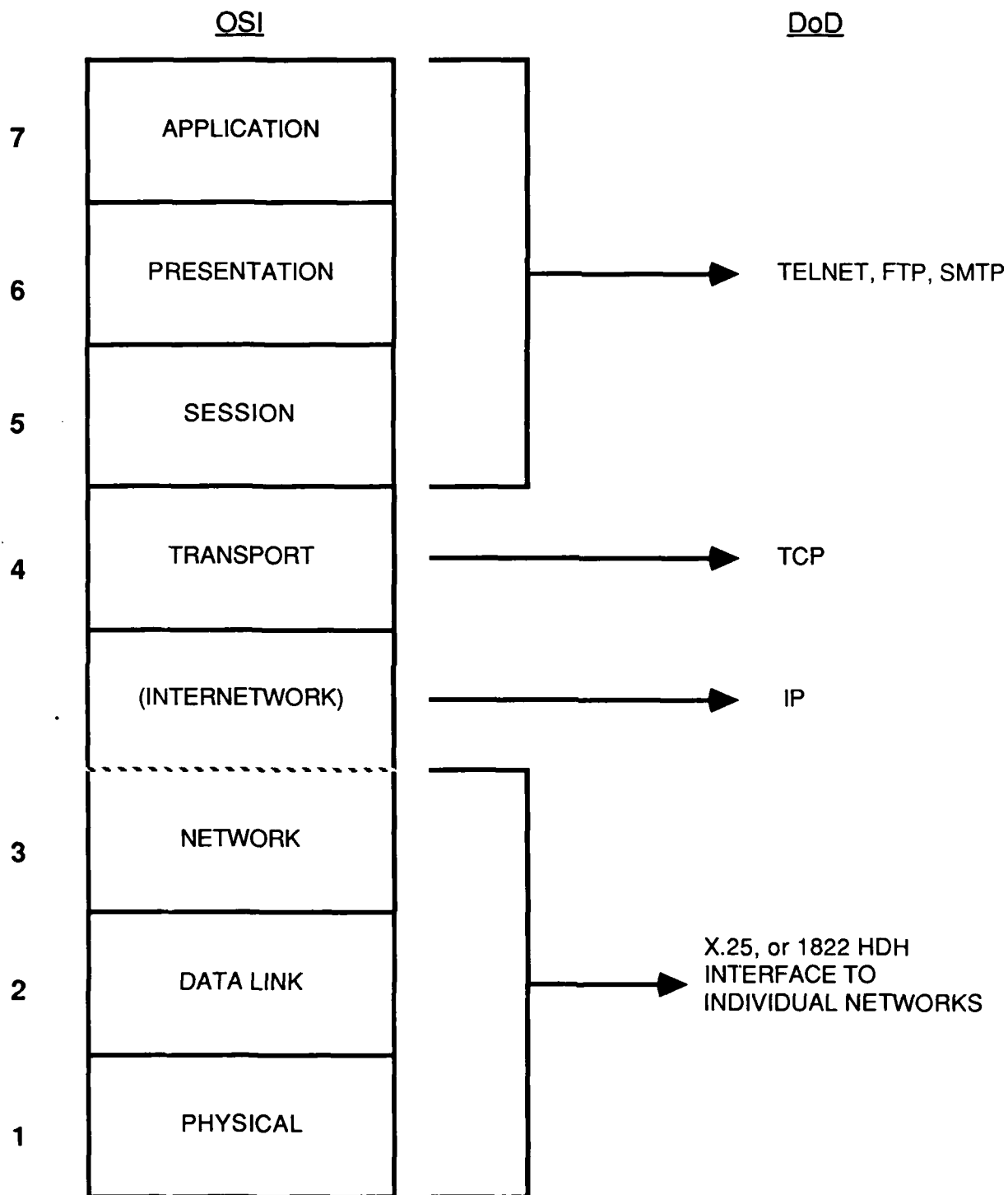
b) Internet Architecture

- The DoD Internet environment necessitates an internetwork architecture, in which the functions of the lowest three OSI equivalent layers are implemented by the individual networks, while layers 4 through 7 are common to the entire internet.
- Individual networks can use their own packet switching network protocols.
- Gateways and hosts that handle internetwork services must implement some or all of the higher layer protocols of the DoD Internet Protocol Suite.
- A gateway between networks must also have interfaces to each of the networks to which it is connected.
- The DoD Internet Protocol Suite adds another layer to the OSI model, the **Internetwork Protocol (IP) Layer**, between the Transport and Network layers. IP handles routing, addressing, etc., across **multiple networks**.
- The DoD Internet Protocol Suite use the packet switching services of the networks transparently. These protocols are unconcerned with the packetizing and routing algorithms used within an individual network, as long as internet messages are transported across them.

c) Dataflow Terminology: Segments, Datagrams, Fragments and Packets

- Messages are enveloped (at the OSI Transport Layer) into TCP **segments**. When internetwork headers are added these become IP **datagrams**. Thus end-to-end internetwork communication is performed using datagrams.
- At each gateway's interface to a network, a datagram may be broken up into datagram **fragments**, if the individual network cannot accept messages as long as the complete datagram. These fragments can be further fragmented at succeeding gateway/network interfaces, if necessary.
- The packet switches of an individual network envelope the fragments into **packets** for routing through that network, while message segmentation, formation of datagrams, and fragmentation take place outside of any individual network.

DoD Internet Protocol Functionality



3) The Layers and Protocols of the DDN

a) The Network Layer and Below

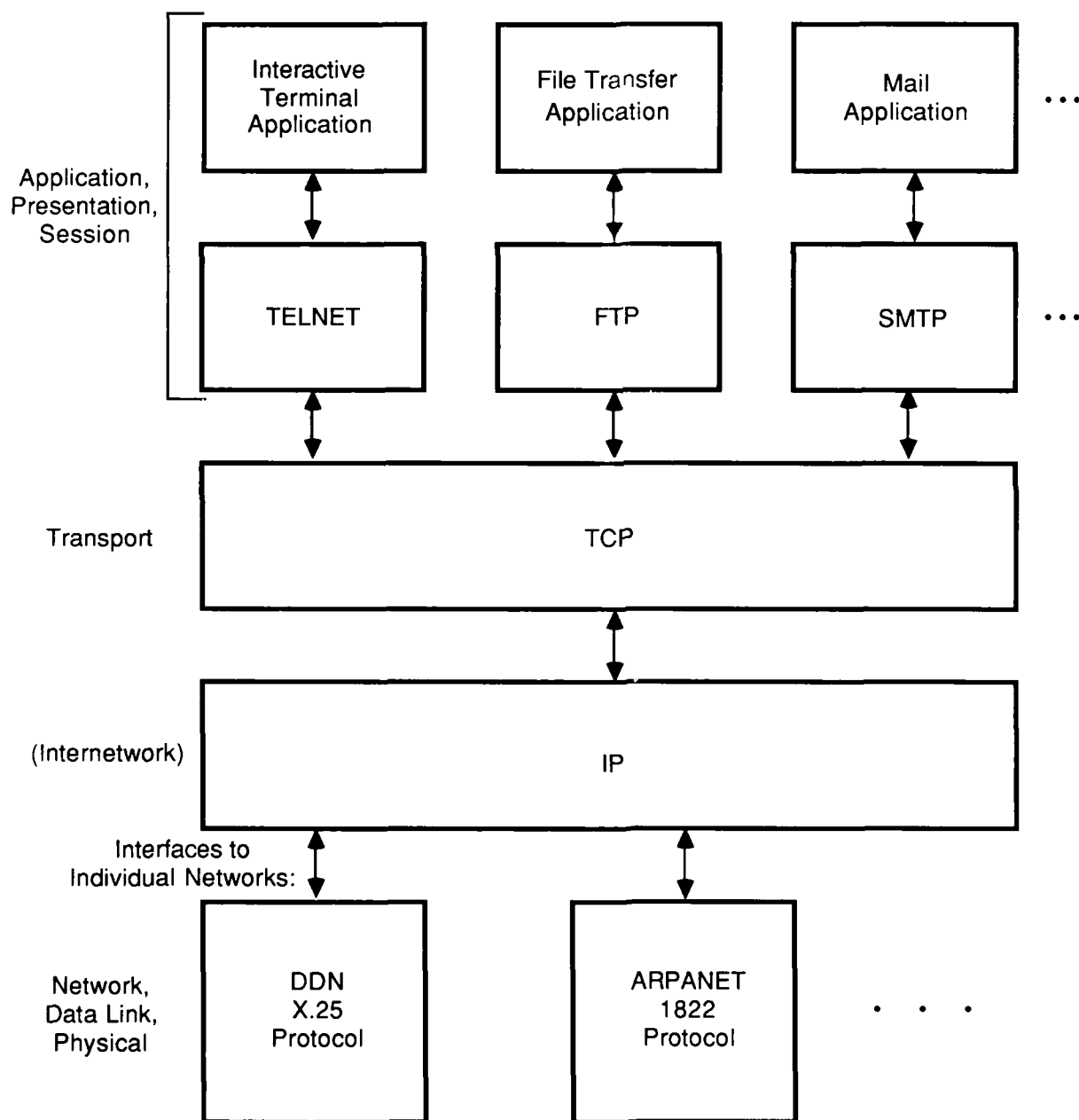
- Externally, the DDN supports two different network access protocols: X.25 and 1822 HDLC Distant Host (HDH). These protocols also encompass the bottom 3 OSI layer functions, and specify how hosts and gateways transmit their data into and receive it from the DDN. They are interfaces to the level 1, 2 and 3 functions provided by the DDN.

b) The Internet Protocol (IP)

- The Internet Protocol (IP) is used to move datagrams end-to-end across one or more networks through intermediate gateways.
- IP does not provide end-to-end reliability, flow control or sequencing of data. These are OSI Transport Layer functions provided by TCP.
- The DoD Internet provides **datagram service** when traversing network boundaries, as compared to the **virtual circuit** service provided by X.25 within a single network.
- IP does provide internetwork addressing, routing and fragmentation/reassembly. These are Network Layer functions provided on an internetwork level. Thus IP adds its own layer, the Internetwork Layer, between the OSI Transport and Network layers.
- IP interfaces with TCP above, and with an individual network's access protocol below.
- IP must reside in all hosts and gateways involved in internetwork communication.
- IP adds its own header to datagrams and datagram fragments for routing across the DoD Internet.

The Layers And Protocols Of The DcD Internetwork Environment

OSI FUNCTIONALITY



c) Transmission Control Protocol (TCP)

- The Transmission Control Protocol (TCP) provides OSI Transport Layer functions.
- TCP is a connection-oriented, process-to-process reliable protocol operating in a multinet environment where individual networks may be unreliable.
- TCP is connection-oriented. Host processes are assigned to **ports**. TCP then establishes a connection between two ports. These can be on different hosts in different networks.
- TCP interfaces above (providing services) to user-written application programs, or DoD presentation layer protocols (Telnet, FTP, SMTP).
- Process messages are broken up by TCP into segments, which include TCP transport headers plus some part of the original message. These are handed to IP which adds its own header to form datagrams. IP takes care of fragmenting and reassembling datagrams, while TCP reassembles messages from segments.
- TCP and IP work together, sharing header information to provide different precedence and security levels.
- As a result, each host involved in internet communication must implement TCP/IP.
- Note that internetwork addressing is not transparent. Each address must be known by all network end user systems. This is another reason why each interconnected host must implement TCP/IP.

d) Telnet, FTP and SMTP

Telnet, FTP and SMTP all perform functions of the OSI Session, Presentation and Application Layers.

- Telnet

Telnet, a virtual terminal protocol, uses TCP to set up a connection between two host ports. This is used for host-to-terminal communication by providing conversion to and from a standard (virtual) terminal protocol, with standard control characters.

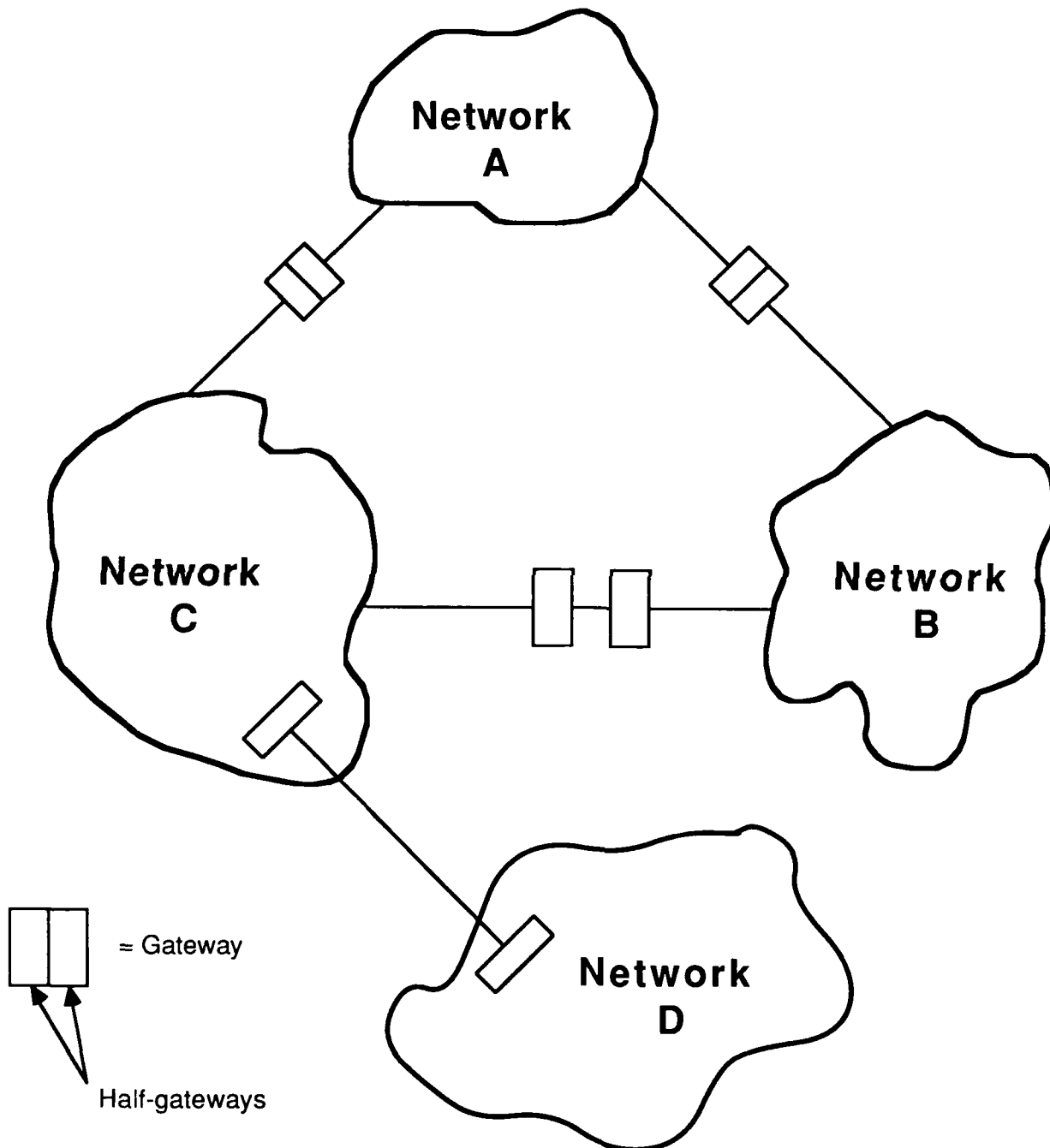
- File Transfer Protocol (FTP)

- The File Transfer Protocol (FTP) provides a standard set of commands for file manipulation.
- FTP allows users to access file storage systems on remote hosts without having to learn the different file management commands particular to each host.
- For example, a user-FTP process establishes a Telnet connection with a server-FTP process, over which FTP commands and replies are sent. A separate data connection is used for the actual file or record transfers.
- Some transformation of file data and format is available in FTP.

- Simple Mail Transfer Protocol (SMTP)

- The Simple Mail Transfer Protocol (SMTP) is a set of commands that allow users at different hosts to send and receive electronic mail.
- SMTP specifies the procedures for sending and forwarding mail messages, obtaining and updating mailing lists, and sending mail to terminals instead of mailboxes.
- SMTP requires a reliable process-to-process transport service, provided by TCP.

Internetworking



E. The DoD Approach to Internetworking

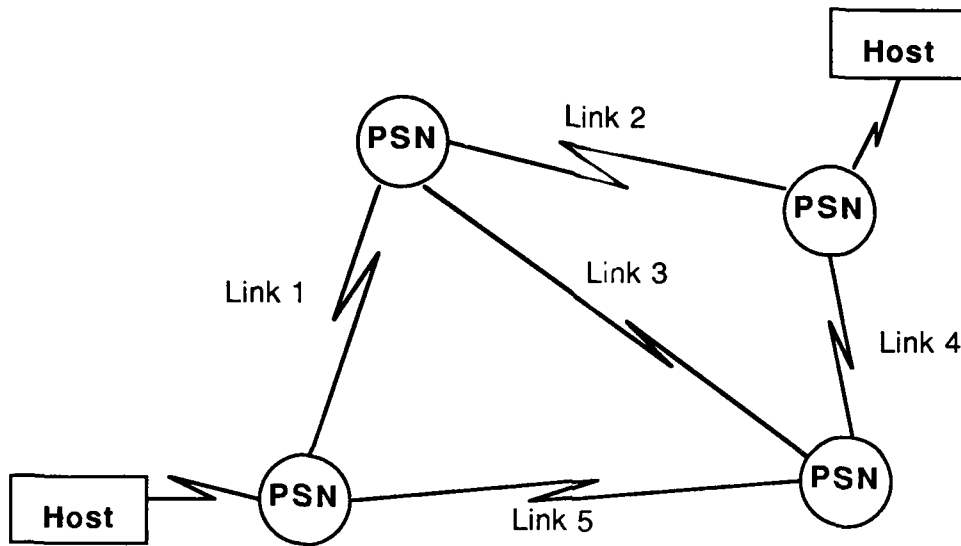
1) Requirements for Interconnection

- a) Allow individual networks to operate in concert as though they were a single network, giving users access to applications, databases and hardware resources in other networks
- b) Retain **network independence**, because:
 - Most traffic is **intra-network**
 - Each network has its own environment (different user groups, security levels, throughput requirements, nature of data)
 - Networks may have different protocol architectures and routing algorithms
 - Need separate network management
 - Keep address/name spaces separate
 - Networks can be modified without impacting other networks
- c) Existing networks can be tied together without redefining them (to avoid overlapping network addresses)
- d) Large networks can be built without danger of running out of address space (insufficient number of network addresses)

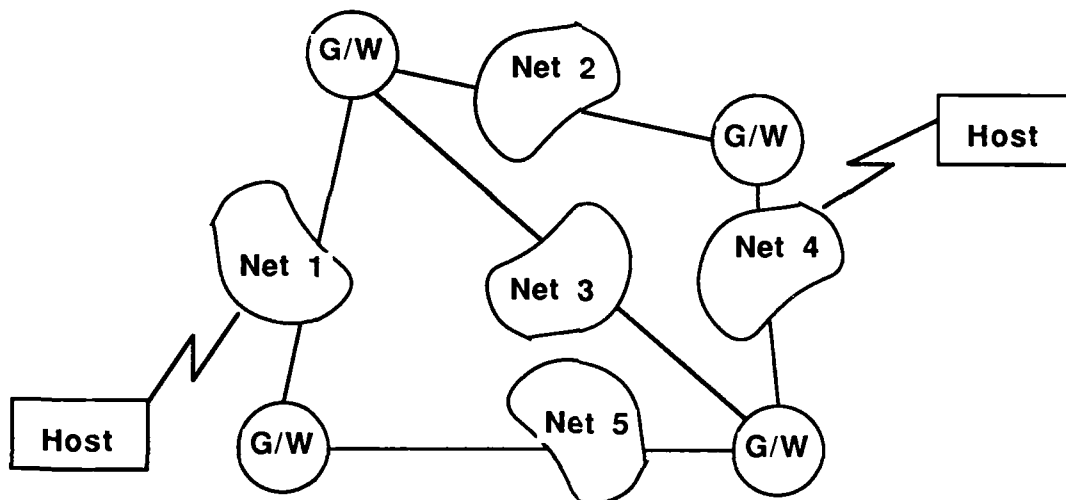
2) Internetwork Gateways

- a) An **internet gateway** provides an interface between two or more networks, allowing users to pass messages from one network to another.
- b) Networks can be connected to each other via gateways to form an "**internet**".
- c) Gateways are often described in terms of **half-gateways**, where each half interfaces to an individual network.
- d) Can be implemented by a dedicated host, packet switch, or host pair (with one half-gateway in each host)
- e) Gateways may provide: virtual circuit or datagram service across multiple networks, protocol conversion between different transport and network layer protocols, fragmentation/reassembly, and network access authorization checks

The Meta - Network



Network



Meta-Network

3) The Meta-Network Concept

- a) A packet-switching **network** is composed of multiple packet switching nodes (PSNs), interconnected via data links (typically leased circuits with modems or DDS circuits with DSUs).

A routing protocol is used between PSNs to exchange status information about the network (e.g., which links are up or down).

In the DDN and the Arpanet this protocol is called the IMP-to-IMP Protocol (IIP).

IIP supports an adaptive routing algorithm within the network. PSNs can reroute packets around links on PSNs that have failed or are congested.

- b) A packet-switching **meta-network** is composed of multiple gateway nodes (G/Ws), interconnected via entire networks (typically packet switching networks like the Arpanet, Milnet or DISNET).

A routing protocol is used between gateway nodes to exchange status information about the meta-network (e.g., which networks are up or down).

In the DoD Internet this protocol is called the Gateway-to-Gateway Protocol (GGP).

GGP supports an adaptive routing algorithm on the internet level. Gateways can reroute datagrams around networks or gateways that have failed or are congested.

- c) The GGP is very similar to IIP, except that it provides routing information *between gateways*, instead of between IMPs. At a PSN, routing tables are used to determine the next link that a packet should use for transmission across the network.

At a gateway node, routing tables are used to determine the next network that an internet datagram should use for transmission across the meta-network (e.g., DoD Internet).

4) DoD Gateways

- a) Gateway nodes are implemented as hosts on each packet-switching network to which they are directly link-attached.
- b) Gateway nodes function as inter-network switches in the meta-network.
- c) Within the DoD Internet, there are two types of gateways: **internal** gateways and **external** gateways.
- d) *Internal Gateways* within an internet are provided by a single vendor and controlled as a single "core autonomous system". In the DoD Internet, the internal gateways are provided by BBN and implemented by PDP-11 minicomputers. GGP is an example of a class of protocols generically called Internal Gateway Protocols (IGP).
- e) *External Gateways* are typically implemented by subscriber organizations and are controlled separately from the DoD Internet core autonomous system.

If a subscriber implements a Local Area Network (LAN) and connects it to the DoD Internet via a gateway, the LAN gateway node would be considered an external gateway. The protocol used between the LAN external gateway and a DoD Internet gateway to coordinate routing and control of information is an example of an **Exterior Gateway Protocol (EGP)**.

Comparison Of Layering In Major Architectures

Layer	OSI	DoD Internet	SNA	Decnet
7	Application	TELNET FTP SMTP	End User	Application
6	Presentation		Presentation Services	
5	Session		Data Flow Control	
4	Transport	Transmission Cntrl (TCP)	Transmission Control	(None)
3	Network		Path Control	Network Services
				Transport
2	Data Link	Internetwork (IP) X.25 level 3 1822 level 3	Data Link Control (SDLC)	Data Link Control (DDCMP)
1	Physical	Physical	Physical	Physical

F. Comparison of the Major Computer Network Architectures

1) OSI Physical and Data Link Layers

- a) All four major architectures implement the same basic functions at these lower levels.
- b) Physical standards are usually RS-232 or V.35, and some subset of HDLC is used at the data link layer.

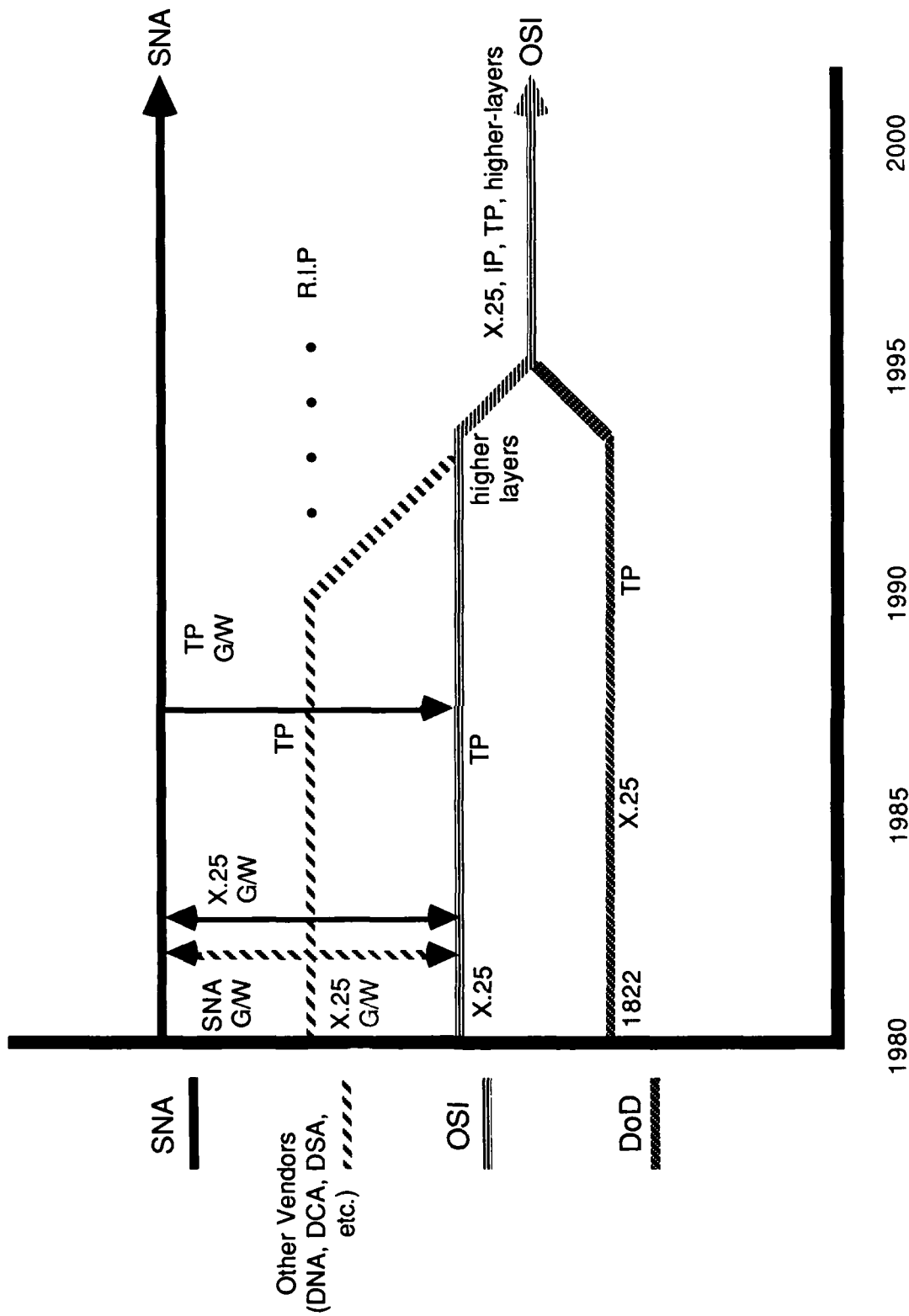
2) OSI Network and Transport Layers

- a) SNA Path Control, DECnet, and the DoD protocols all conform essentially to the OSI Reference Model, and implement reliability in separate Transport Layer protocols. (While SNA includes end-to-end packet sequence numbers at level 3, they are used at level 4).
- b) SNA provides virtual circuit service at the Network Layer, while DECnet uses datagram service at level 3 and the DoD protocols assume unreliable datagram service from the individual networks.

3) OSI Session Layer

- a) SNA splits the functions of this layer:
 - Transmission Control moderates the rate of data flow for a session
 - Data Flow Control toggles the direction of data flow during a session
- b) DECnet currently has no formal Session Layer. Each application must perform Session Layer functions (i.e., establish and maintain sessions).
- c) DoD Internet Protocols integrate Session Layer functions in Presentation / Application Layer protocols (Telnet, FTP, SMTP).

Architectural Migration



G. The Future of Computer Network Architectures

1) The Emerging Dominance of Two Architectures

- a) OSI
- b) SNA

2) The Future of OSI

- a) Developing protocol standards for layers 4-7 (beyond X.25)
- b) Migration of many commercial architectures towards OSI

DEC's DNA and Honeywell's DSA (Digital Systems Architecture) both implement existing international standards conforming to the ISO Reference Model, and are dedicated to supporting future standards.

c) The DoD Internet Protocol Suite converges with OSI

1. DoD architecture moves towards OSI

- X.25 is supported as a DDN network access protocol.
- DoD to eventually replace TCP with ISO/NBS Transport Protocol Class 4 (TP4)

2. OSI moves towards DoD architecture

- TP4 is functionally equivalent to TCP, supporting reliable communication over unreliable networks.
- ISO's new Internet Protocol is based heavily on DoD's IP. It will provide internet datagram service across PDNs, effectively adding an INTERNETWORK LAYER to the OSI model.
- Future OSI layer 5, 6 and 7 protocols are being strongly influenced by DoD high level protocols such as TELNET, FTP, and SMTP.

3) SNA - OSI Compatibility

- Very few functional differences
- X.25 interfaces to SNA networks
- SNA/OSI gateways with upper layer protocol conversion currently under development

SECTION III

THE DDN NETWORK AND THE DoD PROTOCOL SUITE

**OBJECTIVES
OF
THE DDN AND THE DoD PROTOCOL SUITE**

- **To appreciate the importance of the DDN dynamic routing algorithm in providing survivability of the network, particularly during conditions of stress.**
- **To become familiar with the network components, their functions, and the monitoring capabilities provided by the network Monitoring Center so that the student knows the equipment the network provides, how that equipment is monitored, and procedures to follow for getting network related problems resolved.**
- **To know the performance objectives of the DDN architecture to enable the subscriber to configure his network connection to meet his system's requirements.**
- **To understand the levels of security which will be provided by the DDN and the time frame for their implementation so that the student can begin planning the migration of his secure network to the DDN.**
- **To understand the key functional aspects of the DoD protocol suite so that the student will understand the implications of his alternatives in terms of the software needed to connect his system to the DDN and to make it interoperable with other systems on the DDN.**

"All DoD ADP systems and data networks requiring data communications services will be provided long-haul and area communications, interconnectivity, and the capability for interoperability by the DDN. Existing systems, systems being expanded and upgraded, and new ADP systems or data networks will become DDN subscribers. All such systems must be registered in the DDN's User Requirements Data Base (URDB)."

**Office of the Secretary of Defense,
10 March 1983.**

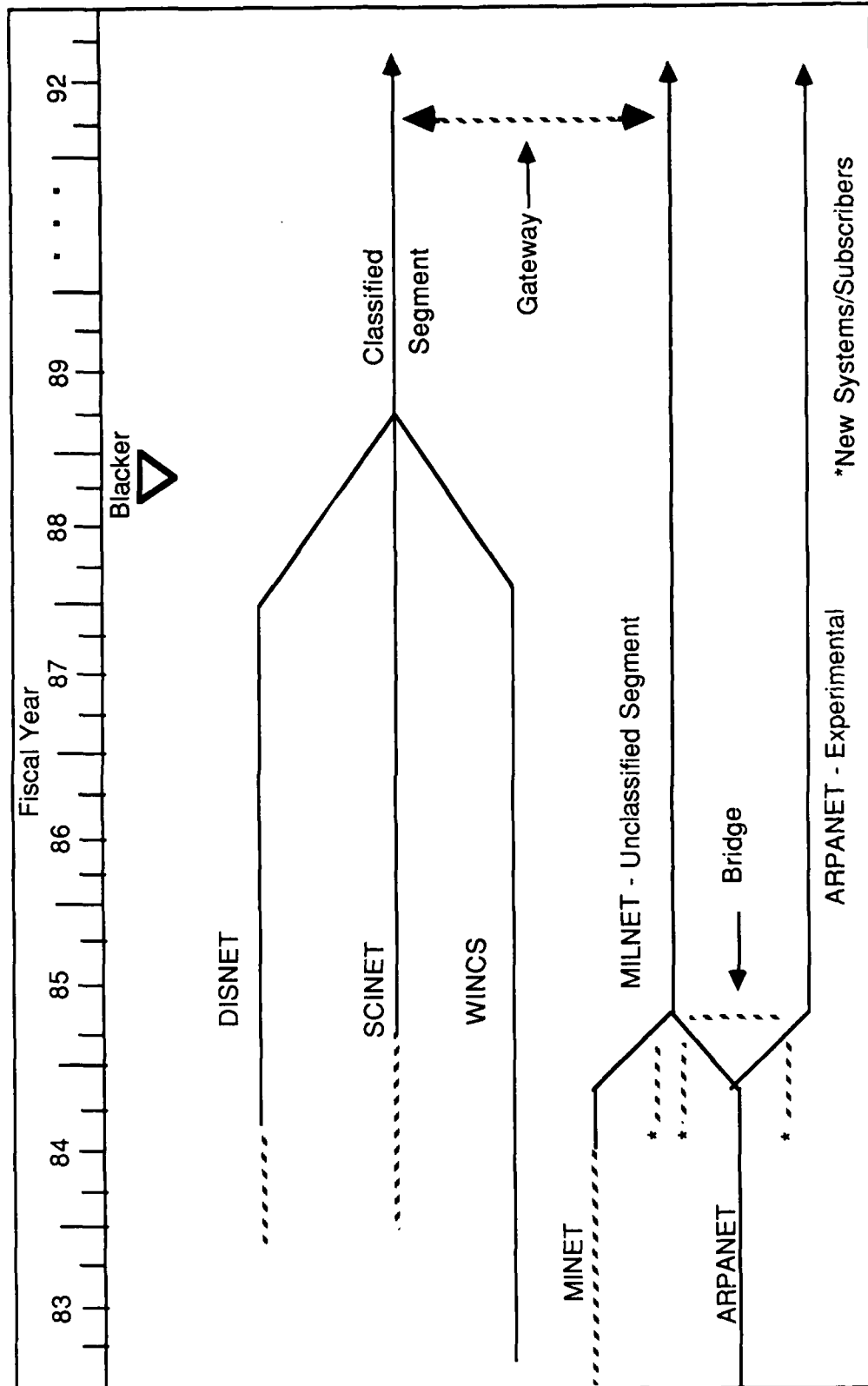
5. The Defense Data Network - Overview

A. Introduction to the DDN

1) Origins of the Defense Data Network

- A study was conducted in 1981 to evaluate the use of AUTODIN II technology vs. ARPANET technology for an integrated DoD data network.
- A plan was formulated for the development of a data network based on ARPANET technology that would provide a low risk, cost effective and expandable system. The proposed Defense Data Network would satisfy worldwide wartime survivability requirements and meet the service and security requirements supplied by the OJCS.
- The DCA and Defense Science Board determined that ARPANET technology was the most promising due to its proven technology and its inherent survivability.
- AUTODIN II project was terminated in April of 1982 .
- Defense Data Network project began 2 April 1982.

SCHEDULE



2) Scope of the Milnet Segment of the Defense Data Network

a) Geographic Distribution of Switching Nodes

By the end of 1986, the DDN will be composed of approximately 174 switching nodes interconnected by 300 leased circuits and satellite backbone links located throughout the Continental US, the Pacific, and Europe.

- European Milnet – 44 PSNs, 81 links (1987)
- Pacific Milnet – 14 PSNs, 28 links (1986)

b) Host Systems and Terminals Supported

There are currently some 340 hosts and 2,500 terminal type devices, not including backside connections, operational on the DDN. Another 1,700 hosts have been identified and have ports reserved.

c) Services Offered

- Basic data transport from 9.6 kbps to 56 kbps
- Link encryption
- Asynchronous terminal support
- Internetwork communications
- Interoperability between diverse hosts systems in terms of file transfer, electronic mail formats, and terminal access

d) Future Services

- Bisynchronous terminal support
- Host-to-host encryption
- Multilevel security
- Guard gateways

NO-A173 472

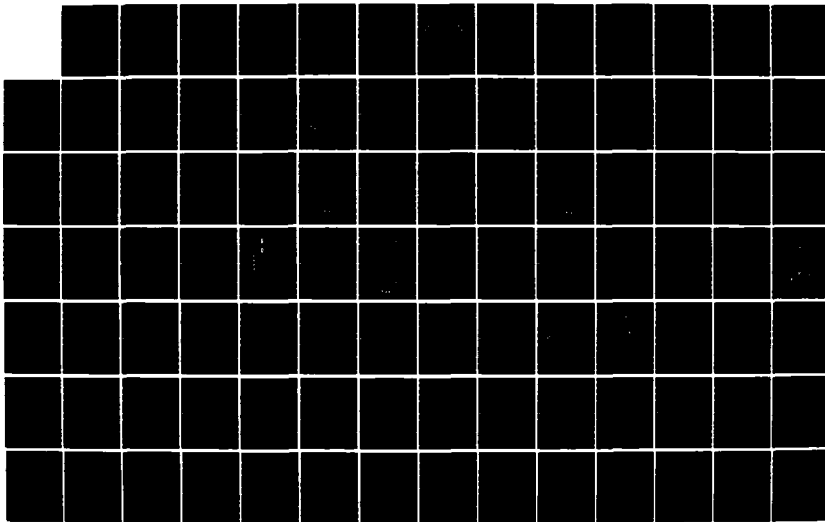
THE DDN (DEFENSE DATA NETWORK) COURSE(U) NETWORK
STRATEGIES INC FAIRFAX VA R DE VERE ET AL. APR 86
DCA100-83-C-0062

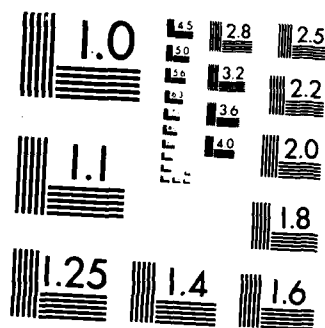
2/4

UNCLASSIFIED

F/G 17/2

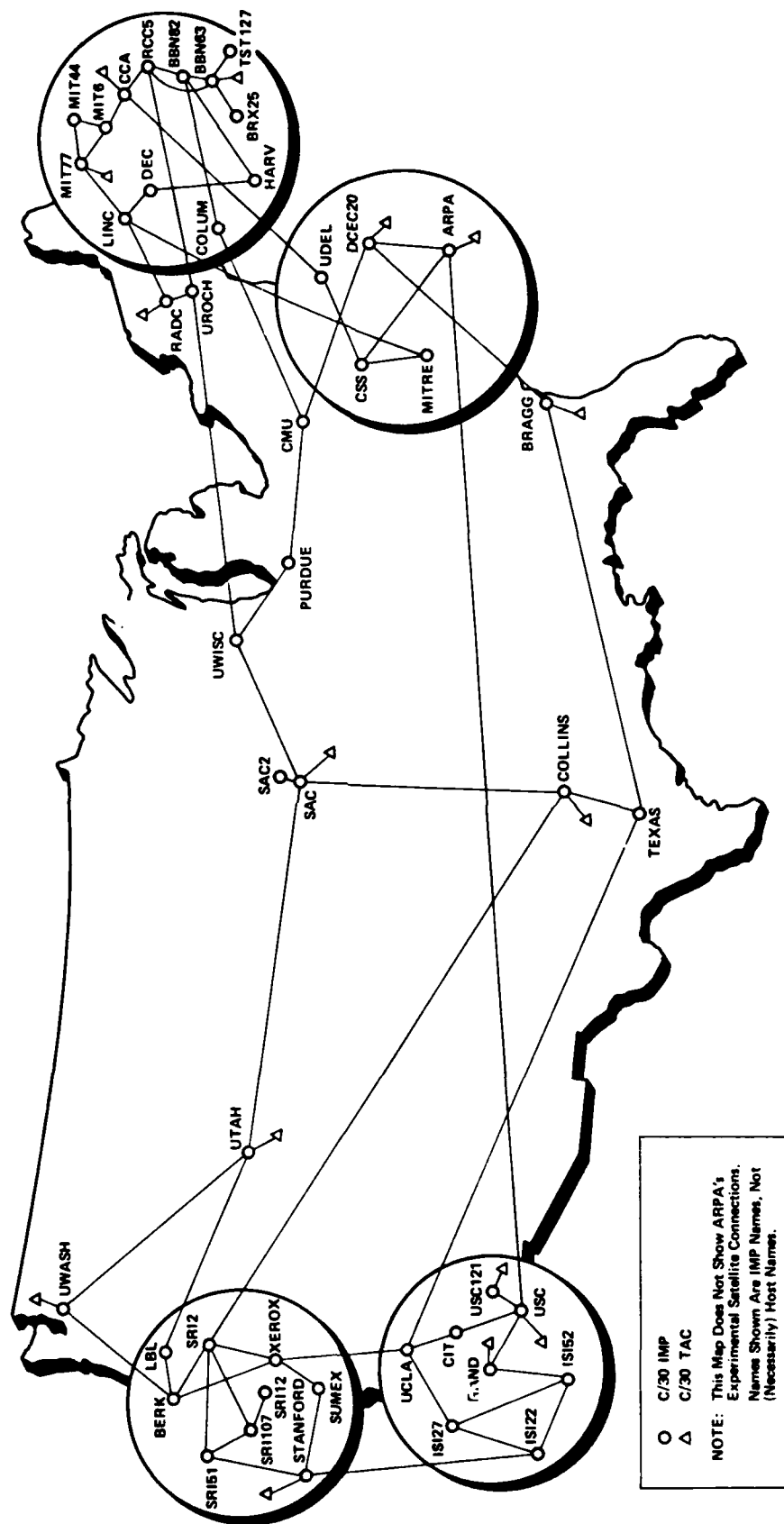
NL



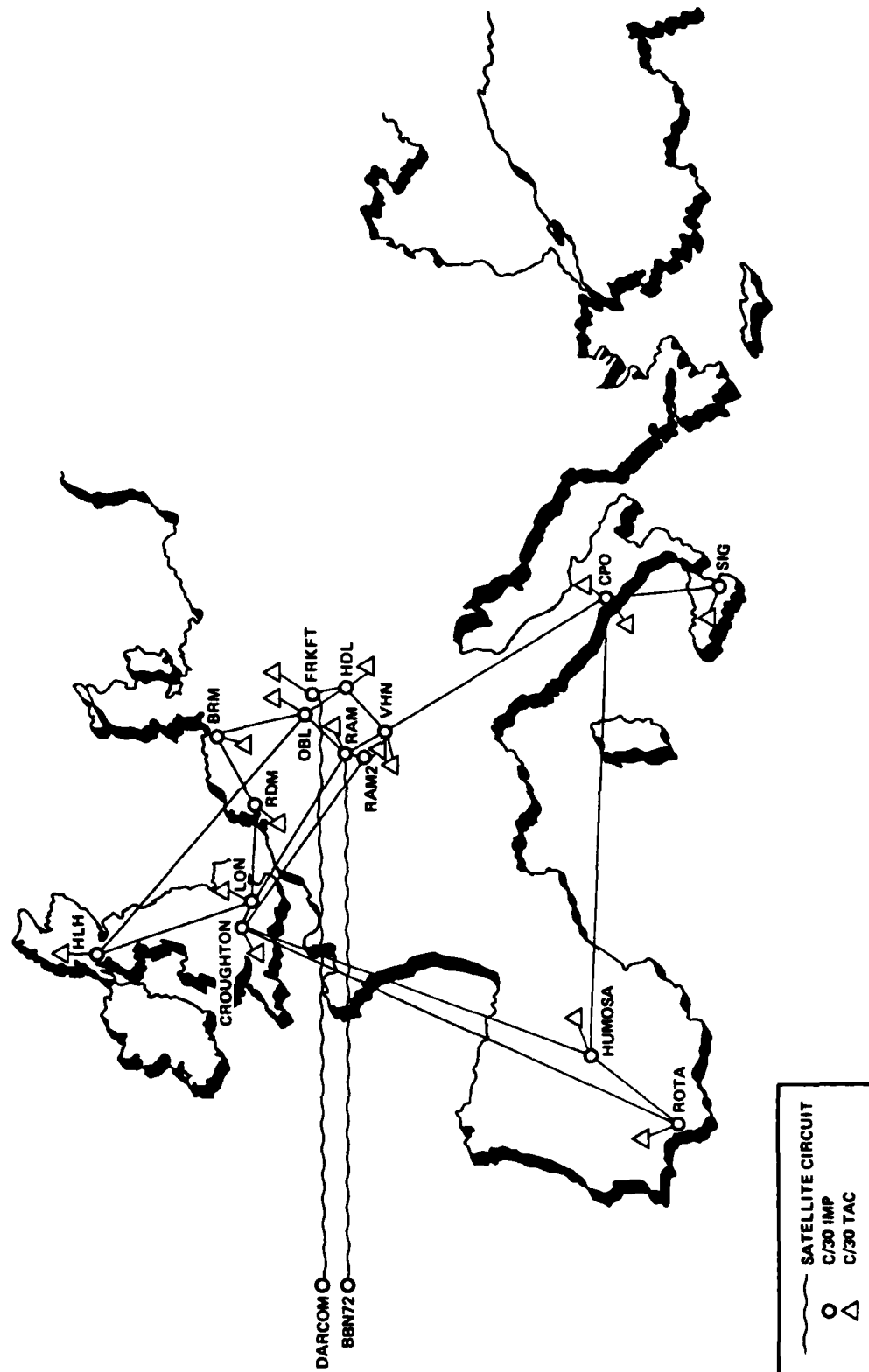


MICROCOPY RESOLUTION TEST CHART
NATIONAL BUREAU OF STANDARDS 1963-A

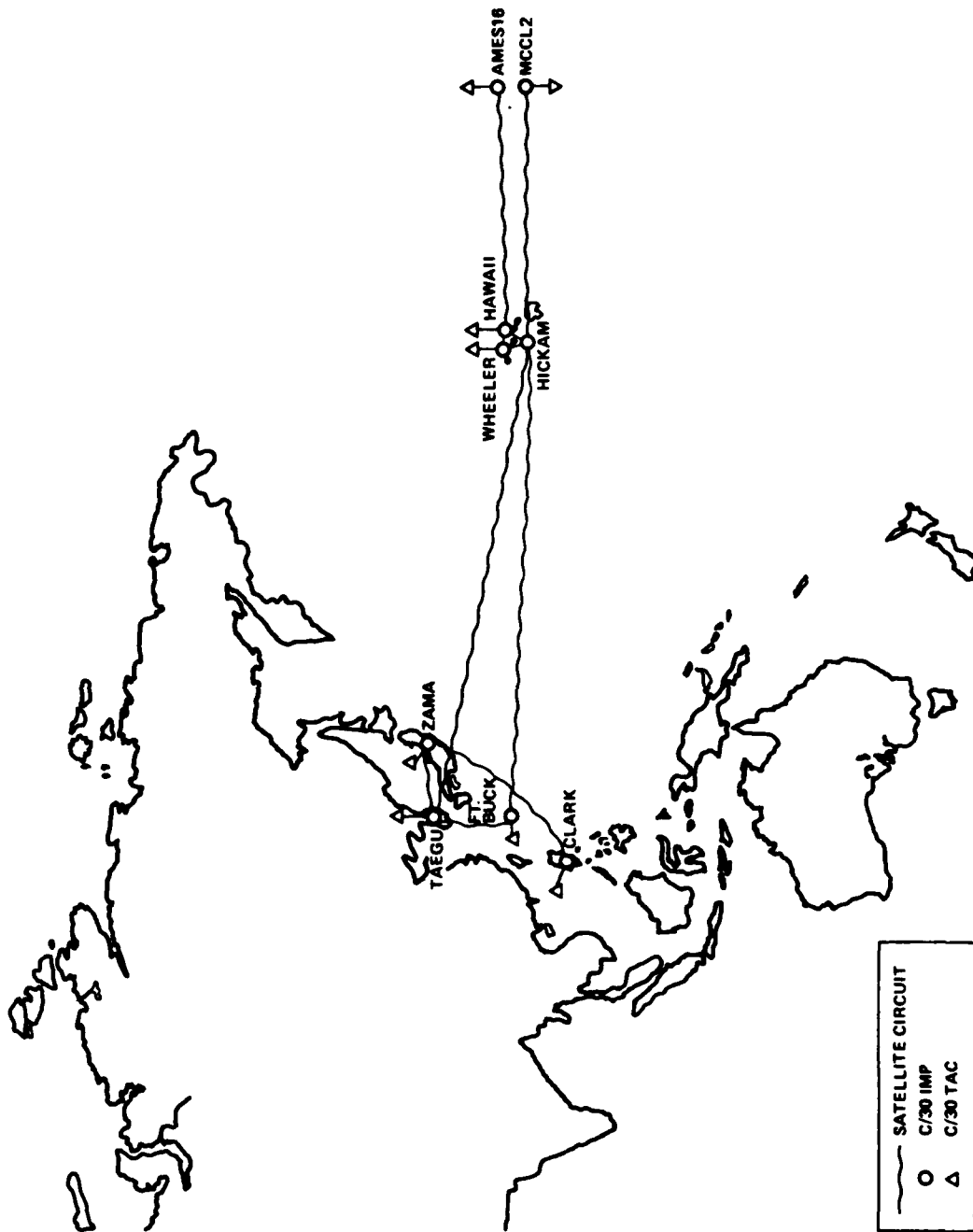
ARPANET Geographic Map, 31 January 1986



European MILNET Geographic Map, 31 January 1986



Pacific MILNET Geographic Map, 31 January 1986



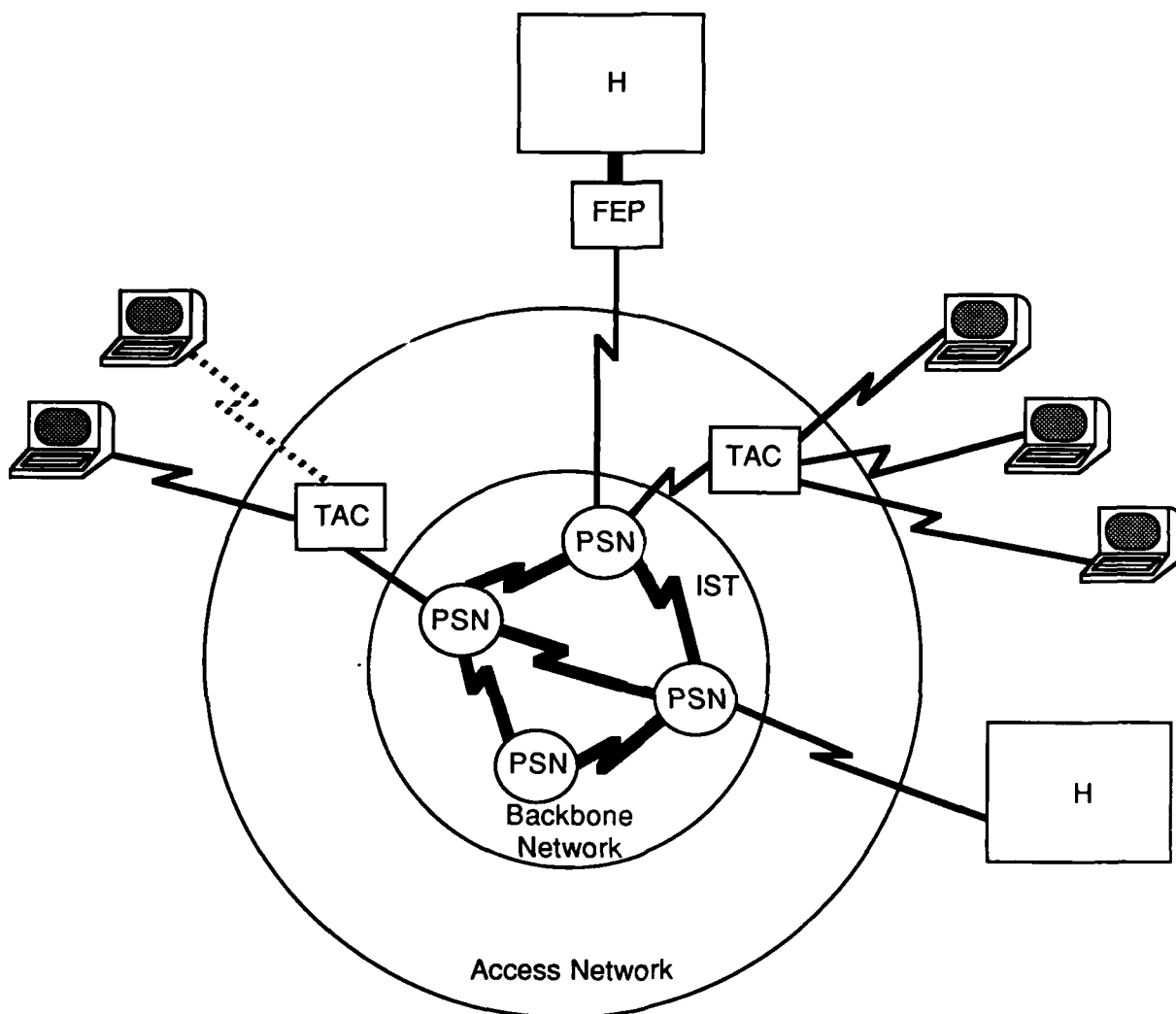
3) Goals of the DDN

The DDN has been designed to meet the specific data communications requirements of the DoD.

- a) *Interoperability* — support communication between diverse computer systems and terminals
- b) *Survivability* — provide the ability to automatically reconstitute the network without operator intervention
- c) *Cost Savings* — achieve "economies of scale" cost benefits by combining communications requirements of many users over a common backbone
- d) *Performance* — provide the high level of availability, low response time, and low error rate necessary for military applications
- e) *Precedence and Preemption* — accommodate the precedence and preemption features required by military applications to ensure that vital time-sensitive data can "get through"

4) DDN Security and Privacy

- a) End-to-end encryption — security level separation of classified subscriber traffic.
- b) Link encryption — on backbone trunks and access lines
- c) Physically secure facilities — for packet switches and terminal access devices
- d) TEMPEST certified packet switches and terminal access devices for classified networks
- e) Terminal access restriction via passwords



5) Technical Overview of the Defense Data Network

a) Design Criteria

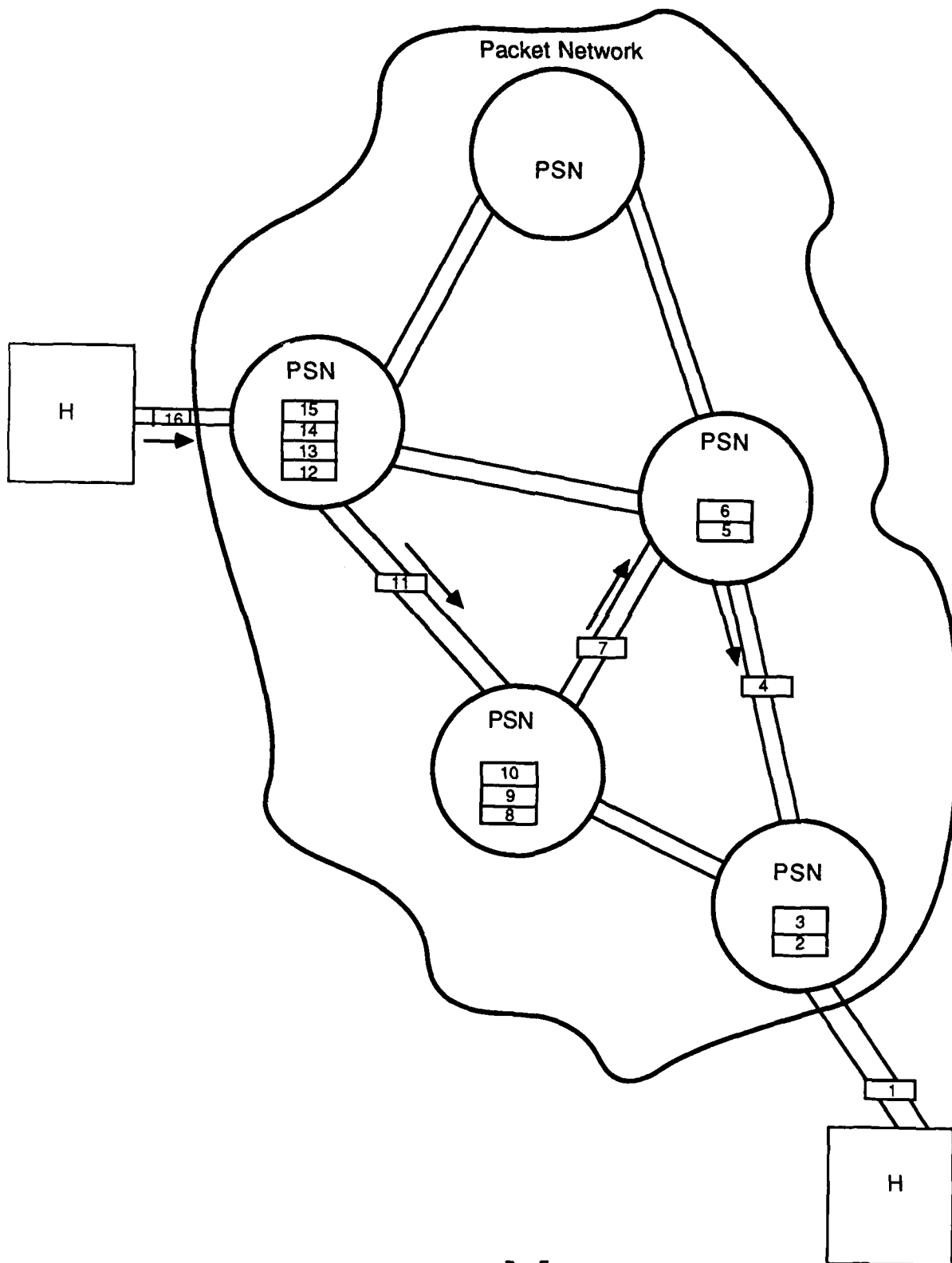
- Low risk, cost effective system that can be implemented in a short time frame and can support DoD communications requirements through the 1990s.
- Design is based on proven technologies — most of the hardware, software, and operations and maintenance procedures were adopted or adapted from existing operational networks, i.e., the ARPANET.
- Switching nodes and subscribers can be added or removed at low incremental cost and without impacting the operations of the network or other subscribers.
- The switching nodes employ a routing algorithm that will automatically adapt to new topologies in the event of failure of any network component.

b) DDN Functional Areas

The DDN is an integrated packet switching network composed of two functional areas — the Backbone Network and the Access Network.

- 1) **Backbone Network** is composed of Packet Switching Nodes (PSNs) and high speed inter-switch trunk circuits (usually 56 Kbps digital or 50,000 bps analog circuits) that interconnect the packet switches. PSNs support only host interfaces, and, therefore, anything connected to a PSN must look like a host.
- 2) **Access Network** is composed of leased circuits, dial-up circuits, and equipment necessary to connect host computers and terminals to the PSNs and the backbone network.

STATIC ROUTING



B. DDN Packet Routing Technique

One of the principle differences between the Defense Data Network and Public Data Networks or commercial Value Added Networks is its unique packet routing algorithm. This routing algorithm was adopted by the DoD because of its ability to meet the specific needs of the defense community in the areas of survivability and hands-off network control.

The details of a packet routing algorithm are transparent to users of a network as the algorithm is implemented only in the packet switches themselves.

1) Introduction

Packet routing algorithms are the processes by which a network of packet switches decides how to route each user's traffic from source to destination. There are two basic categories of routing algorithms as mentioned in Chapter 2 — Static and Dynamic.

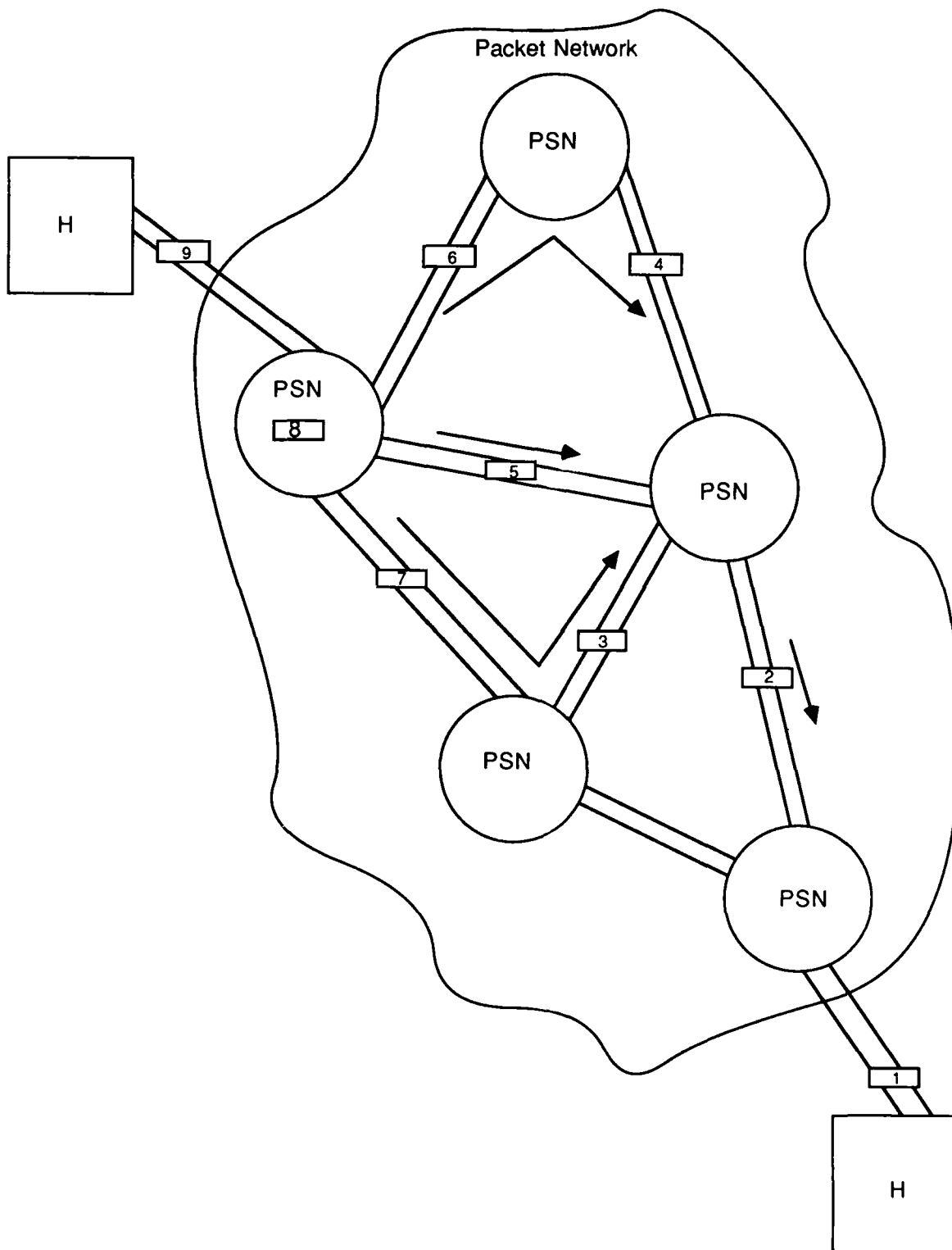
a) Static Routing Algorithms

The path through the network, i.e. the nodes and inter-switch trunks (ISTs), are determined at the time of call setup and remain static throughout the length of the call. All packets follow the same physical path unless a failure occurs, in which case the network may be able to re-establish a connection over a different route.

Examples of packet networks using static routing algorithms:

- Tymnet
- Telenet
- Uninet

DYNAMIC ADAPTIVE ROUTING



b) Dynamic Adaptive Routing Algorithms

In dynamic adaptive routing, the path through the network may differ for each packet from a given user. The path of any packet depends on a decision made by the routing algorithm as to which route is best at the time that packet arrives at a switching node. In most networks, the "best" route is usually the one that offers the least total delay. This type of algorithm has the advantage that it can dynamically alter the route of a user's data stream due to changes in network status such as failures or congestion.

Examples of packet networks using dynamic routing algorithms:

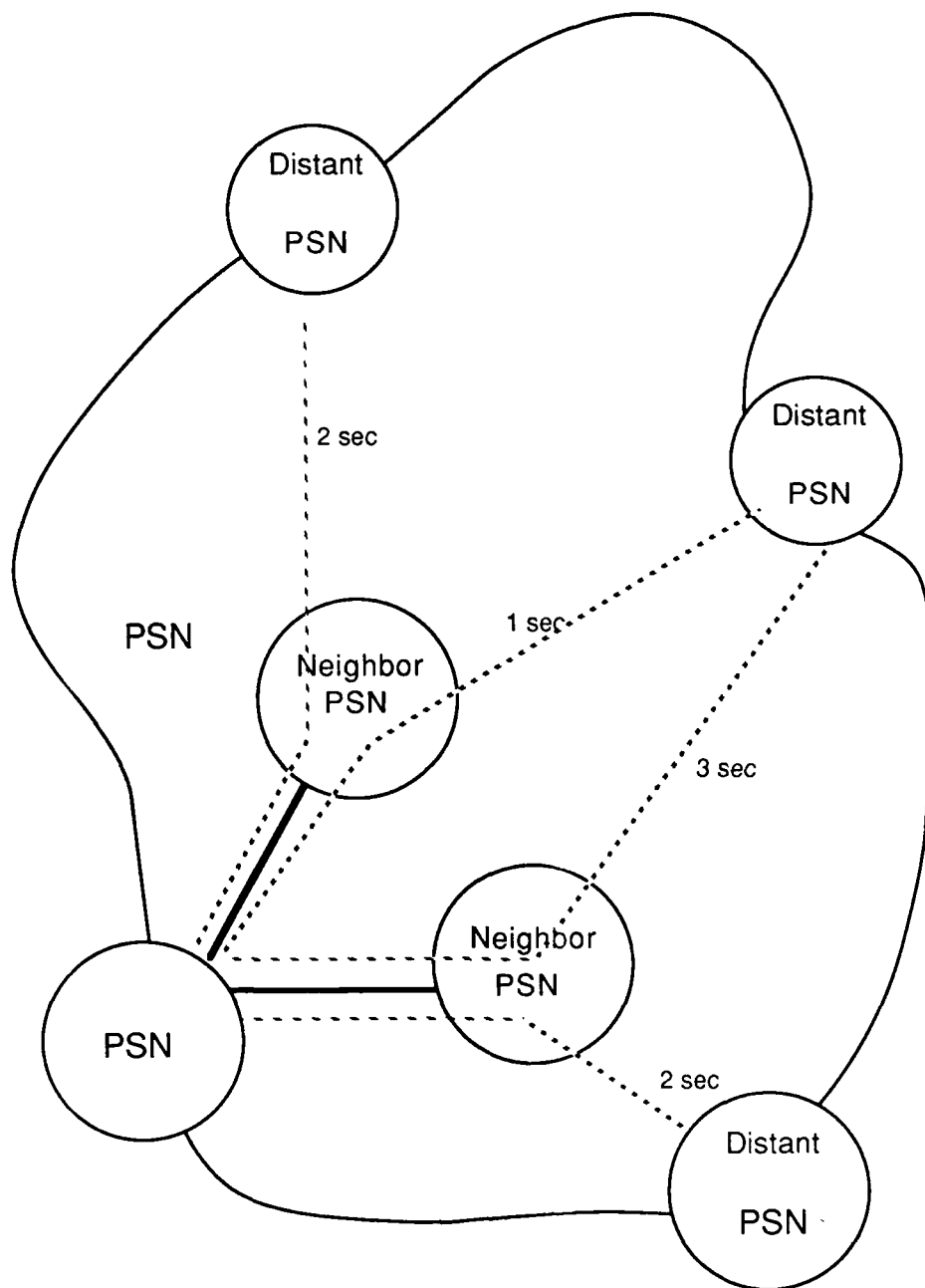
- DDN
- ARPANET

2) Background of the DDN Packet Routing Algorithm

- a) Initially developed at BBN as part of the ARPANET project in the late 1960s
- b) Refined and fine tuned over the years by universities and BBN

3) DDN Design Goals

- a) Employ dynamic adaptive routing — very survivable
- b) Accommodate large numbers of nodes and destinations
- c) Provide completely distributive control — no single point of failure



4) Description of DDN Routing Algorithm

The dynamic adaptive routing algorithm of the DDN provides the capability for each node automatically to route traffic so as to bypass congested, impaired, or damaged interswitch trunks and/or packet switch nodes.

User precedence and preemption capabilities of the DDN routing algorithm allow network resources to be allocated to meet changing network conditions at any point in time.

a) Features of the DDN Packet Routing Algorithm

- Shortest Path First (SPF) algorithm developed by BBN
- Each node has a complete view of the network from its perspective at some given time, i.e. , each node knows "how long" it takes a packet to travel from itself to any other node over each of its interswitch trunks (ISTs).

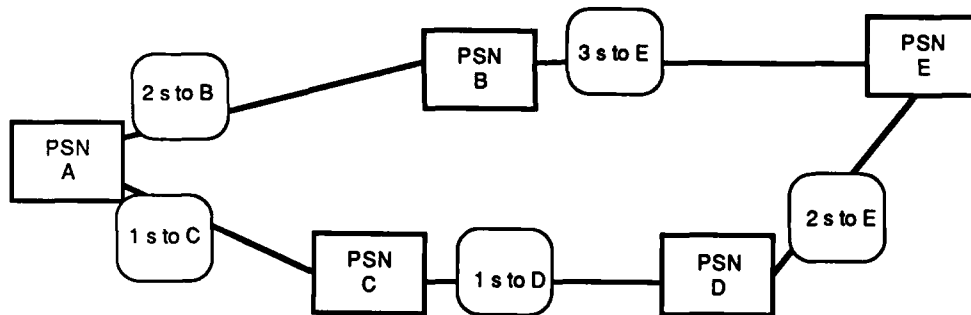


Figure A

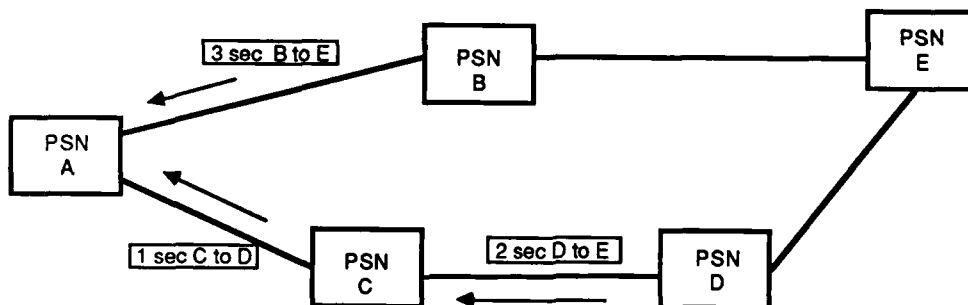


Figure B

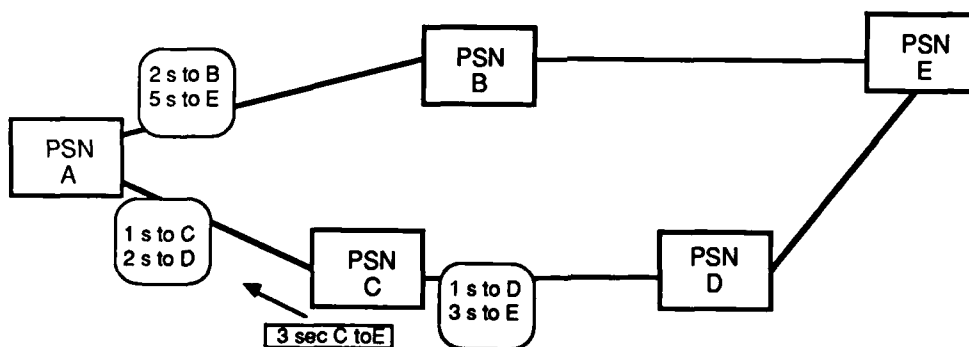


Figure C

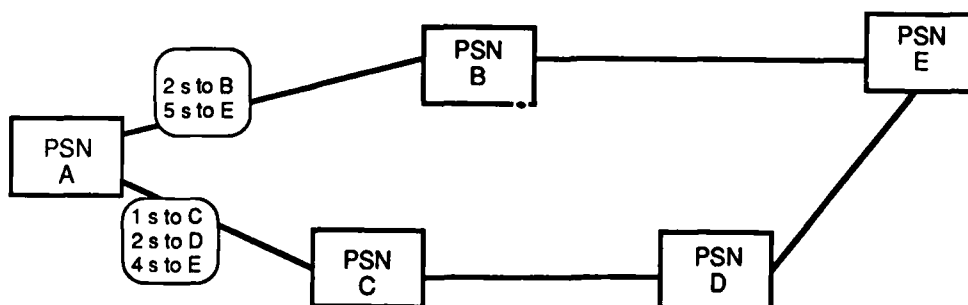
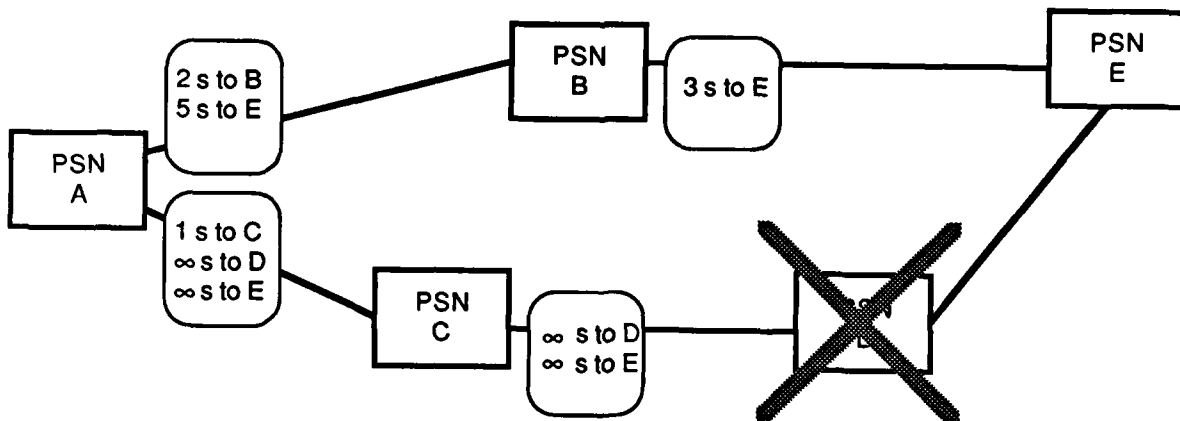
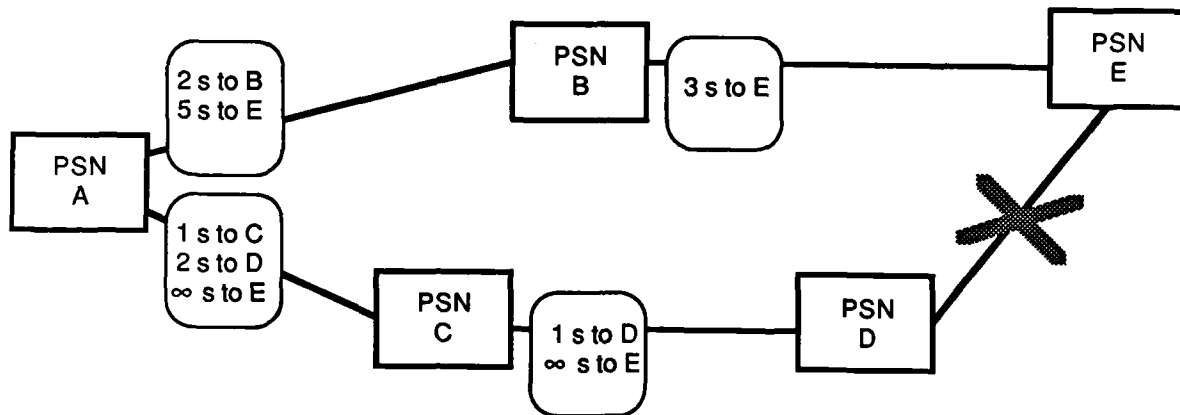


Figure D

b) Operation of the DDN Packet Routing Algorithm

- Periodically, each node calculates the amount of time it takes a packet to get from itself to each of the other nodes directly connected to it (i.e., neighboring nodes). This time is also called the "distance" between the nodes. Figure A
- At regular intervals, each node transmits to each of its neighboring nodes the "distance" from it to all of its neighbors. Figure B
- From this information a node can calculate the amount of time required to send a packet from itself to any node directly connected to one of its neighbors. Figure C
- Finally, this information is then passed to all neighbors which can then calculate another level of redirected delays. Figure D
- Finally, each node will have calculated the average amount of time (distance) from itself to any node not connected directly to it (i.e., a distant node). These calculations are incorporated in a "routing table" which is used to route individual packets until the next update cycle.
- When a node receives a packet:
 - It examines the source and destination addresses
 - Looks up in its routing table which of its links will provide the least delay to the destination
 - Determines the packet's precedence and priority level
 - Places the packet in that link's output queue at a position which is consistent with the precedence and priority level

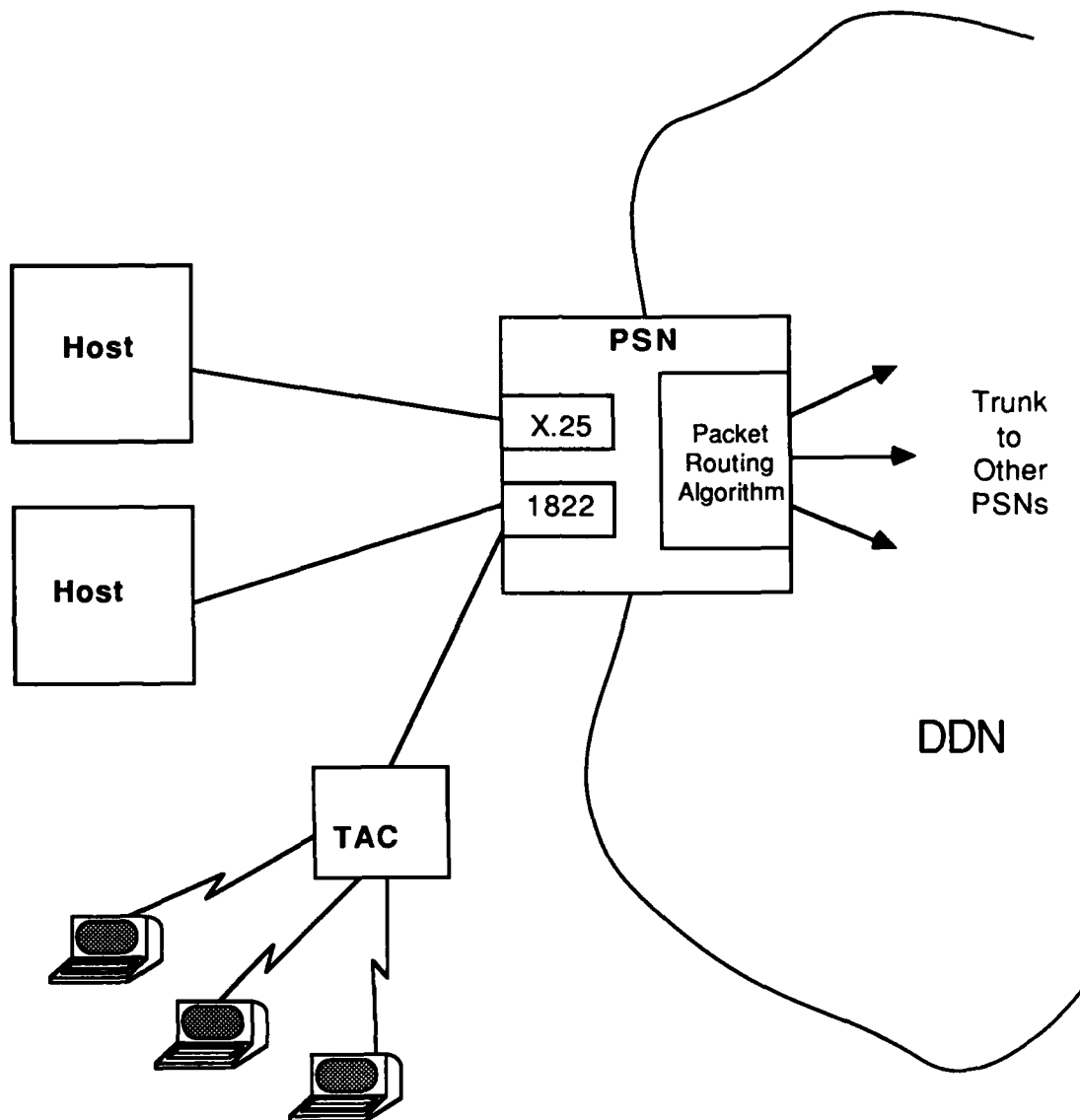
LINK AND NODE FAILURES



c) Implications of the DDN Packet Routing Algorithm

- Because nodes update their routing tables at different times each node may have different knowledge of the network.
- No centralized control is necessary
- Routing information introduces overhead traffic to the network.
- Routing information transfer is minimized where possible, and the update cycle is adjusted so that adequate adaptive routing is achieved without creating excessive overhead.
- *Each packet must contain source and destination information so that each node can make an independant decision as to which link to send it over next.*
- Any link failure between two nodes will cause the delay (distance) measurement across that link to go to infinity, thus causing packets to be routed over any other link which shows a lower delay.
- Any node failure will cause all of its neighboring nodes to conclude that the delay to that node is infinite, thus causing them to route packets over alternate paths, bypassing the failed node.
- Update messages propagate at highest priority level.

NETWORK INTERFACE



C. DDN Packet Switching Devices

1) Overview

a) Background

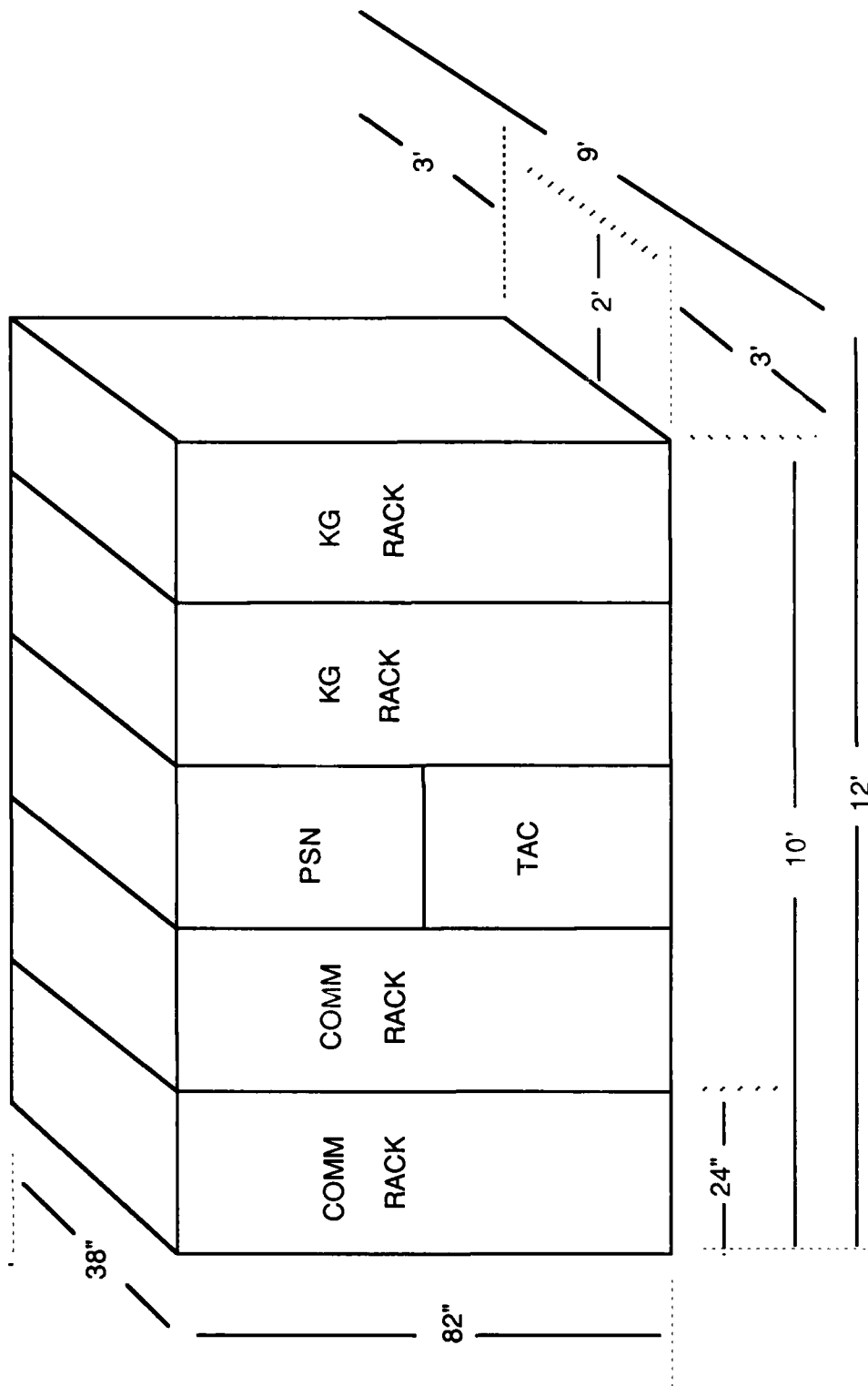
- The packet switching device employed in the DDN is a Bolt, Beranek, and Newman (BBN) C/30. The BBN C/30 is a programmable communications processor which can be used as a Packet Switch Node (PSN) or as a Terminal Access Controller (TAC) depending upon the software and hardware configuration.
- In ARPANET parlance the packet switch is commonly called an Interface Message Processor (IMP).
- The PSN is one component of the "standard" DDN node which is considered a Network Asset and is, therefore, provided by DCA.
- The PSNs are often located at subscriber locations and thus are designed to be virtually maintenance-free.
- The C/30's modular architecture allows nodes to be custom configured to meet subscriber-defined hardware and software requirements.

b) Functions

The PSN performs two functions in the DDN.

- The PSN routes packets through the network, from a subscriber's host or terminal, through the network of PSNs and trunk circuits, to the destination host. The PSN implements the packet routing algorithm described in the previous section.
- PSNs provide the interface for hosts and terminal access devices from the access network to the backbone network. The C/30 PSN implements two host access protocols — X.25 and 1822 Arpanet Host Interface Protocol (AHIP).

STANDARD MILNET SUITE OF NODE EQUIPMENT



2) Hardware Configuration Description

a) Standard Configurations

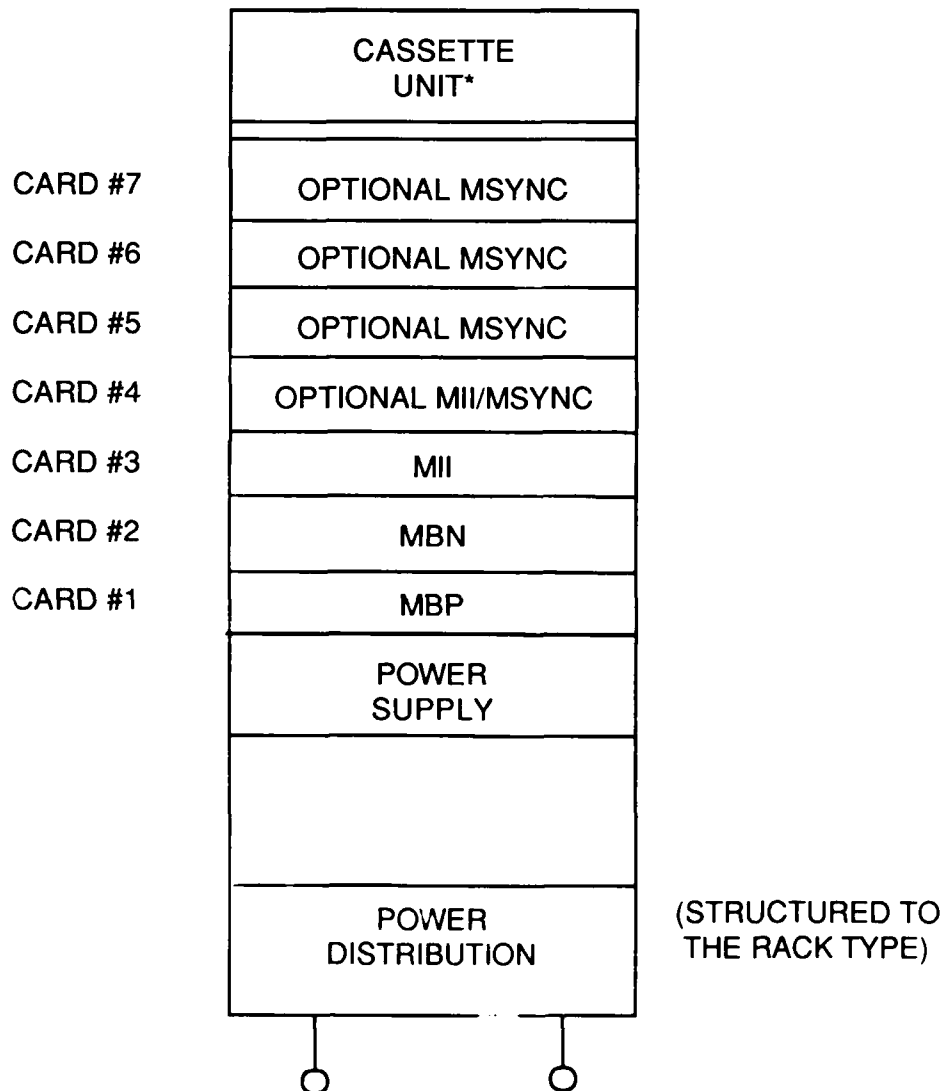
- PSNs and TACs in the same equipment cabinet
- PSNs and TACs enclosed in separate equipment cabinets
- Dual PSNs in one equipment cabinet
- The numbers of IST and host connections allowed
- TEMPEST vs non-TEMPEST shielded

b) Physical Characteristics

The PSN is one component of the standard DDN node which consists of five hardware cabinets 82"h x 24"w x 38"d:

- 1 C/30 equipment cabinet
- 2 communications cabinets (containing the modems and DSU/CSUs)
- 2 KG-84A cabinets

STANDARD CONFIGURATION C/30 PSN LAYOUT



c) Electronic Components

1. Power supply board

2. Processor Boards

- MBP processor motherboard
 - UD8 daughter board which stores processor microcode
 - MHI daughter board which decodes macro instructions

3. Memory Boards

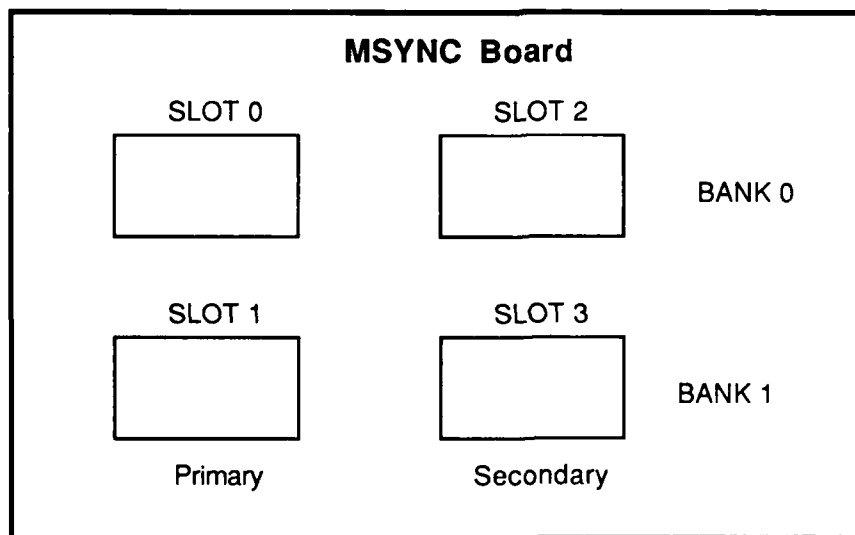
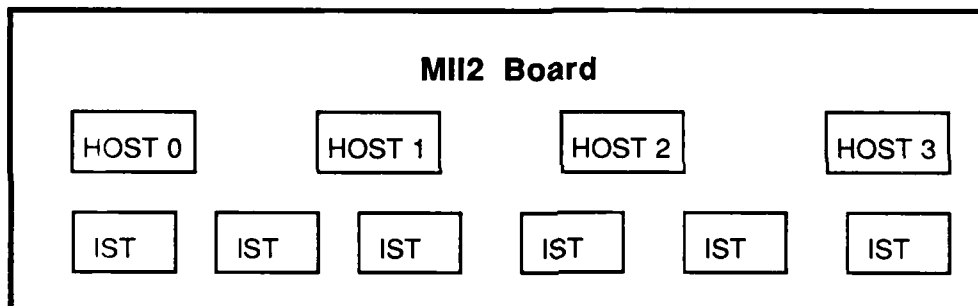
- MBN 128Kw main memory
 - MHA daughter board which decodes memory addresses
 - MEY64 daughter board with an additional 128 Kw

4. I/O Boards

- Maximum of five, actual number depends upon network and subscriber requirements
- Support input data streams with clock rates from 1.2 Kbps up to 64 Kbps
- Supports three physical interface standards:
 - EIA RS-232C
 - EIA RS-449, MIL STD 188-114 balanced
 - CCITT V.35

C/30 PSN INPUT/OUTPUT

PHYSICAL INTERFACE	Line Speed In Kbps		
	1.2 to 9.6	14.4 and 19.2	48 and Higher
RS-232C and equivalent	Avail.	Avail.	Not Avail.
RS-449/442 B MIL 188-114	Avail.	Avail.	Avail.
RS-449/423 unbal. MIL 188-114	Avail.	Not Avail.	Not Avail.
CCITT V.35	Not Avail.	Not Avail.	Avail.



- Each I/O board requires line adapters for each host or trunk connection.
- MII Board
 - requires a single line adapter per port connection
 - supports 4 1822DH connections
 - supports 6 trunk connections
- MSYNC Board
 - requires a daughter board that allows up to eight port adapters
 - supports 16 1822HDH/X.25 HDLC host/trunk connections
 - port configurations:
 - 8 RS-232C connections
 - 4 RS-232C and 4 V.35 connections
 - 8 MIL-STD 188-114 connections

TOTAL CONNECTIONS TO A C/30 MACHINE

Non-Tempest C/30 PSN

	<u>Maximum</u>	<u>Typical</u>
Host Connections:	30	8
Interswitch Trunk Connections:	14	6
Total Connections:	44	14

TEMPEST C/30 PSN

Host Connection:	2 x 1822 DH connections & 4 connections to modems
Interswitch Trunk Connections:	4 maximum
Total Connections:	10 (limitation of TEMPEST fantail)

d) TEMPEST Shielding

- Metallic shield against emanating electro-magnetic radio waves
- Enclose circuit terminations and switching devices
- Used for transmission of classified secret or higher
- PSN supports 10 connections
- Future configurations will allow up to 26 connections (April 1986)

2) Software Configuration Description

- The C/30 PSN software resides on the C/30 processor board.
- BBN provides new software releases to DCA. These software upgrades are introduced into the network after evaluation, testing, and acceptance by DCA.
- The Operations Management Division is responsible for deploying the software upgrades.
- The software can be downline loaded to the newer C/30 nodes; otherwise, it is loaded via cassette tape locally.
- Software releases:
 - PSN 5.0 — supports Basic X.25, Basic X.25 and 1822 HDH on same PSN, fielded in Milnet
 - PSN 6.0 — supports Standard and Basic X.25, fielded on a limited basis in Milnet
 - PSN 7.0 — supports precedence, will not support 1822 VDH, to be fielded 1st quarter 1987

C/30 PSN Throughput Specifications

CONNECTION	THROUGHPUT [*]
PSN - PSN	~ 175 packets / sec
HOST - PSN	~ 100 packets / sec
HOST - PSN - HOST	~ 160 packets / sec

* Assumes: Software release 5
750 bits per packet
Maximum of 5 ISTs per PSN
Maximum of 8 hosts per PSN
ACK packets are not counted

3) Performance of the C/30 PSN

The two areas of performance that will be discussed are:

- Delay
- Throughput

a) Switch Through-Delay

The average switch through-delay is dominated by two factors: packet processing time and the queueing of output packets at the communications circuits.

- **Packet Processing Delay** is a function of the PSN's hardware architecture, processor clock rate, and routing algorithm. PSN-to-PSN traffic is processed by the CPU with a higher priority than host-to-PSN traffic. Therefore, host traffic cannot adversely affect PSN-to-PSN traffic, but PSN-to-PSN traffic can cause host traffic delays.
- **Queueing Delay** occurs when the PSN needs to transmit many packets over a single communications facility, and must, therefore, force some of the packets to "wait their turn." Queueing delays will increase the greater the traffic being processed by the PSN. This is because there is a greater probability that two or more packets will be routed to a common output port at the same time.

b) Throughput

- Throughput is a function of the PSN software.
- The tandem traffic throughput (PSN to PSN traffic) is approximately 175 packets per second with packet sizes of 750 bits per packet.
- Host throughput has been measured at slightly over 100 packets per second with packet sizes of 750 bits per packet. For maximum throughput, a PSN should have no more than 4-5 ISTs and 7-8 full service hosts connected to it.

Network Access Device	Functionality	Supplied By
Terminal Access Controller (TAC)	Provides network access to asynchronous terminals	DDN
Mini Terminal Access Controller (Mini-TAC)	Provides network access to asynchronous terminals and synchronous IBM terminals	DDN
Terminal Emulation Processor (TEP)	Provides network access to multiple asynchronous host ports	Subscriber
Host Front-End Processor	Provides network access to multiple host ports employing the Host to Front-End Protocol	Subscriber

D. Network Access Devices for the DDN

1) Introduction

Network access devices provide access to the backbone packet switching network for user equipment, including hosts and terminals, that are not directly connected to the C/30 PSN.

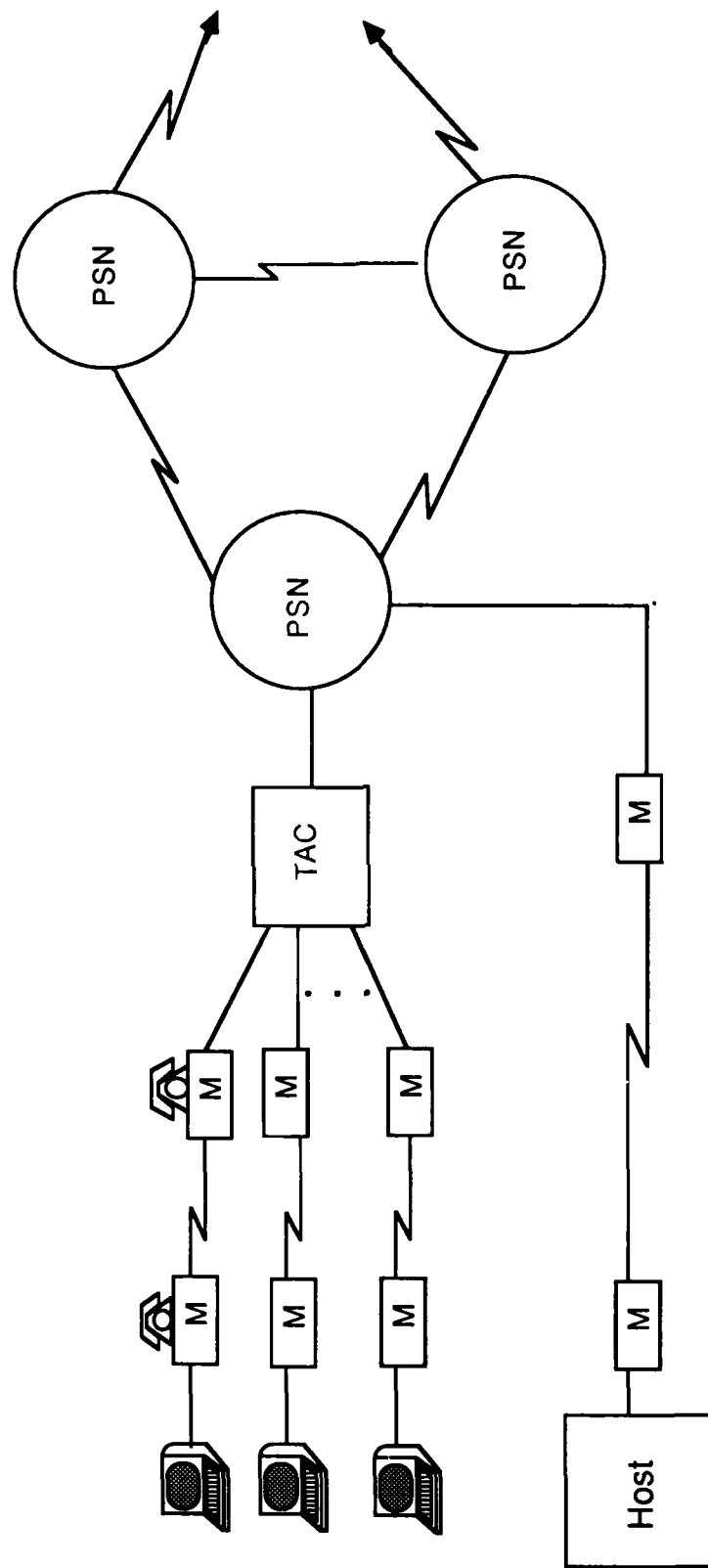
a) Standard DDN network access devices

- Terminal Access Controller (TAC)
- Network Access Components (NAC)
 - Mini - Terminal Access Controller (Mini-TAC)
 - Terminal Emulation Processor (TEP)
 - Host Front-End Processor (HFEP)

b) Other network assets used for providing access

- Leased circuits
 - Analog leased circuits
 - Digital leased circuits
- Modems and DSU/CSUs

Terminal Access Controller (TAC)



2) Terminal Access Controller (TAC)

a) Introduction

- The Terminal Access Controller (TAC) is based on the BBN C/30 communications processor.
- The TAC and PSN differ in the physical configuration of the I/O boards, their software, and the functions of the devices.
- DCSDS is responsible for the TAC hardware configuration and subscriber port allocation.
- TACs can be configured as TEMPEST or non-TEMPEST devices.

b) Supplied by DCSDS

The TAC is considered a Network Asset and is thus supplied and maintained by DCSDS.

c) Functions

- Provides a method for asynchronous terminals to access the backbone network
- The TAC supports one high speed port to connect all users to a PSN and the DDN backbone.
- The TAC provides a network security function through the Terminal Access Controller Access Control System (TACACS). TACACS requires the user to identify himself via a user name and password .
- The TAC supports the TELNET User protocol functions which convert various formats of asynchronous terminal data to Network Virtual Terminal (NVT) format.
- The TAC also acts as a traffic concentrator allowing 62 asynchronous terminal users to access the network, while only using one PSN port.

d) Configuration and Performance

- Up to 62 asynchronous connections to the DDN backbone network
- Dedicated terminal lines — maximum of 46 per TAC
- Dial-up Lines — minimum of 16 per TAC
- Terminal access port speeds — 75 to 9600 bps
- The most common physical configuration dictates the PSN and TAC be collocated in one communications cabinet.
- Remote TACs are deployed in the DDN as determined by the network modeling.

3) Network Access Components (NAC)

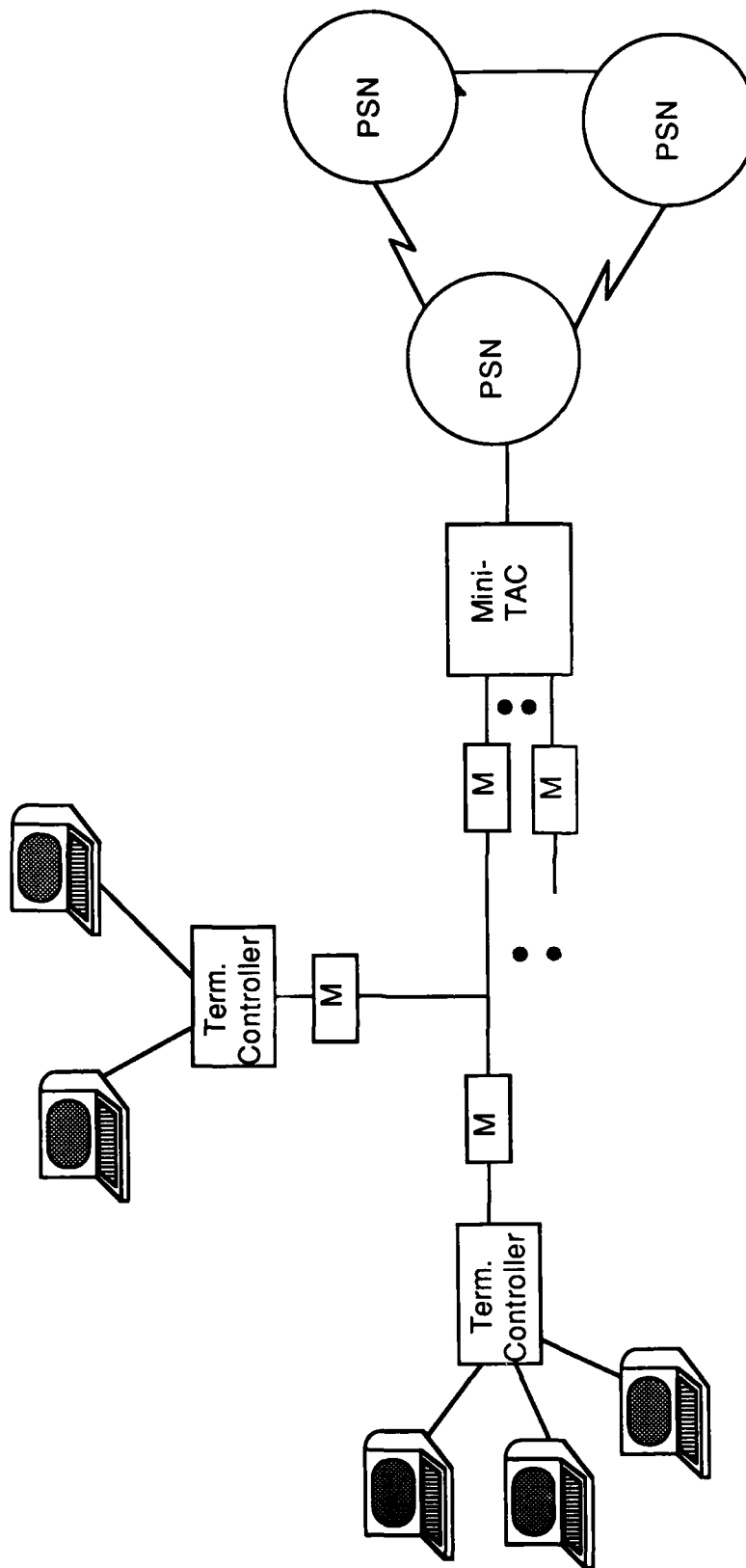
a) Introduction

- The DDN is funding the development of a specialized set of DDN access devices called the Network Access Components (NAC).
- Developed under contract to Aydin Monitor Systems.
- The NAC can be configured to perform the functions of three distinct network access devices:
 - Mini - Terminal Access Controller (Mini-TAC)
 - Terminal Emulation Processor (TEP)
 - Host Front-End Processor (HFEP)

b) Configuration

- All NACs will have identical hardware modules which will be housed in a cabinet approximately 17"w x 13"h x 20"d.
- The cabinet will be rackmountable in a DDN equipment cabinet.
- The differences will be in the software to support each functional requirement.
- The NACs will support fully qualified full service DDN interfaces.
- The CPU/system controller will consist of the following:
 - C language micro operating system, called AMOS
 - 4 68010 10MHz multiprocessor devices
 - 1 DDN interface board
 - 1 ST1, will support 8 ports
 - 1 ST2, will support 8 ports
 - 512K bytes of dual port RAM
- DCSDS will field a limited number of each component type and the prototypes of these components are to be available in the first quarter of 1987.

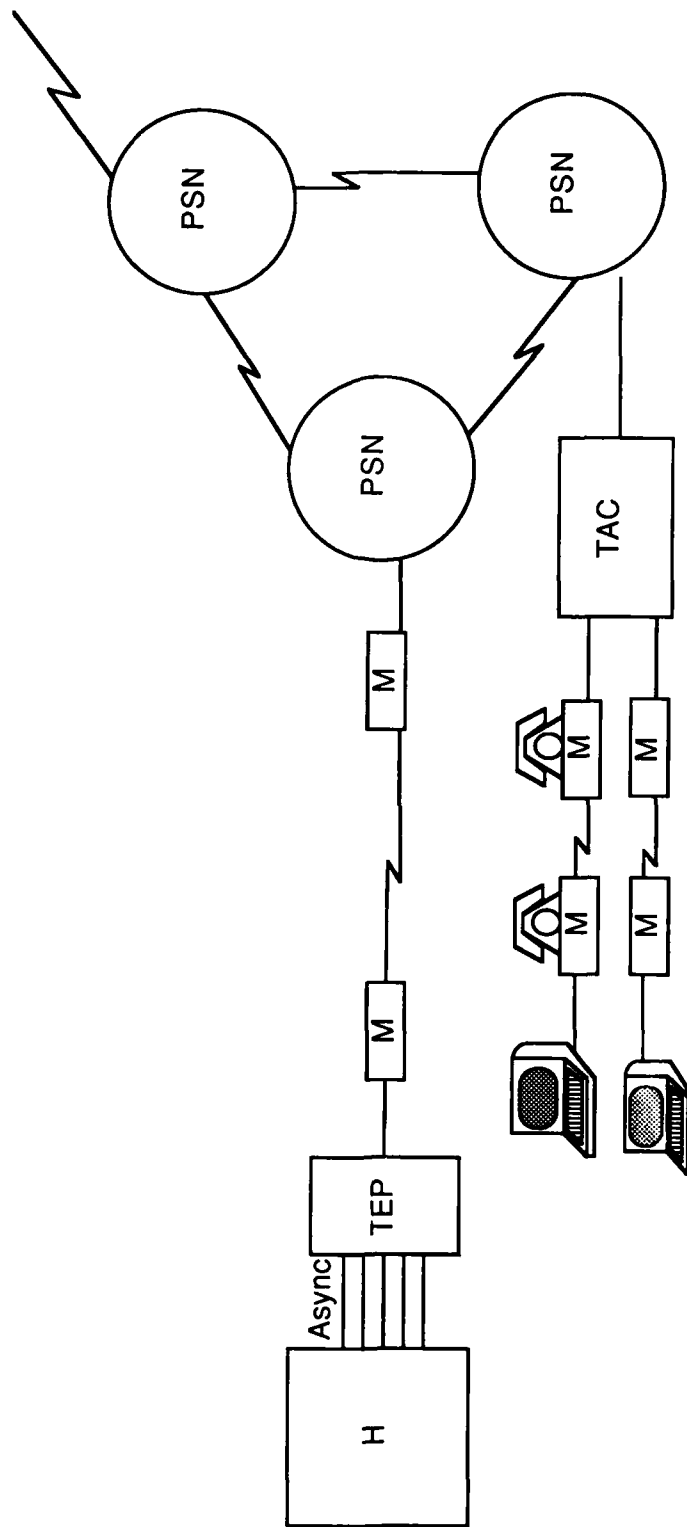
Mini-TAC



c) Mini-TAC

- The Mini-TAC will be a **DCSDS provided network asset**.
- The mini-TAC functions similarly as a TAC; however, it will allow both asynchronous and **IBM 3270 BSC** terminals to connect to the DDN.
- 16 ports, configurable in groups of 4 plus one port for a network connection
- The possible configuration options for an asynchronous port include:
 - half or full duplex
 - 75 to 9600 bps
 - ASCII or BCD characters
- The possible configuration options for a synchronous port include:
 - up to 19.2 Kbps
 - ASCII or EBCDIC characters
- The mini-TAC will support terminal-to-remote host communications, but will not support terminal-to-terminal communications.
- In most cases a terminal controller will connect to the mini-TAC.
- There can be no more than 64 TCP connections per mini-TAC.
- The mini-TAC will only support single security level access.

Terminal Emulation Processor (TEP)

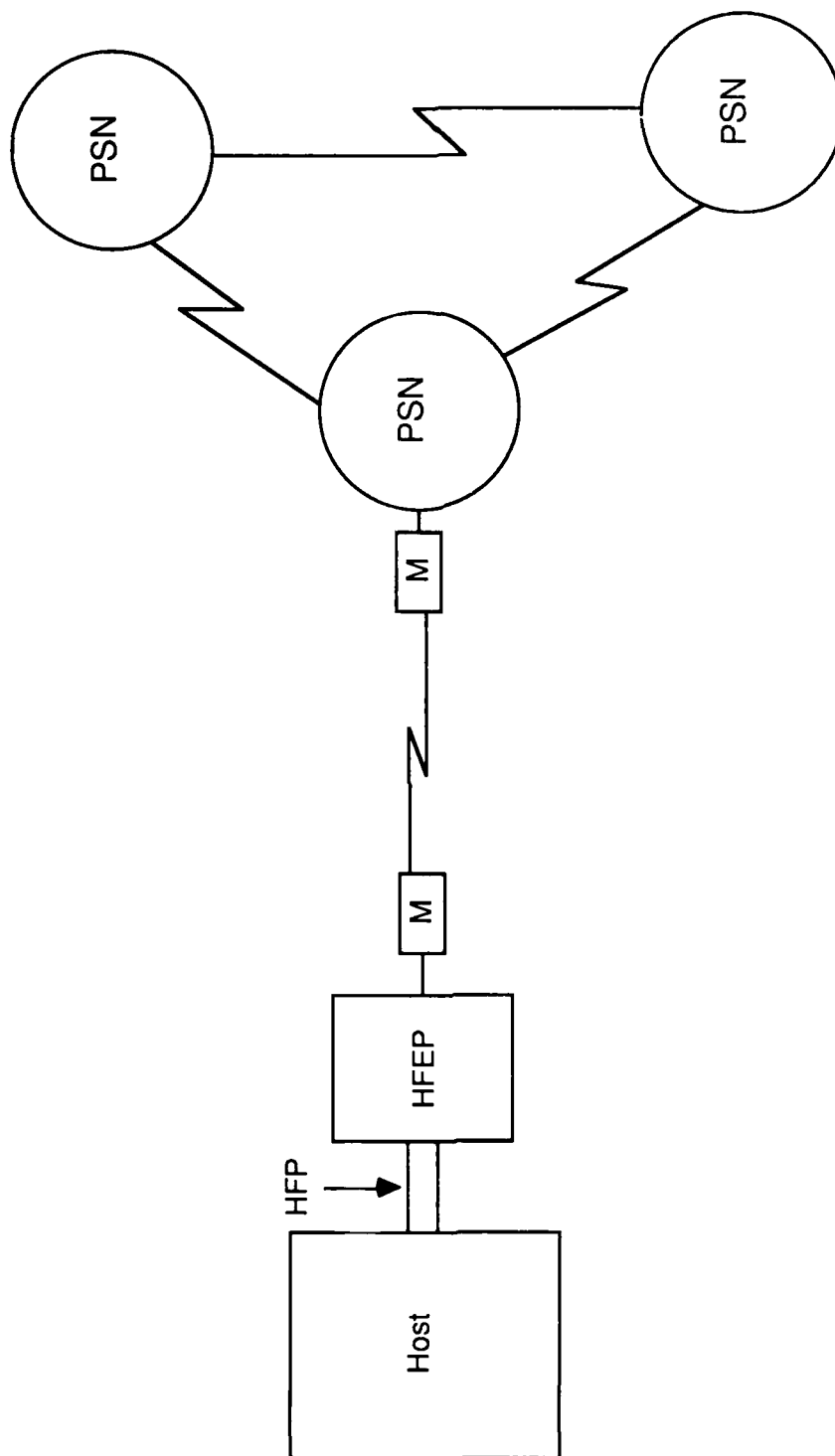


d) Terminal Emulation Processor (TEP)

The TEP provides a wire replacement for direct terminal connections at the host end (the terminal end will be handled by a TAC or mini-TAC). The TEP allows a subscriber's host to communicate with terminals through the DDN, but not with other hosts on the DDN.

- The TEP is the reverse of a TAC or mini-TAC, it emulates terminals connected to a host.
 - When acting as the mirror image of a TAC, the TEP will support multiple asynchronous connections to the host.
 - When acting as the mirror image of a Mini-TAC, the TEP will support multiple IBM 3270 BSC compatible connections to the host.
- The network is transparent to the host and only the terminals are able to initiate communications over the DDN.
- The TEP will support up to 16 host terminal ports.
- Does not require software changes to the host.
- DCSDS provides hardware and software support for TEPs. If a subscriber application dictates a TEP, the subscriber must procure the TEP.

Host Front-End Processor (HFEP)



e) Host Front End Processor (HFEP)

- The HFEP will support the DDN protocols to include X.25 and TCP / IP.
- The HFEP will also implement the Host to Front-End protocol, which must also be implemented in the host.
- The subscriber is required to implement the host part of the Host to Front-End protocol in the host computer.
- The HFEP will be able to operate at transmission speeds from 4.8 Kbps to 56 Kbps.
- The HFEP will support up to 2 host connections and one network connection to the DDN.

f) Circuits — Analog and Digital

- DCSDS provides the leased circuits for both InterSwitch Trunks (ISTs) and subscriber access circuits.
- **DCSDS** initiates all IST and access circuit Telecommunication Service Requests (TSR).
- Digital circuits such as DDS are used when the communications requirement is 56 Kbps. If not available, 50 Kbps analog circuits are used.
- All circuit requests are submitted to DECCO with the provision that the vendor provide "end-to-end responsibility" (CONUS). The vendor is responsible for providing the circuit and the modems or DSU/CSUs.

g) Modems and DSU / CSUs

- DCSDS has implemented a standard modem contract in an effort to standardize the modems being used on the network.
- DDN provided modems and DSU/CSUs will be deployed at the direction of DCSDS.

E. Network Monitoring

1) Functions of the Network Monitoring Center

The Monitoring Centers (MC) perform monitoring, control, and managerial functions for the Defense Data Network.

a) Network Monitoring

The MC is responsible for detecting failures and configuration anomalies in the PSNs, the backbone links, TACs, and when available, mini-TACs. Each MC is capable of continuously checking each of the above mentioned components in its portion of the network and signalling operations staff in the event of a failure. The DDN is designed to be able to continue operation without manual intervention in the event of failures. Operations staff is required to dispatch repair personnel to equipment sites, coordinate Telco or vendor repair activities, and track outages.

b) Network Control

The DDN has been designed to operate unattended. Thus there are very minimal control functions associated with an MC. An MC is able to reboot a remote PSN and is able to downline load configurations to all the DDN PSNs.

c) Network Administration

The MCs are responsible for coordinating all changes to any of the DDN PSNs, access devices, or circuits.

2) Location of Network Monitoring Centers

Currently there are three Regional Monitoring Centers for the MILNET and one for the ARPANET.

a) MILNET Monitoring Center

- Located at DCA Headquarters in Arlington, Virginia
- Primary responsibility for the CONUS portion of MILNET
- Acts as the command center for all MCs

b) European Monitoring Center

- Located in Vaihingen, Germany
- Responsible for the European components of the DDN

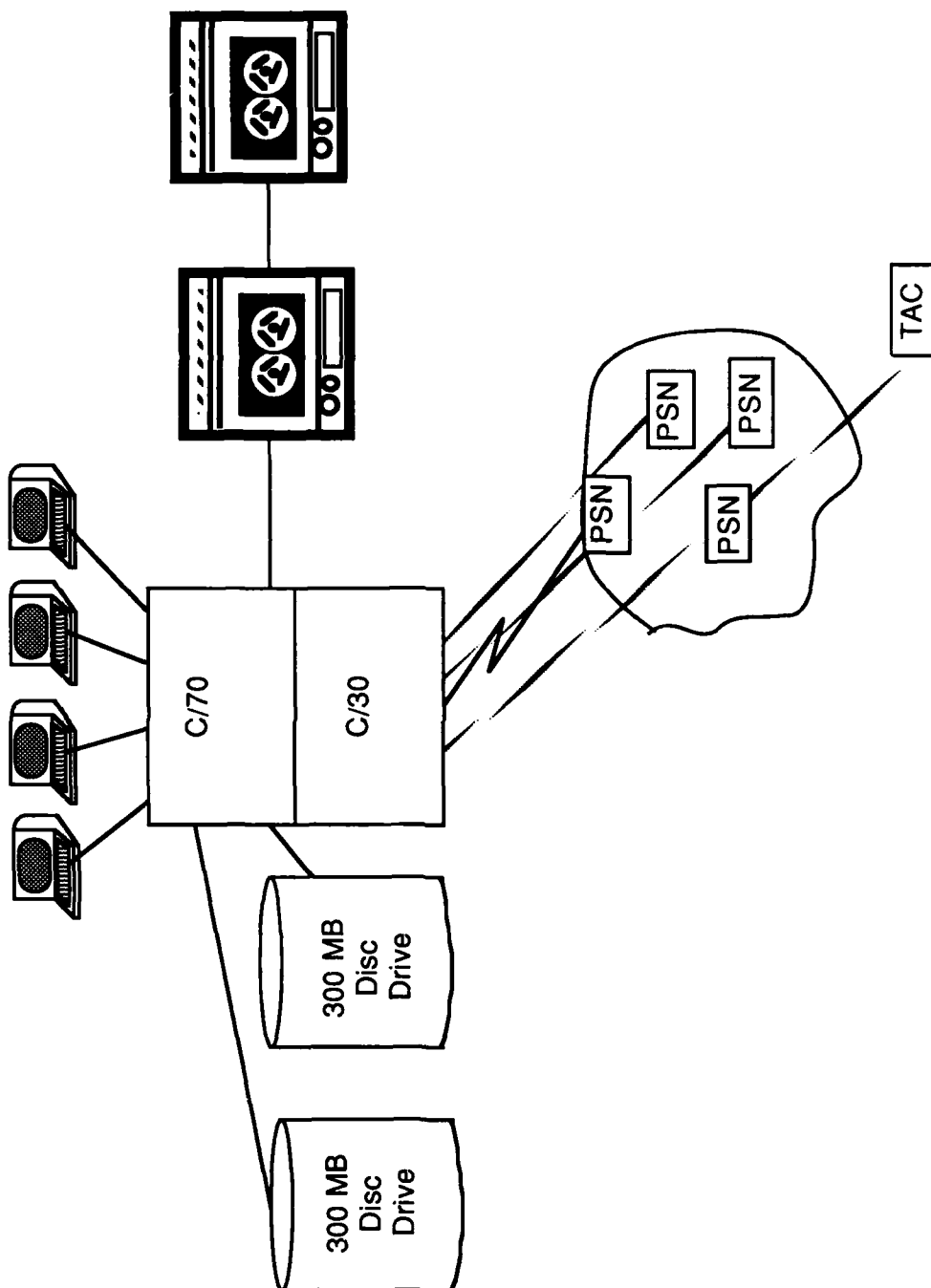
c) Pacific Monitoring Center

- Located at Wheeler AFB, Hawaii
- Responsible for the Pacific region

d) Cambridge MILNET Monitoring Center

- Located in Cambridge, MA
- Responsible for the ARPANET and new installations on the MILNET

MONITORING CENTER



3) Monitoring Center Components

Each MC is composed of hardware and software needed to perform the necessary monitoring and control functions for the DDN.

a) BBN C/70 Minicomputer

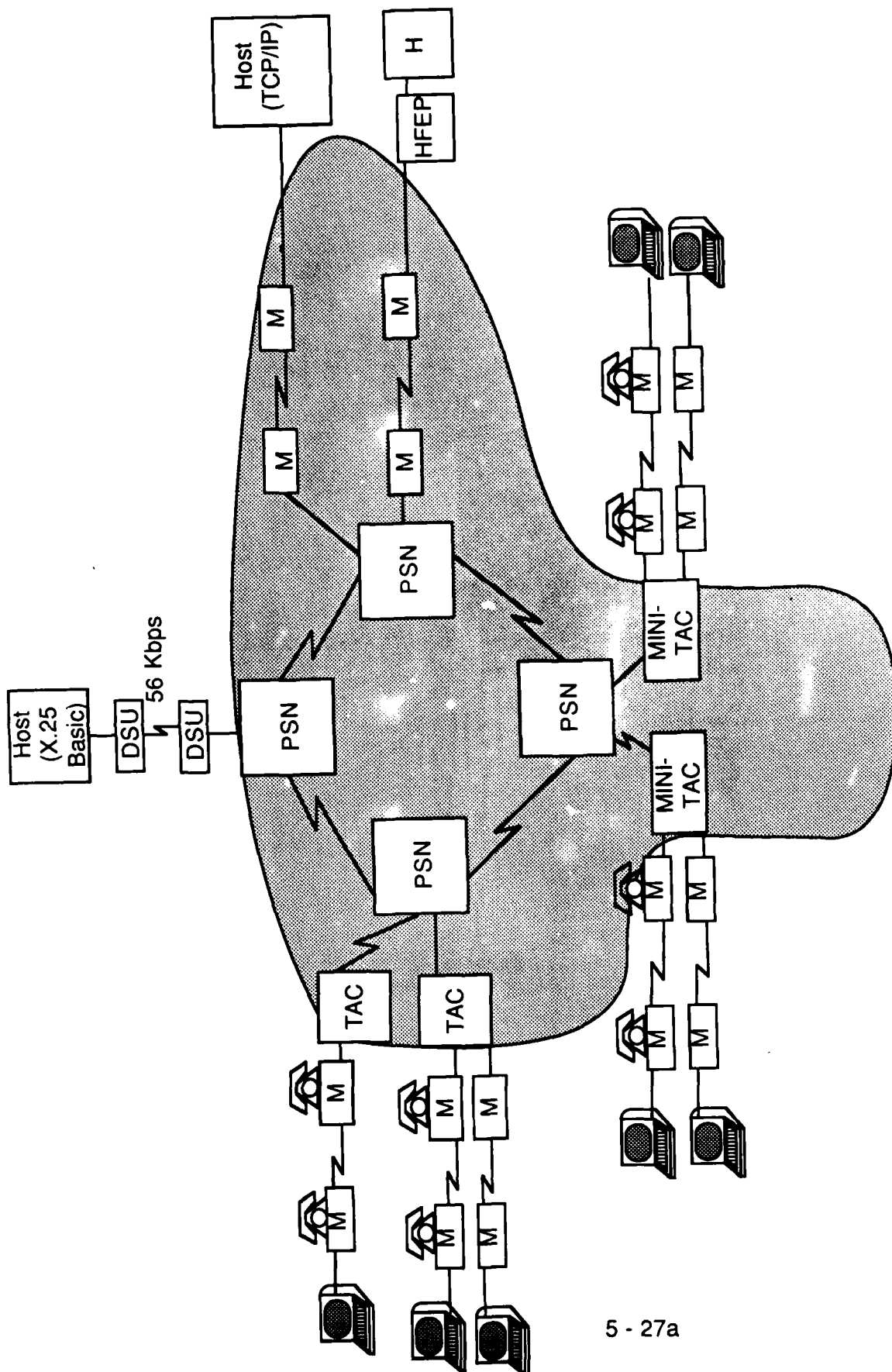
All monitoring and control functions are resident on this BBN minicomputer. The following is a list of peripheral components of the C/70 minicomputer:

- Disk System — The 300 MB drives are used to store system faults and error messages
- Tape System — The tape system is used to archive system faults associated with the network
- BBN Operating System — This is a UNIX-based operating system with BBN enhancements
- Various terminals and printers used for displaying and printing information

b) Network Utilities (NU)

This is a BBN software product that runs on a C/70 and is designed to automate the monitoring, control and management of the network. This same system is used commercially by other networks based on BBN C/30 packet switches, e.g., MCI. The Network Utilities perform the following functions:

- PSN control commands — loop, dump, reload
- TAC configuration aids — turn port on, turn port off
- Software testing aids — for testing patches



4) DDN Component Monitoring

Monitoring, or passive listening, occurs in one of two ways — an intelligent network component such as a PSN or TAC can be "polled" for status information or it will report its status periodically to its MC.

a) Network Components the MC Monitors

- Trunk circuits between switches
- Packet Switching Nodes (C/30-based PSNs)
- Terminal Access Components (C/30-based TACs)
- Mini-TACs (when they become available)
- Host access circuits for hosts that implement TCP/IP

b) Network Components the MC Cannot Monitor

- Terminal access circuits at the TAC
- Host access circuits connecting X.25 basic hosts

	10	20	30	40	50	60	190	200
12345678901234567890123456789012345678901234567890	12345678901234567890123456789012345678901234567890	12345678901234567890123456789012345678901234567890	12345678901234567890123456789012345678901234567890	12345678901234567890123456789012345678901234567890	12345678901234567890123456789012345678901234567890	12345678901234567890123456789012345678901234567890	...	1234567890

	10	20	30	40	50	60	190	200
12345678901234567890123456789012345678901234567890							• • •	1234567890

[illegible]

Node Isolated: 14

Node Down: 3, 10, 12, 20, 22, 59

TAC Down:

DDN1 MILTAC down

• = presently up, X = down,  = status change

5) Monitoring Center Tools

a) Monitoring Commands

- Statistical Gathering Commands — a function used for gathering throughput data
- Status Commands — issued by network controller for PSN, TAC, and host interface status

b) Network Monitoring Displays

- Lightbox — displays current status of nodes and lines
- Netlogger — displays trap and status messages along with controller actions messages

6) Network Management Functions of the MC

a) Administrative Functions

Hardware and software configurations need to be maintained in a database in order to support network topology monitoring and control. The two software modules that perform these functions are:

- Network Administrator — responsible for new installations and configuration changes made to network topology
- Database Administrator — responsible for maintenance of configuration files of PSNs and TACs

NETLOGGER

* Trap Messages

08:43 BBN83 {83} * (41: 100047 1) modem 1 reload req from Ram {42}
[Node 83 received a reload request from its neighbor, node 42 which has dropped into its loader/dumper program for some reason.]

08:44 NSIS2 {64} * (72: 0 132) killed line to DCAPMO {87}

08:45 NSIS2 {64} * (74: 141 132) lineup to DCAPMO {87}
[Node 64 reports that it brought its line to node 87 down, then up.]

08:49 NLM56 {56} * (80: 20 1) modem 1 up with only 16 channels

[Node 56 is warning that there may be a mismatch in the configuration data its has versus what its neighbor node (off its modem 1) has.]

* Status Messages

08:53 Host WIND {11/0} tardy

08:54 Host WIND {11/0} up

[The interface to the host named WIND, node 11's host interface 0, is reported tardy then up.]

09:00 Line 124 {83/1 42/3} Line errors: DTS83 {83} missed 37 in 40

[Line 124, connecting nodes 83 and 42 off their modems 1 and 3 respectively, is experiencing line transmission errors serious enough to report.]

* Controller Actions

08:52 RAM {42} Dump: ram copied to ram:d0817.0844.1.

08:53 RAM {42} Reload: Initiated reload of ram from n5 through n83

09:02 RAM {42} Clrcrsh: Clear crash at ram

09:03 RAM {42} Configver: CONFIG words are being updated

09:04 RAM {42} Configver: Correcting CONFIG block checksum.

09:05 RAM {42} Restart: Restart imp ram

[This series of controller events shows actions taken in response to a power failure at a site. The controller took a dump of node 42's (RAM) memory, reloaded the node, cleared the crash locations, verified the configuration data, and restarted node 42.]

b) Problem Reporting Procedures

- OCONUS Subscriber – calls either the European or Pacific MC
- CONUS terminal user who cannot access a TAC — calls the NIC via the 800 number displayed on the CRT ((800)235-3155). NIC works with user to resolve the problem and, if necessary, forwards the call to the appropriate MC.
- User who cannot access a host — calls the Host Administrator who verifies whether the host is operating correctly. If the problem is network related, the host administrator reports it to the MC and obtains a trouble ticket number for future reference.

c) Escalation Procedures

- For problems which exist for an abnormal amount of time — the Host Administrator contacts the Milnet Manager at the Packet Switch Operations Branch, either via infomail (MILNETMGR@DDN1) or phone ((703) 285-5230, autovon 356-5230).
- Fire Reports are opened for operational problems requiring technical assistance
- Problem Reports
- Problem Review Board reviews all problems opened and decides whether an Investigative Report needs to be opened
- Investigative Reports — opened by BBN at the discretion of the Problem Review Board. Closed by IR managers at DCSDS and BBN.

d) Fault Repair

- Network Hardware

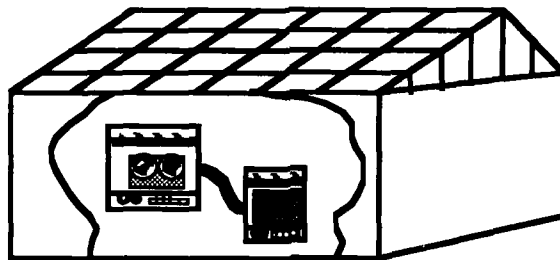
BBN Field Engineers must respond to hardware problems within two hours to the next half-day (12 hrs) depending on node location, proximity to BBN field office and restoration priorities (CONUS and OCONUS). Milnet has a single level of restoration priority.

- Circuits and Modems (56 Kbps DDS and voice grade circuits)

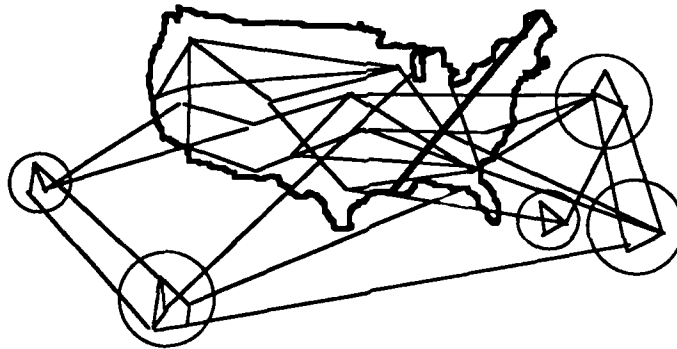
The DDN MC is responsible for the maintenance of all circuits and modems for which DCSDS initiated service. The vendor must respond to circuit and modem problems within 24 hours. Maintenance for all circuits and/or modems obtained through other means are the responsibility of the subscriber.

DDN FEATURES PROVIDING SURVIVABILITY

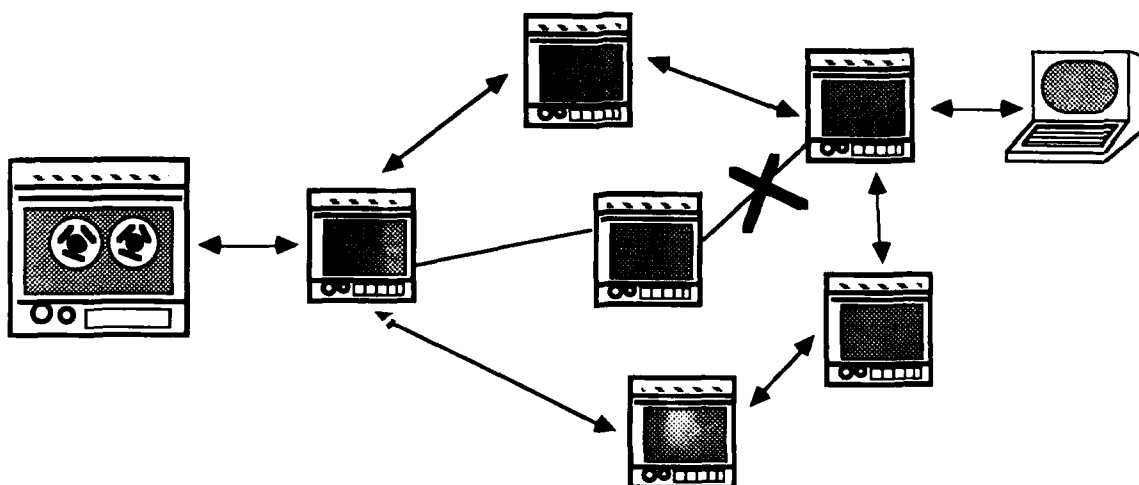
COLOCATED EQUIPMENT



CIRCUIT AND NODE REDUNDANCY



ADAPTIVE ROUTING



6. DDN System Performance

A. Survivability

DDN is a highly distributed network with built in features that will ensure that the network will survive the JCS postulated threats.

1) Redundancy

- 174 fixed switching nodes, with backups at critical locations
- Fixed Regional Monitoring Centers
- 5 mobile Monitoring Centers (planned)
- Dual homing of critical users
- Dense trunking grid to provide many alternate routes

2) Dispersion

Switching nodes are widely dispersed over the system and whenever possible located away from targeted areas. In many cases nodes are colocated with subscriber equipment so that the node will be as survivable as the subscriber systems it supports.

3) Dynamic Adaptive Routing

Dynamic adaptive routing automatically routes traffic around congested, damaged, or destroyed switches and trunk circuits, allowing the system to continue working over the remaining portions of the network.

4) Precedence / Preemption

DDN will provide four levels of precedence and preemption capabilities to ensure that critical, time sensitive, data can get through in the event of surges in traffic during peactime or in the event of degraded network capabilities due to stress conditions.

5) Graceful Degradation

Due to its high degree of redundancy and its ability to automatically monitor the switches, trunks, and access lines; the DDN is able to degrade gracefully when a limited number of transmission paths or switching nodes are down. The network responds automatically to such failures by routing traffic around all inoperative components.

NETWORK AVAILABILITY

Configuration	Availability	Non-availability
Single Homed Host	99.3%	2.5 days/year
Dual Homed Host	99.95%	4.4 hr/year

6) Hardening and HEMP (High-altitude Electro Magnetic Pulse) Protection

All DDN components will have HEMP protection in the form of E&M shielding, line isolation, and surge arresting protection. At selected sites with no backup power, an uninterruptible power supply may be provided to ensure continued operation in the event of power outages.

7) Reconstitution

To facilitate system reconstitution in the event of extreme stress or post-attack, five mobile reconstitution nodes, equipped with MC capability, will be positioned in least targetable areas in the theaters and in the continental US. Some of the mobile units will have multi-media access capability to allow critical users to access the DDN through a variety of transmission facilities.

B. Availability

- The DDN is designed for continuous operation 24 hours per day, 7 days per week.
- The network will support at least 99 % availability to any pair of "single-homed" users that want to communicate with each other.
- Enhanced availability will be available by "dual-access" (two access lines to the same switching node), or by "dual-homing" (two access lines, one to each of two different switching nodes).
- Dual homed users will achieve an availability of 99.95 %.

BER Performance

Probability of Undetected Error	4.2×10^{-18}	1 error in 174,000 yrs.
Probability of Misdelsivered Packet	5.5×10^{-12}	1 error in 181 billion packets

Backbone Network Delay

Category	Traffic Type	Domestic	Overseas
Average	High Precedence	0.09 sec	0.39 sec
	Low Precedence	0.122 sec	0.422 sec
99th Precentile	High Precedence	0.224 sec	0.524 sec
	Low Precedence	0.458 sec	0.758 sec

C. Transmission Quality and Bit Error Rate

- An error can occur in the DDN network in either the access lines, the trunk circuits, a switching node, or an access device.
- A 16 bit CRC is used on the access circuits and on all trunk circuits.
- 16 bit checksums are used on an end-to-end basis with all subscribers implementing TCP in their hosts.
- The overall undetected Bit Error Rate (BER) depends upon the access configuration. A host which implements the TCP protocol will experience an undetected BER of less than 2.9×10^{-19} .

D. Network Delay

Delay has been computed for the backbone network using an analytic model which takes into account:

- Network topology
- Routing tables
- Traffic volumes
- Overhead

Two priority levels were analyzed.

SECURITY ASPECTS

- **Data Confidentiality**
 - **Mandatory**
 - **Discretionary**
 - **Traffic Flow**
- **Data Integrity**
- **Identification, Authentication and Access Control**
- **Data Origin Authentication**
- **Non-Repudiation**
- **Availability of System**

7. SECURITY

A. Security Services

DDN must provide security services for its users to comply with DoD security policy. Responsibility for security is split between the subscriber and the DDN.

1) Data Confidentiality

- a) **Mandatory** — data at a formally assigned security level cannot be disclosed to anyone not cleared for that security level
- b) **Discretionary** — protects against unauthorized disclosure of information to persons who do not require the information for their official duties, but who may be cleared for that security level ("need to know" basis)
- c) **Traffic flow** — protects against observation of information flows within the system

2) Data Integrity

Protect against tampering, or as a minimum, detects tampering of data

3) Identification, Authentication, and Access Control

Prevent unauthorized access

4) Data Origin Authentication

Joint validation of network user and of data

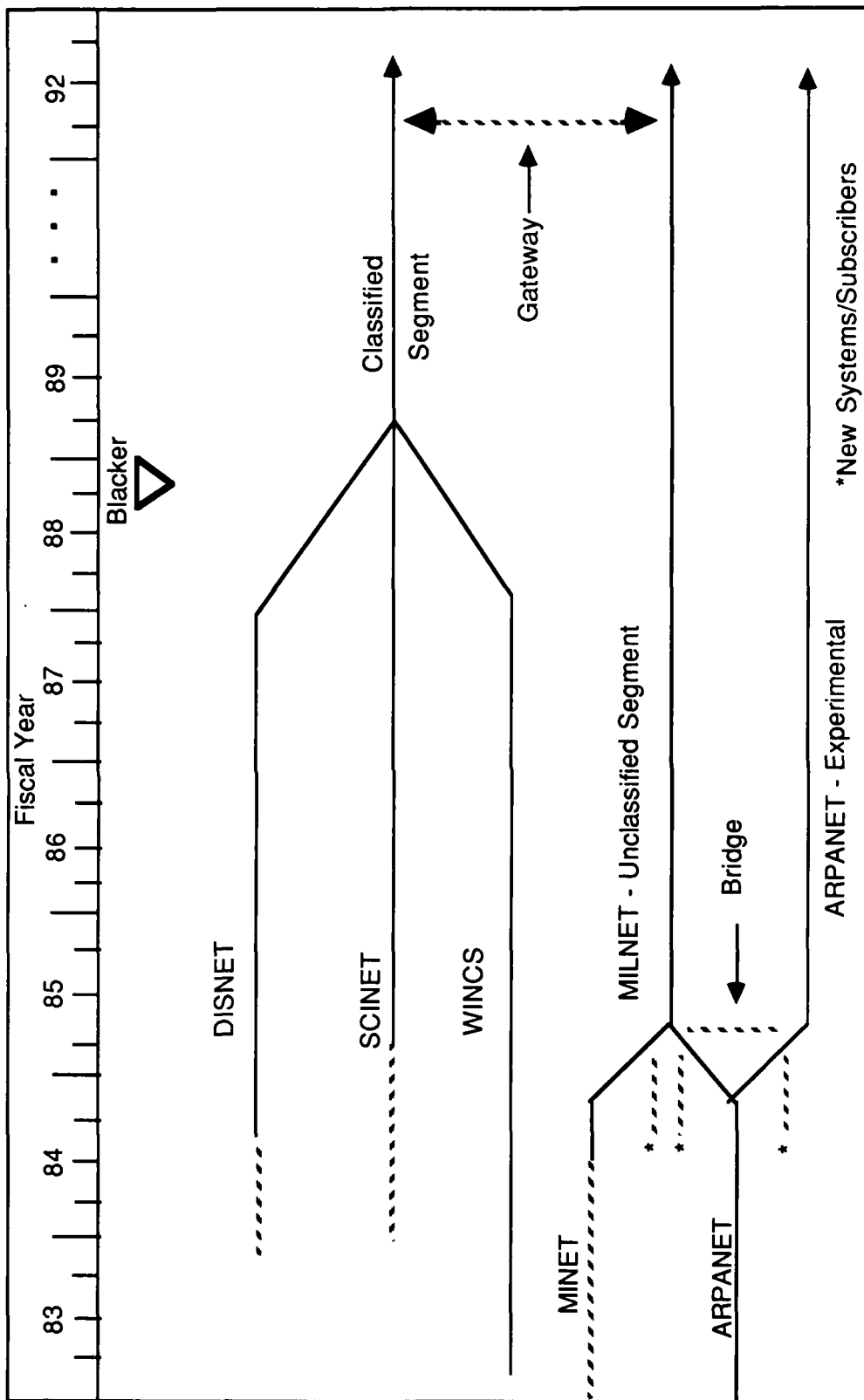
5) Non-repudiation

Unforgeable proof of shipment and receipt of data

6) Availability of System

Prevent denial of service

SCHEDULE



B. DDN Security Mechanisms

1) Physically Separate, System High Networks

a) DISNET — Defense Integrated Secure NETwork (DSNET1)

- Secret network
- 41 planned PSNs

b) WINCS — World Wide Military Command and Control System (WWMCCS) Information Network Communication Subsystem (DSNET2)

- Top secret network
- Operational with 17 PSNs (23 total)
- 41 planned PSNs

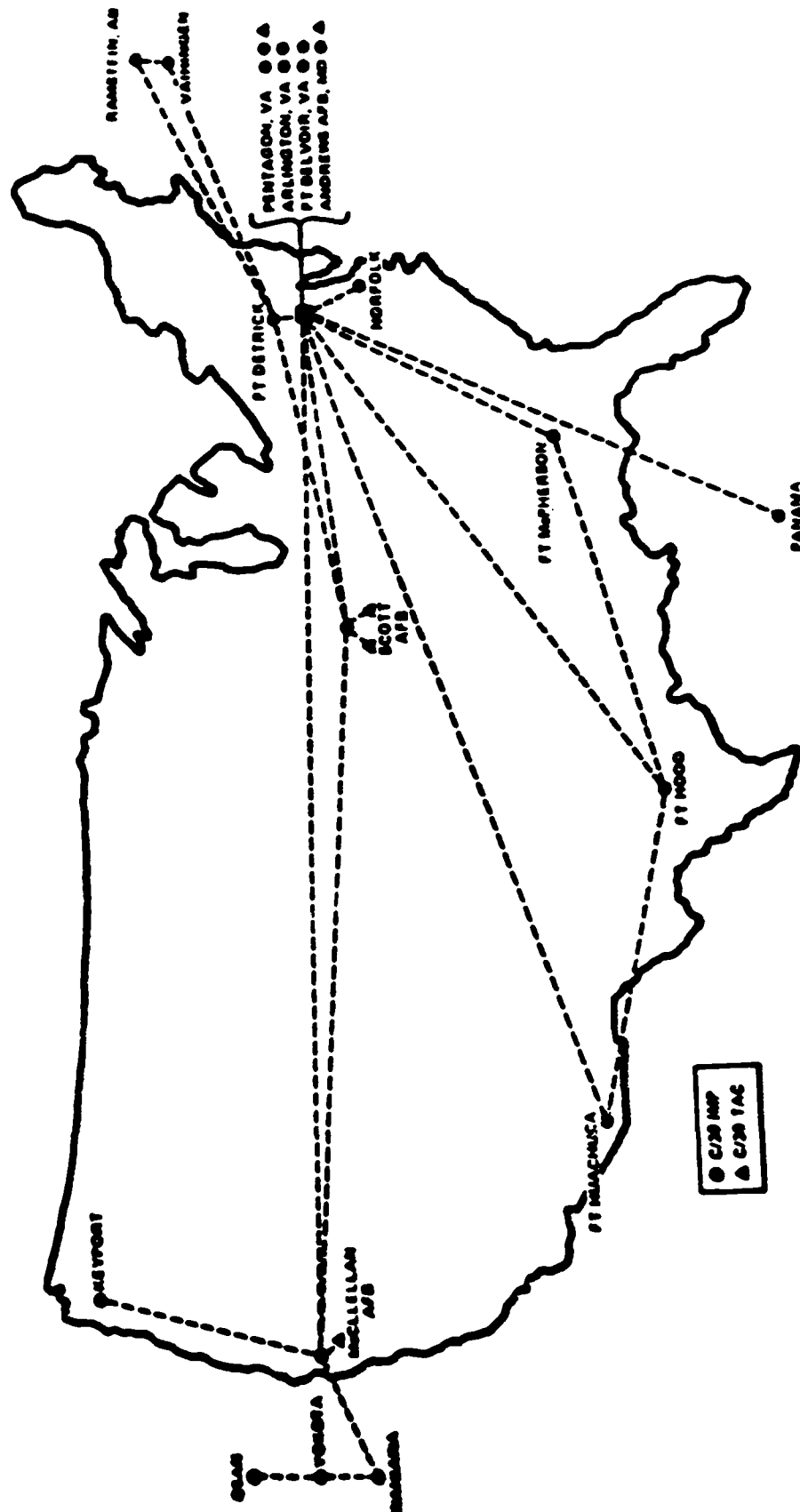
c) SCINET — Sensitive Compartmented Information NETwork (DSNET3)

- TS/SCI network
- Serve DIA requirements
- 42 planned PSNs by 1988

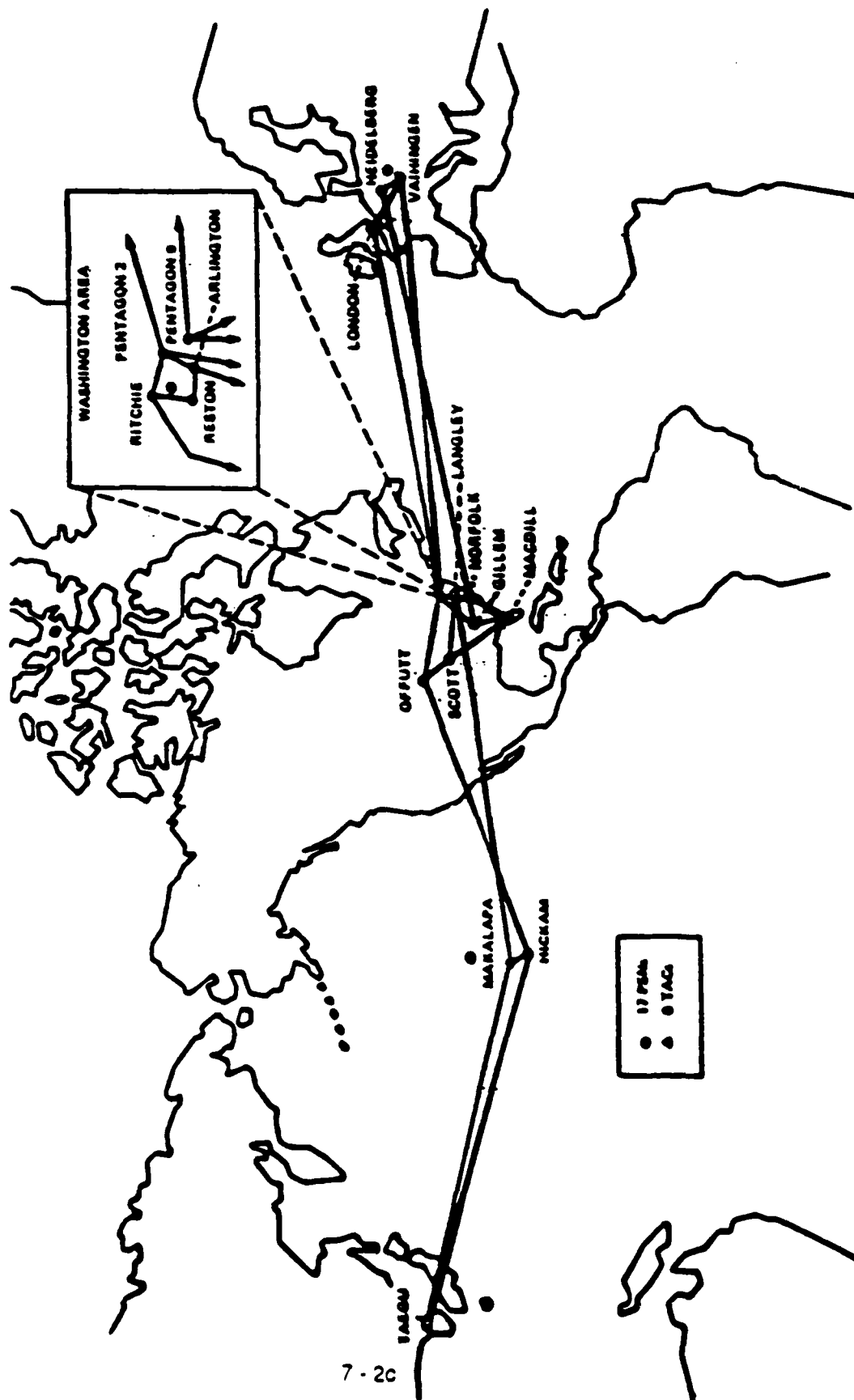
2) Guard Gateways - 1992

- Multinet Gateway equipment being developed by Ford Aerospace for the USAF. Designed to be TCSEC class A1
- Allow low to high data transfer
- Mark packets from less secure environments
- Allow communication through internet guard gateways only, not through backside connections
- On DISNET, guard gateways will be identified as unclassified, single level hosts

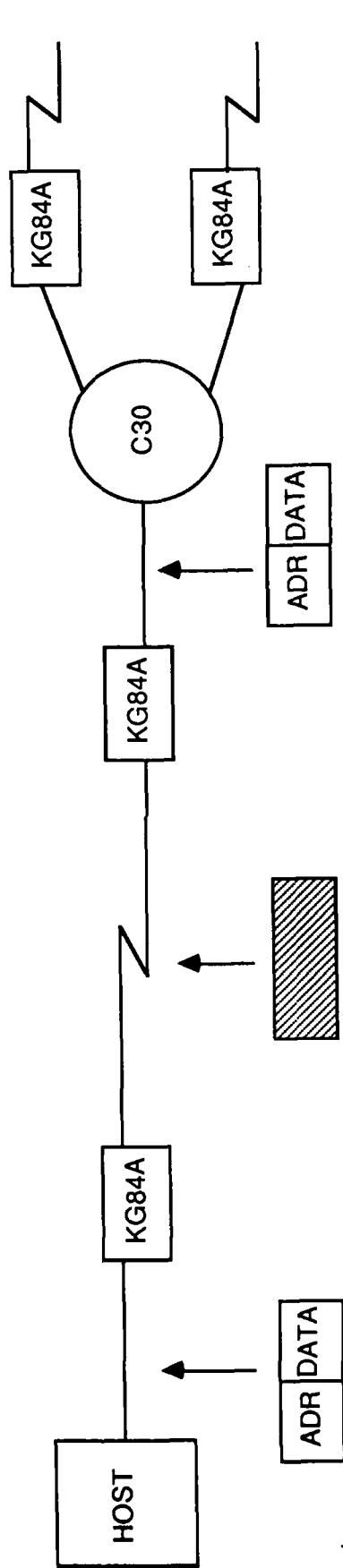
DISNET (85 -- 86/87)



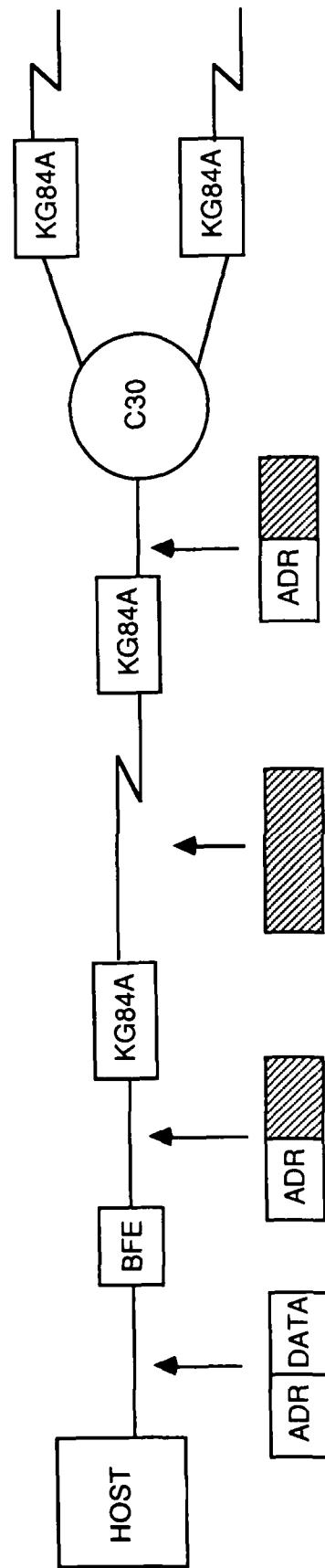
WIN COMMUNICATION SUBSYSTEM



LINK VERSUS HOST-TO-HOST ENCRYPTION



7 -3a



3) Link Encryption

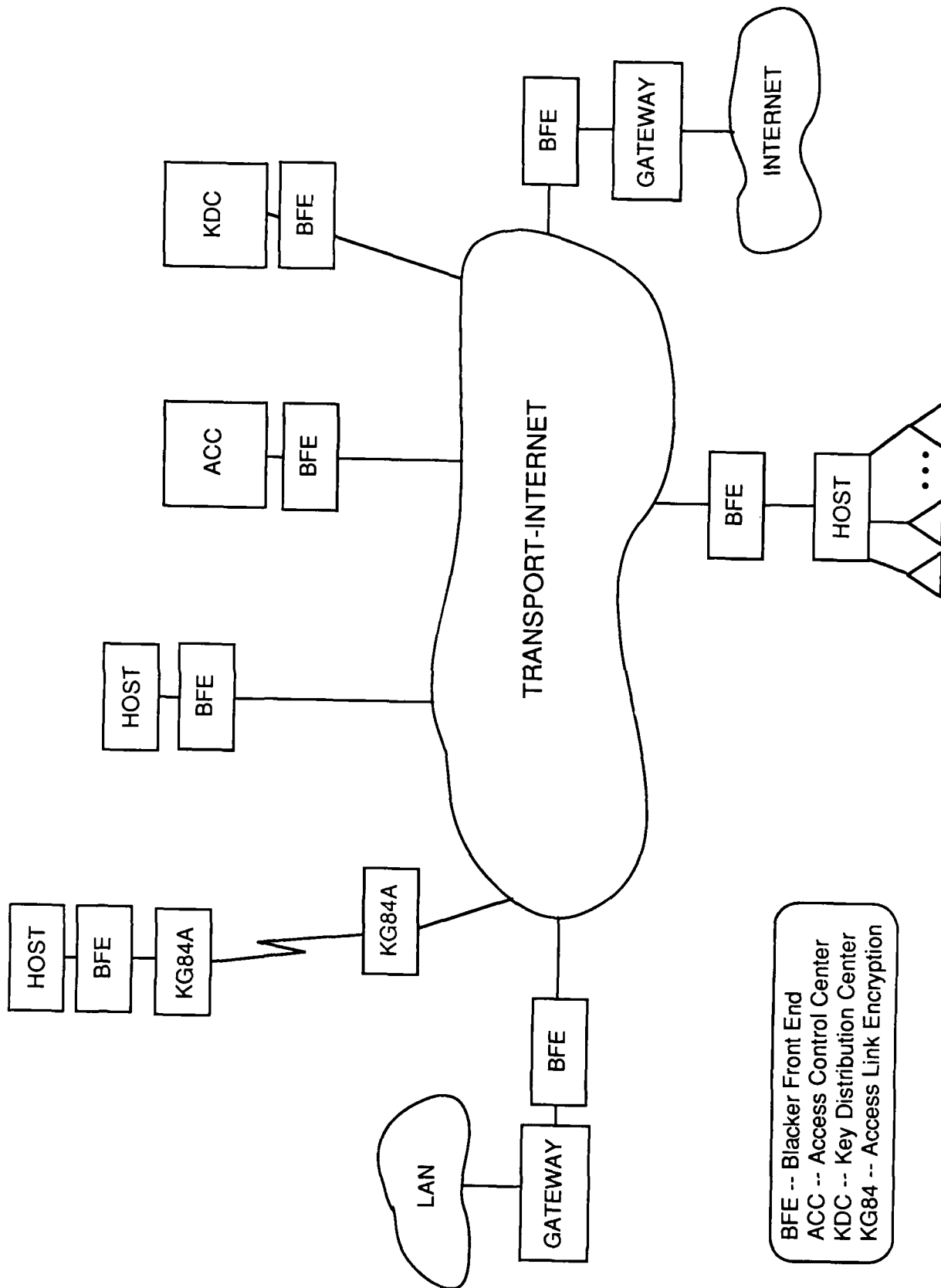
a) KG84A

- Replaces Data Encryption Standard (DES) equipment on Milnet
- Required on trunk and remote access lines
- Implemented on OCONUS and CONUS-OCONUS lines
- To be installed on CONUS trunks

b) Low-cost Encryption and Authentication Device (LEAD)

- Required on all terminal access lines
- DCSDS will fund for and acquire LEAD devices for all terminal access ports on TACs and Mini-TACs only
- Interface specification available first quarter 1987
- Approximate cost is less than \$500 each

TYPICAL BLACKER APPLICATION



4) Host-to-Host Encryption

a) Blacker Front End (BFE) — KI-111

- Replaces the Internet Private Line Interface (IPLI) in security architecture
- Will enable merging separate classified backbones
- Separate cryptographic keys will protect information at different security levels and for different accreditations
- Encrypts data, leaves address information in the clear
- Stores keys to communicate with 1,000 other BFEs
- Checks that encryption key is the same as decryption key
- Minimizes human intervention for key management
- Certified to A1 level, COMSEC certified
- Approximate cost \$8,000
- Initial delivery July 1987
- 1,000 in FY 1988 - 1989 funded by DCSDS and Services

b) Access Control Center (ACC) — SI-111

- Maintains tables of hosts and security classifications
- Three Access Control Centers and Key Distribution Centers located at DCA
 - Operations Center (OC), part of Monitoring Center (MC)
 - DCA Europe OC, part of European Regional MC
 - DCA Pacific OC, part of Pacific Regional MC
- 1,000 hosts can be run by Access Control Center
- Approximate cost \$85,000

c) Key Distribution Center (KDC) — SI-112

- Generates keys per host pair and per security level
- Approximate cost \$85,000

5) Terminal Access Control

TAC Access Control System (TACACS)

- Id and password are required to access a TAC
- Id and password are validated by network before access is allowed

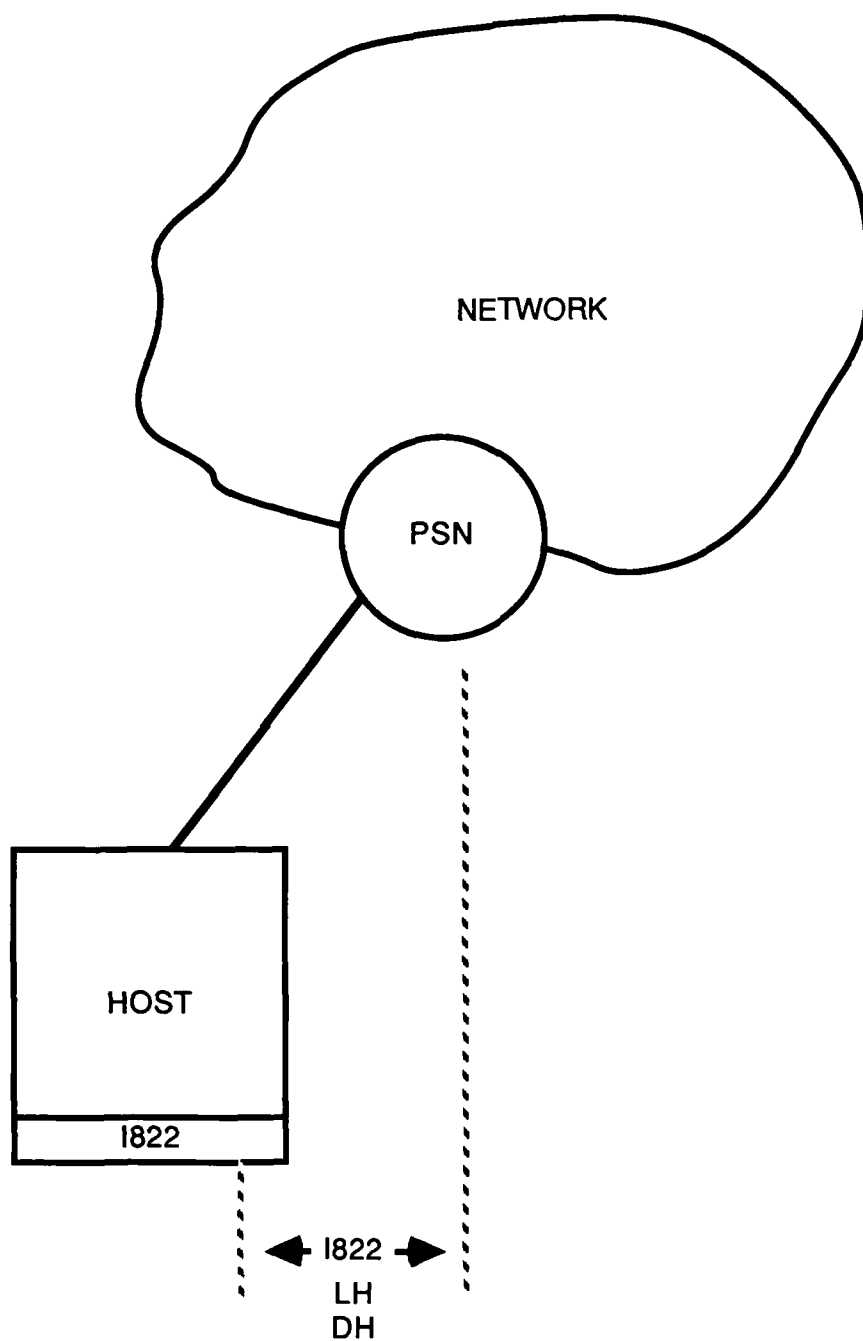
6) TEMPEST Shielding

- Used for all classified PSN and TAC requirements
- Installed at system high locations
- Mini-TAC will be fully compliant

7) Subscriber Hosts

- Checksum features of HDLC and TCP detect randomly generated errors
- Open system for hosts that meet discretionary access control C2 level
- Closed community for systems that do not meet multi-level or system high requirements
- Single level hosts must meet TCSEC class C2 requirements (1992)
 - Discretionary access control
 - User authentication
 - Documentation
 - Testing
- Multi-level secure hosts must meet Computer Security Center criteria levels as stated in "DoD Trusted Computer System Evaluation Criteria", 15 August 1983, CSC-STD-001-83 (Orange book); and "Guidance for Applying the DoD Trusted Computer System Evaluation Criteria in Specific Environments", 25 June 1985, CSC-STD-003-85 (Yellow book).

1822 LOCAL HOST/DISTANT HOST



8. The DoD Protocol Suite

A. DDN Access Protocols - Layers 1 through 3

1) 1822

a) Introduction

- Developed by BBN for the ARPANET to enable hosts to communicate through a network
- Interface is named after the document which describes the protocol, BBN Report No. 1822
- Also referred to as *Arpanet Host Interface Protocol* (AHIP)
- 4 variations, all using the same Network Layer Protocol
 - Local Host (LH)
 - Distant Host (DH)
 - Very Distant Host (VDH)
 - HDLC Distant Host (HDH)

b) Physical and Link Level Interfaces

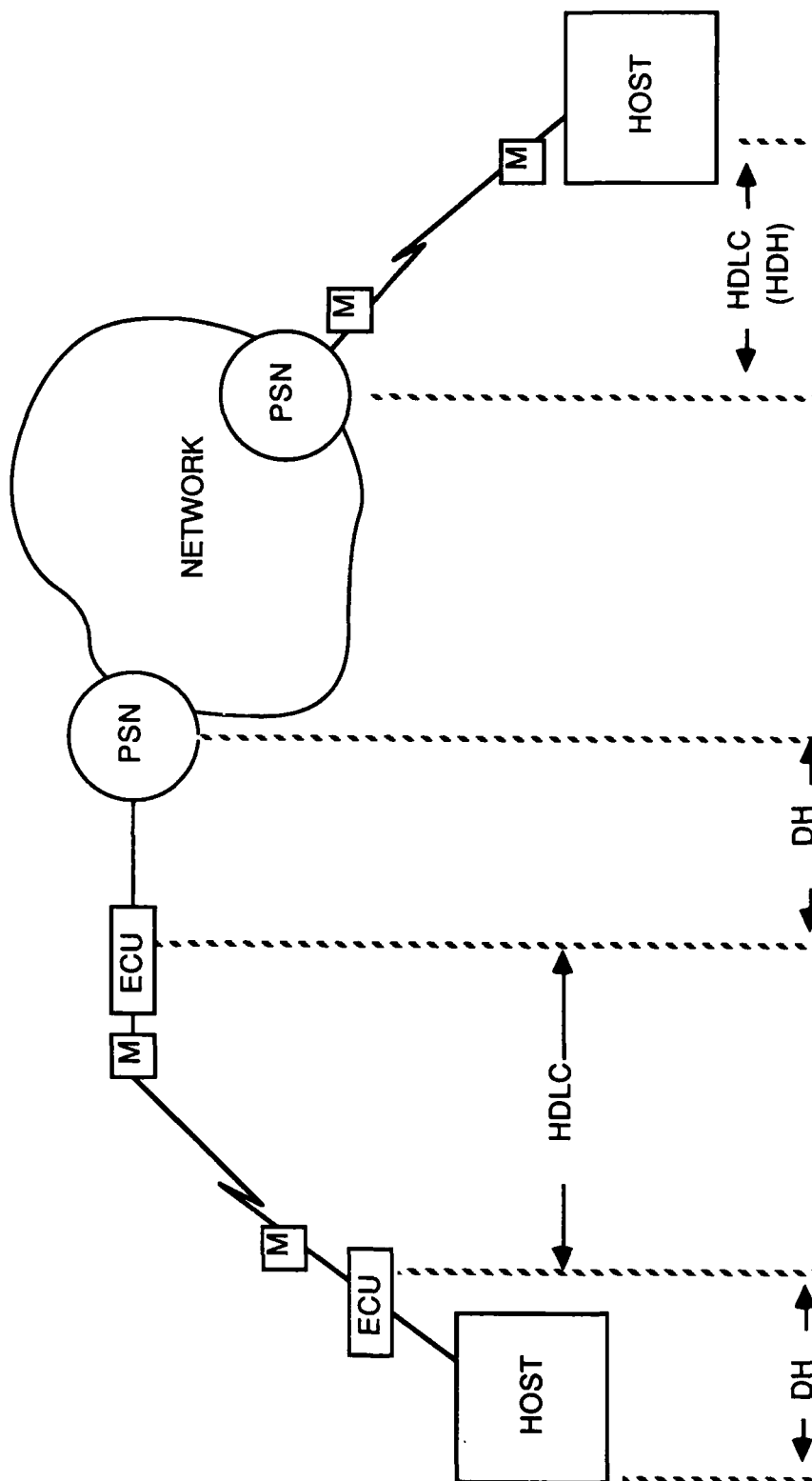
1. Local Host (LH)

- Distances up to 30 ft
- Cable contains 32 twisted pairs
- Uses 1822 bit serial network access protocol
- Arpanet only, not for new DDN subscribers

2. Distant Host (DH)

- For distances up to 2,000 ft
- Balanced cables are required with 10 twisted pairs plus 2 spare pairs
- Host must provide balanced drivers and receivers
- Uses 1822 bit serial network access protocol
- Host end and PSN end each require an Advanced Computer Communication (ACC) Error Correction Unit (ECU) box to "fake-out" the host and PSN by emulating an LH interface.
- HDLC is used between ECUs
- Arpanet only, not for new DDN subscribers

1822 OVER DATA LINK



3. Very Distant Host (VDH)

- For distances greater than 2,000 ft
- Uses 1822 bit serial network access protocol
- Arpanet only, not for new DDN subscribers
- Not supported in software release 7, to be fielded first quarter 1987

4. HDLC Distant Host (HDH)

- 1822 messages are encapsulated in one, or if necessary several, HDLC information frames
- Uses HDLC framing between host and PSN
- Implemented by new DDN subscribers as alternative to X.25
- Uses synchronous interface similar to X.25

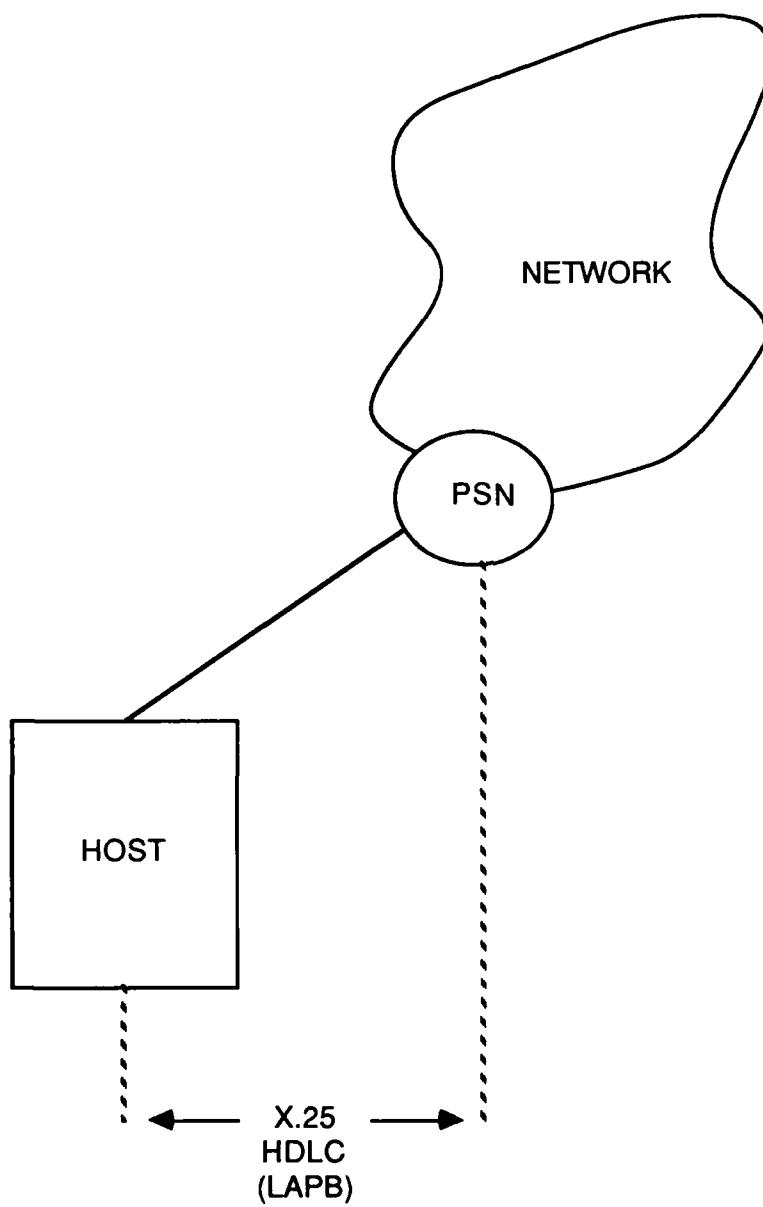
c) Network Layer

- All 4 variations of 1822, (LH, DH, VDH, and HDH), use the 1822 packet format
- Header information provides routing, flow control

d) References

"Interface Message Processor - Specifications for the Interconnection of a Host and a PSN", Report No. 1822, BBN.

X.25 COMMUNICATION



2) DDN X.25

a) Introduction

- In 1968, the International Telegraph and Telephone Consultative Committee (CCITT) established a study effort to develop international standards in the field of data communications.
- In 1972, Study Group VII was formed to develop standards for public data networks.
 - Work resulted in the X-series of Recommendations
 - Recommendation X.25 defines the interface between Data Terminal Equipment (DTE) and Data Circuit-terminating Equipment (DCE)
 - Originally published in 1976, augmented in 1980, and again in 1984

b) X.25 Protocol Layers

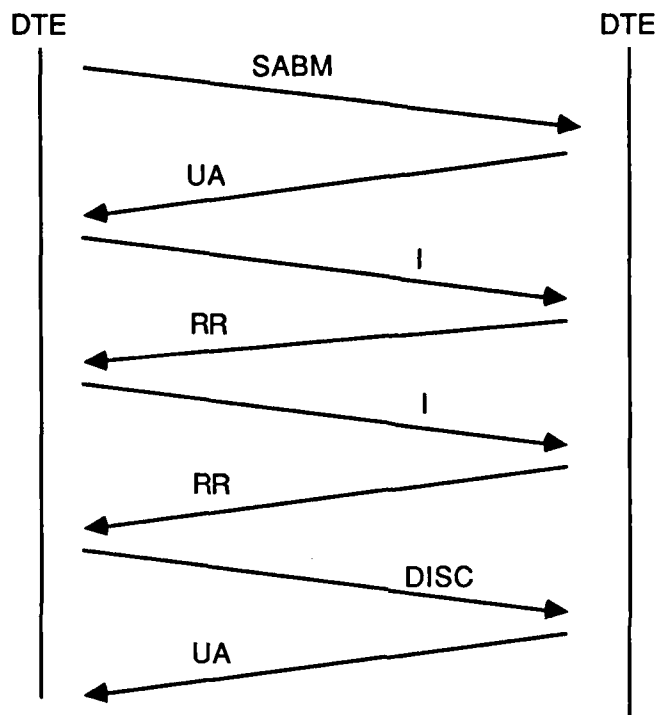
1. Physical Level

The C/30 PSN supports the following 4 synchronous interfaces:

- EIA RS-232-C, CCITT V.28 & V.24-unbalanced
 - 25 pin connector
 - Used for serial and parallel voice-band modems, public data network interfaces, telegraph/telex interfaces and automatic calling equipment
 - Supports data rates up to 19.2K bps at distances to 50 ft

- MIL-STD-188-114 balanced, EIA RS-449 & 422, CCITT V.11, FED. STD. 1031/1020
 - Used for serial voice-band and wide-band modems
 - Supports data rates up to 56K bps
- MIL-STD-188-114 unbalanced, EIA RS-449 & 423, CCITT V.10, FED. STD. 1031/1030
 - Used for serial voice-band and wide-band modems
 - Supports data rates up to 9.6K bps
- CCITT V.35
 - Balanced electrical characteristics used on data and timing circuits
 - 34 pin connector used for wide-band modems
 - Supports data rates up to 56K bps

LINK SET-UP (HDLC LAPB) AND DISCONNECT



Flag	Address	Control	Information	FCS	Flag
01111110	8-bits	8-bits	X.25 Packet N-bits	16-bits	01111110

HDLC Information Frame

2. Link Level

Link access procedure for data interchange across the link.
Asynchronous Balanced Mode of HDLC (ISO Standard) or LAPB
(CCITT Standard)

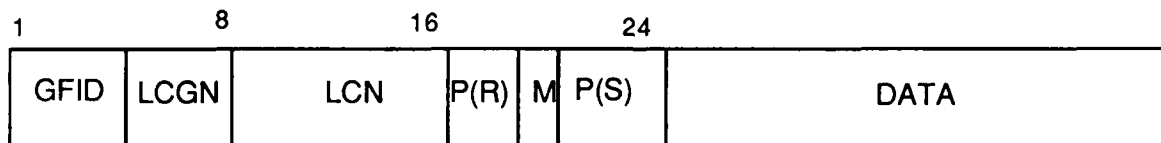
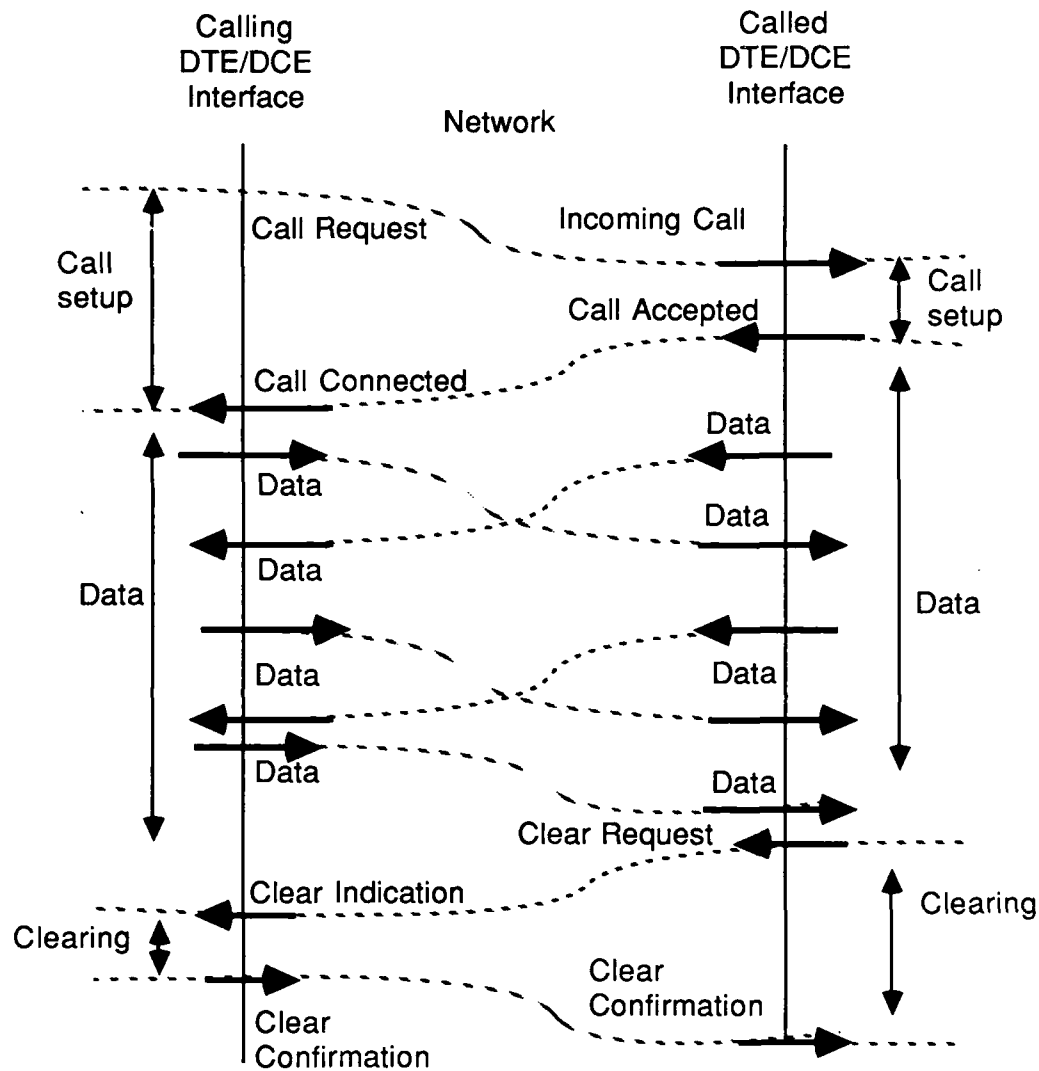
a) Frame Types

- Information (I)
- Supervisory (S)
 - Receive Ready (RR)
 - Receive Not Ready (RNR)
 - Reject (REJ)
- Unnumbered (U)
 - Set Asynchronous Balanced Mode (SABM)
 - Disconnect (DISC)
 - Disconnect Mode (DM)
 - Unnumbered Acknowledgement (UA)
 - Frame Reject (FRMR)

b) Frame Structure

- Flag sequence
 - Delineates frames
 - Transmitted continuously on active channel when no packets are being sent
- Frame Check Sequence (FCS)
- Sequence numbering
- Maximum of 7 unacknowledged frames

CALL ESTABLISHMENT, DATA TRANSFER, CALL CLEAR OF A VIRTUAL CIRCUIT



Data Packet

3. Network Level

Defines call set-up and clearing procedures.
Builds X.25 packet header.

- Logical channels
 - Enable simultaneous virtual circuits
 - 16 logical channel group numbers
 - 256 logical channel numbers
 - Total of 4,096 logical channels
 - Assigned during call set-up
- Delivery confirmation bit (D bit)
 - For end-to-end acknowledgement of delivery of a packet
 - Does not eliminate need for reliable higher level protocol for recovery from user or network generated resets and clears
- More data mark (M bit)
 - Indicates sequence of more than one packet (more data to follow)
- Flow control
 - Modulo 8 packet sequence numbering
- Throughput
 - Access line characteristics, window size
 - Number of active logical channels
 - Use of D bit

INTEROPERABILITY

	DDN Basic X.25	DDN Standard X.25	1822 HDH
Requires TCP/IP		x	x
Requires vendor ULP	x		
Support HDLC at link level	x	x	x
Communicates w/1822 HDH Hosts		x	x
Support Homogeneous Hosts	x	x	x
Support Heterogeneous Hosts		x	x
Communicate Across DDN Gateways		x	x
Reliability provided by transport protocol		x	x
Compatible with International Standard	x		
Provide for DDN Terminal to Host communication		x	x
Communicates with Basic X.25 Hosts	x		
Supports Blacker Devices		x	

c) Basic X.25 (DDN terminology only)

- Type of DDN X.25 service is specified in the Call Request packet at call set-up, Basic X.25 is the default.
- Supports D bit for end-to-end ack of sequence number
- Used by hosts with higher level protocol implementations requiring reliable packet delivery at the network level
- Not compatible with 1822
- Homogeneous hosts
- Cannot communicate across gateways
- Allows commercially available implementations

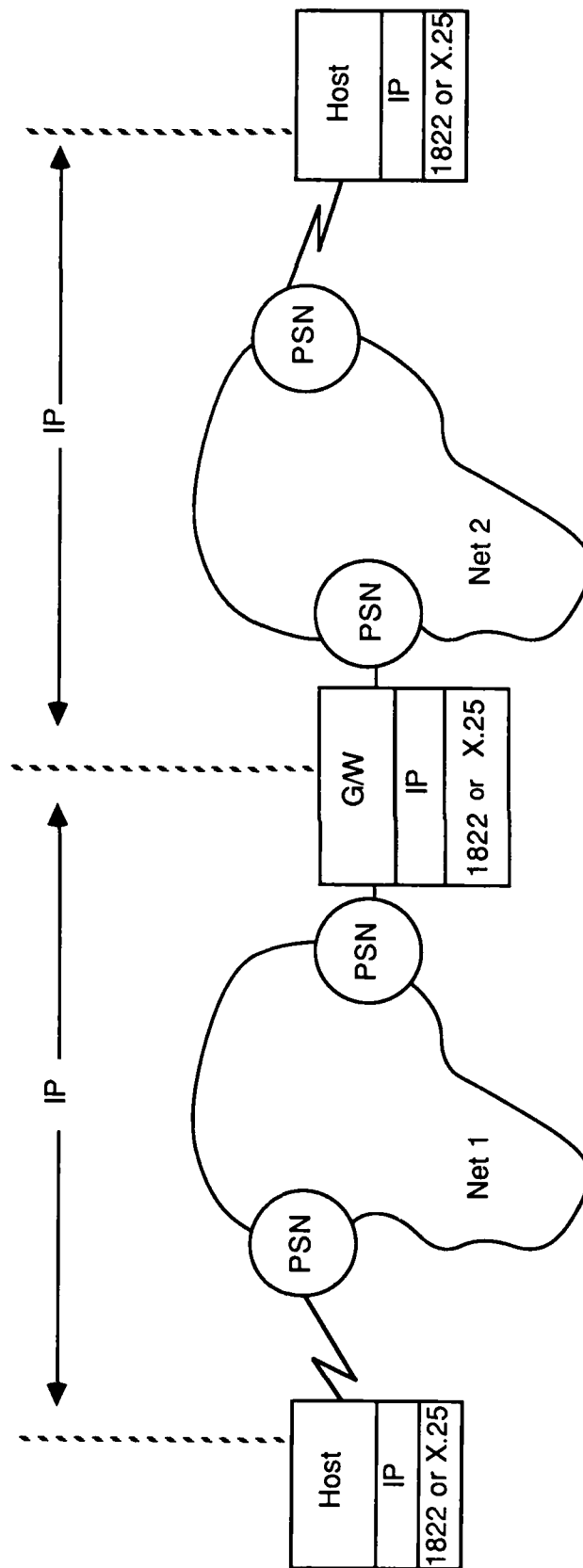
d) Standard X.25 (DDN terminology only)

- Provides local DTE to local DCE support
- D bit for end-to-end ack has no significance
- Reliability is provided by the transport protocol
- Compatible with 1822
- Maximum of 8056 bits per packet to be compatible with 1822 limitation of 8063 bit messages
- Maximum packet size of 1024, bytes best uses IP datagram size of 576 bytes
- Supports call precedence
- Call Request packet modified to indicate type of service is Standard X.25, and TCP/IP will be used in upper levels
- *Data packets remain the same as in Basic X.25*

e) References

"DDN X.25 Host Interface Specification", 1983, BBNCC.
FIPS 100/Federal Standard 1041.
"CCITT 1980 Yellow Book".

IP COMMUNICATION



B. INTERNET PROTOCOL (IP)

1) Introduction

- Traces its roots to a joint Xerox-Darpa project at Stanford University
- Interconnects networks with minimal impact on each network
- Interconnects networks with different internal protocols and performance
- Defines the format of internet packets and rules for protocol functions based on control information in the packet header
- Supports delivery of datagrams from source to destination. Each is an independent entity. There are no acks, no data checking, no retransmissions, and minimal flow control.
- One shot datagram protocol

2) Type of Service

- A generalized set of parameters is used to select characteristics for transmission through each network.
- Parameters require trade-offs between low-delay, high-reliability, and high-throughput.
 - Normal delay versus low delay
 - Normal throughput versus high throughput
 - Normal reliability versus high reliability
 - Generally, 2 of these 3 indications should be set
- 4 levels of precedence are used by the DDN to measure the importance of a datagram
 - Flash
 - Immediate
 - Priority
 - Routine

3) Length

- Hosts are required to accept or reassemble datagrams that are up to 576 bytes long
- Maximum length - 65,535 bytes, including header
- Minimum length - 28 bytes (20 bytes of header, 8 bytes of data)
- Default length - 576 bytes (512 bytes of data, 64 bytes of header)
- Maximum header length - 60 bytes
- Typical header length - 20 bytes (allows margin for higher level headers)

4) Fragmentation & Reassembly

- Required when a datagram originates in a local net that allows a large packet size and must traverse another net that limits packets to a smaller size
- A datagram marked "don't fragment" which is too large to be delivered to its destination without fragmentation, is discarded and an error message is returned to the host.
- Internet module must be able to forward datagrams of minimum 68 bytes (60 bytes of header, 8 bytes of data)

5) Time To Live (TTL)

Specifies the amount of time that the datagram is allowed to remain in the system. When TTL = 0, the datagram is discarded. Decreased each time the internet header is processed to reflect time spent processing the datagram.

Maximum length - 255 sec or 4:15 min.

6) Header Checksum

- IP level checksum is computed only on the IP header field
- The upper level protocol is responsible for checksums on its header and data fields
- Protects internet header fields from transmission errors
- Recomputed if header changes, (for example: changes to TTL, or to options, or changes due to fragmentation)

7) Addressing

To provide for flexibility in assigning addresses to networks and allow for the large number of small to intermediate size networks, the interpretation of the address field is coded to specify a small number of networks with a large number of hosts, a moderate number of networks with a moderate number of hosts, and a large number of networks with a small number of hosts.

Class A	7 bits of network, 24 bits of host
Class B	14 bits of network, 16 bits of host
Class C	21 bits of network, 8 bits of host

The local address must allow for a single physical host to act as several distinct internet hosts. The mapping between the host addresses and network interfaces must allow the interface to have more than one address and allow each host to have more than one interface.

8) Options

Options must be implemented by all IP hosts and gateways but they do not have to be transmitted in any particular datagrams.

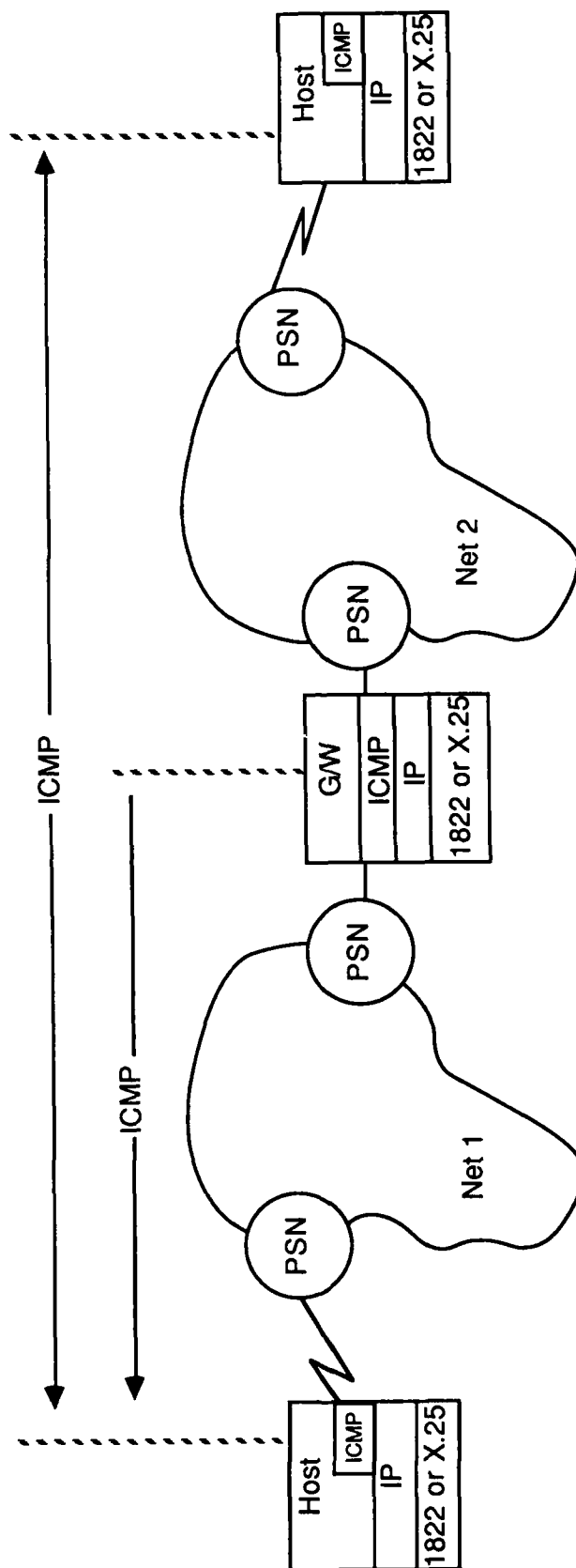
- Security - includes compartmentation, handling restrictions, transmission control code parameters
- Loose source routing - gateway or host IP can use any intermediate gateways to reach next address in route.
- Strict source routing - gateway or host IP must use next address in source route, (i.e., for small networks connected in adhoc arrangements where the destination may be unknown to the gateway)
- Record route - record the route of datagram
- Stream identifier - allows 16 bit SATNET stream id to be carried in networks that do not support stream data
- Internet timestamp - inserted by IP modules

9) References

"Internet Protocol", RFC-789.

"Internet Protocol", MIL-STD 1777, August 1983.

ICMP COMMUNICATION



C. INTERNET CONTROL MESSAGE PROTOCOL (ICMP)

1) Introduction

- Must be implemented in every IP module
- Used by a gateway or destination host to notify a source host of error conditions
- Uses the basic support of IP, including IP headers, as if it were a higher level but it is actually an integral part of IP implementation
- Designed to supply feedback about problems in network communications only
- Not designed to make IP reliable
- ICMP messages are sent when:
 - Datagram cannot reach its destination
 - Gateway does not have buffering capacity to forward a datagram
 - Gateway can direct the host to send traffic on a shorter route
 - Errors in handling fragment when fragment offset = 0

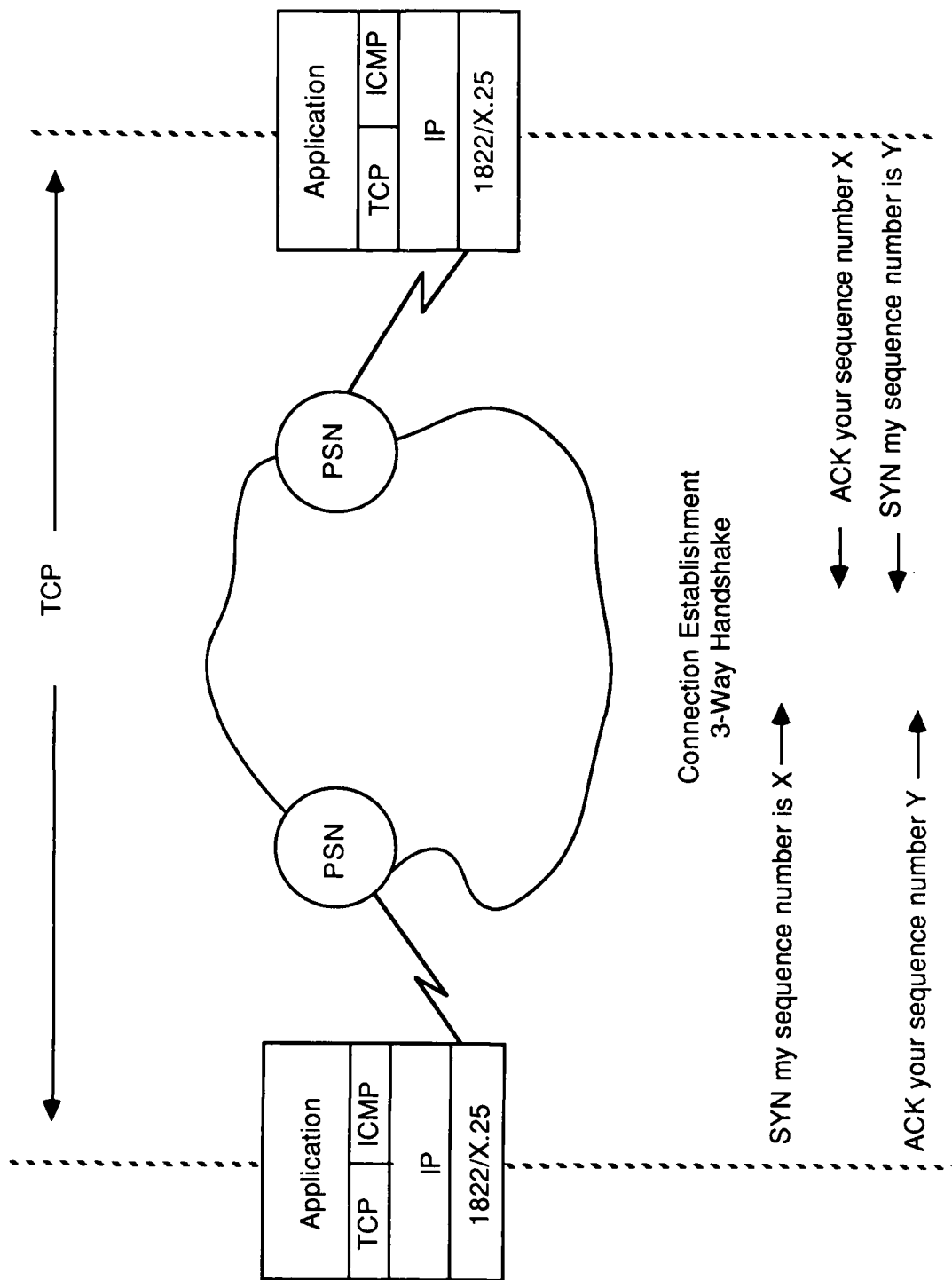
2) Message Types

- Redirect: indicates a shorter path
- Source quench: gateway discarded datagram due to insufficient buffer space
- Time exceeded: gateway discarded datagram because $TTL = 0$
- Parameter problem: either header is incorrect or options field contains an incorrect argument
- Destination unreachable: destination host or network is not available
- Echo or echo reply: aid in identifying a session
- Time stamp or time stamp reply: indicates when the message was manipulated last
- Information request or information reply: host can find out which network it is on

3) References

"Internet Control Message Protocol", RFC-792, September 1981.
"Internet Protocol", MIL-STD 1777, August 1983.

TCP



D. TRANSMISSION CONTROL PROTOCOL (TCP)

1) Introduction

- TCP was developed to replace the Network Control Protocol (NCP), a procedure for applications to send messages with a minimum of protocol mechanisms.
- TCP guarantees delivery and protects against duplicate datagrams
- TCP is connection oriented
- TCP complements IP to provide a reliable connection

2) Description

- Provides reliable inter-process communication between pairs of processes in hosts
- Designed to fit into a layered hierarchy of protocols which support multi-network applications
- Responsible for flow control, sequencing, reliability and host-to-host services
- Interfaces to user or application processes on one side and to a lower level protocol such as Internet Protocol, on the other
- Provides translation of the application name to a lower level address for routing through the network

3) Reliability

- Capable of recovering from data that is damaged, lost, duplicated or delivered out of order
- A copy of the sent segment is added to the retransmission queue and a timer is started
- If an ack is received, the segment is deleted; if an ack is not received and the timer expires, the segment is resent
- The ack indicates that the receiving TCP is delivering the segment to the end user
- The receiver uses the sequence numbers to arrange the segments in order and eliminate duplicates
- The checksum is checked and damaged segments are discarded

4) Flow Control

The receiver must be able to control the amount of data sent to it by the sender so that it does not get overloaded. The receiver uses a "window" to indicate an allowed number of bytes that the sender may transmit.

5) Multiplexing

- TCP provides a set of addresses or ports within each host to allow many processes within a host to use TCP simultaneously
- This number is concatenated with the network and IP protocol addresses to form the socket
- A pair of sockets uniquely identifies a connection.
- Well-known socket identifies a standard service, i.e., Telnet, FTP

AD-A173 472

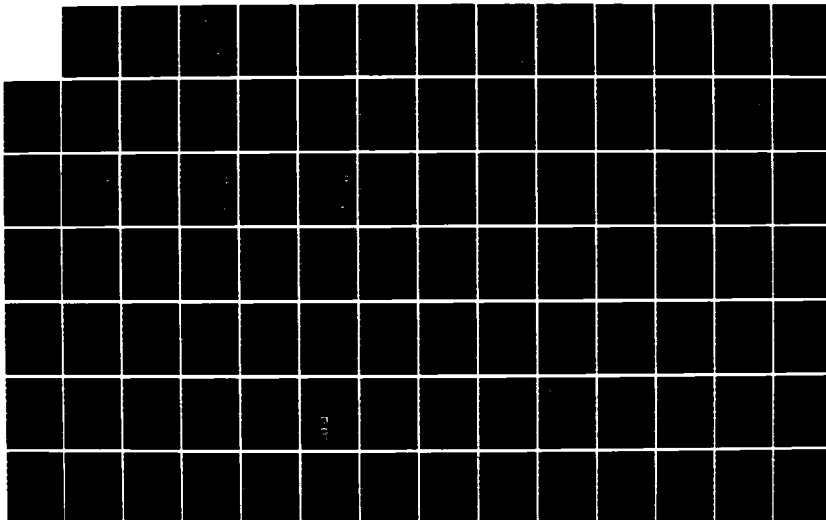
THE DDN (DEFENSE DATA NETWORK) COURSE(U) NETWORK
STRATEGIES INC FAIRFAX VA R DE VERE ET AL. APR 86
DCA100-83-C-0062

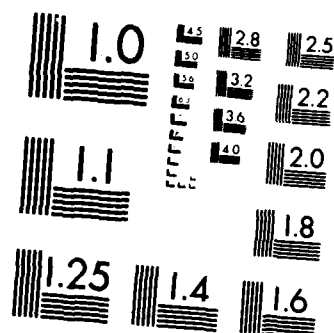
3/4

UNCLASSIFIED

F/G 17/2

NL





MICROCOPY RESOLUTION TEST CHART
NATIONAL BUREAU OF STANDARDS-1963-A

6) Maximum Segment Lifetime

Time TCP must wait upon startup or recovery from crash before assigning sequence numbers so as not to use ones remaining in network, approx. 2 min.

7) 3-Way Handshake for Connection Establishment

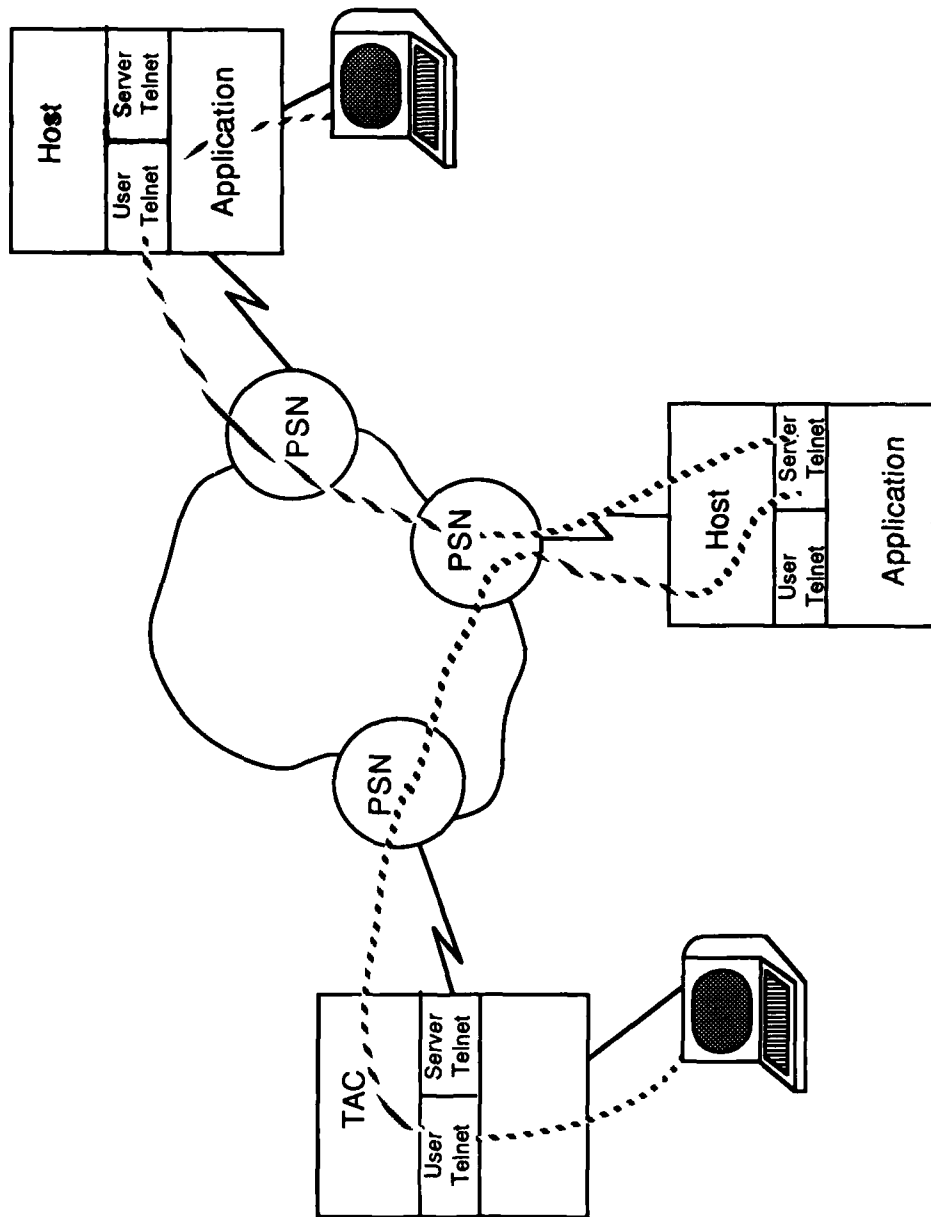
- The two TCPs synchronize on each other's initial sequence numbers
- Synchronization (SYN) requires each side to send its own initial sequence number and to receive confirmation of it in an ack from the other side
- Steps 2 and 3 (of diagram) can be combined in a single message so this is called the 3-way handshake

8) References

"Transmission Control Protocol", RFC-793, September 1981.

"Transmission Control Protocol", MIL-STD 1778.

TELNET



E. TELNET PROTOCOL

1) Introduction

- Not to be confused with the GTE-Telenet Public Data Network
- Telnet enables asynchronous terminals and terminal oriented processes to communicate
- It is based upon the following concepts:
 - The Network Virtual Terminal (NVT)
 - Negotiated options

2) Transmission of Data

- Full duplex connection
- NVT viewed as a half-duplex device operating in line-buffered mode
- Data may be accumulated in the host until a complete line is ready for transmission

3) Network Virtual Terminal

- Designed to provide a standard network-wide representation of a terminal
- Provides the options available to configure terminals when a connection is established
- The host does not need to keep information about terminal characteristics
- A party may refuse a request to enable an option, but can never refuse a request to disable an option
- All parties must be prepared to support the NVT

TELNET SESSION

DDN1-> telnet

* help

TELNET commands

Only enough of each command name to uniquely identify it need be typed.

help	Briefly explain each command.
?	Briefly explain each command.
verbose	Announce all subsequent option negotiation
brief	Announce only important option negotiations (remote echo)
ip	Interrupt process (send IP and Synch)
ao	Abort output (send and Abort-Output and Synch)
break	Break: that is, send a Break and Synch
ec	Erase last character (send EC)
el	Erase to beginning of line (send EL)
ayt	Ask foreign host if it is still alive (send AYT)
synch	Send a Synch
ga	Send a Go-Ahead
stty	Invoke the UNIX stty command
set	Set special characters
open	Open a connection to the specified host.
connect	Open a connection to the specified host.
close	Close the current network connection
x	Pass the rest of the line to the shell for execution
quit	Exit from TELNET immediately
* open ddn2	
TCP trying...	
Open	
Remote echo	

Welcome to DDN2 running BBN O/S BBNCC Rel. 5.3 23-Jan-1984 kernel cc5.3
; login:

Password:

BBNCC Release 5.3 23-Jan-1984

WELCOME to DDN-2 MASSACHUSETTS 26.3.0.72 C Machine Release 5.3

*** THIS HOST IS A DDN MAIL SERVER ***

*** PLEASE RESTRICT USE TO INFOMAIL ONLY ***

Term = (unknown) vt100

Erase set to Backspace

Kill set to Control-U

DDN2->

a) User vs. Server Telnet

- User Telnet is located in the host which initiated the connection or to which the terminal is normally connected
- Server Telnet is in the host which terminates the connection or provides a service

b) Definitions

- Carriage return, line feed, null: have specified meanings and codes (13, 10, 0, respectively)
- Bell, back space, horizontal tab, vertical tab, form feed: defined, but not required, meaning and codes (7, 8, 9, 11, 12, respectively)

c) Control Functions

Telnet provides a standard representation for the following functions which are implemented by most server systems:

- *Interrupt Process (IP): to terminate an unwanted user process*
- *Abort Output (AO): clear output produced but not printed or displayed*
- *Are You There (AYT): provide visible evidence that system is still up and running*
- *Erase Character (EC): delete last undeleted character*
- *Erase Line (EL): delete entire line*

d) Options

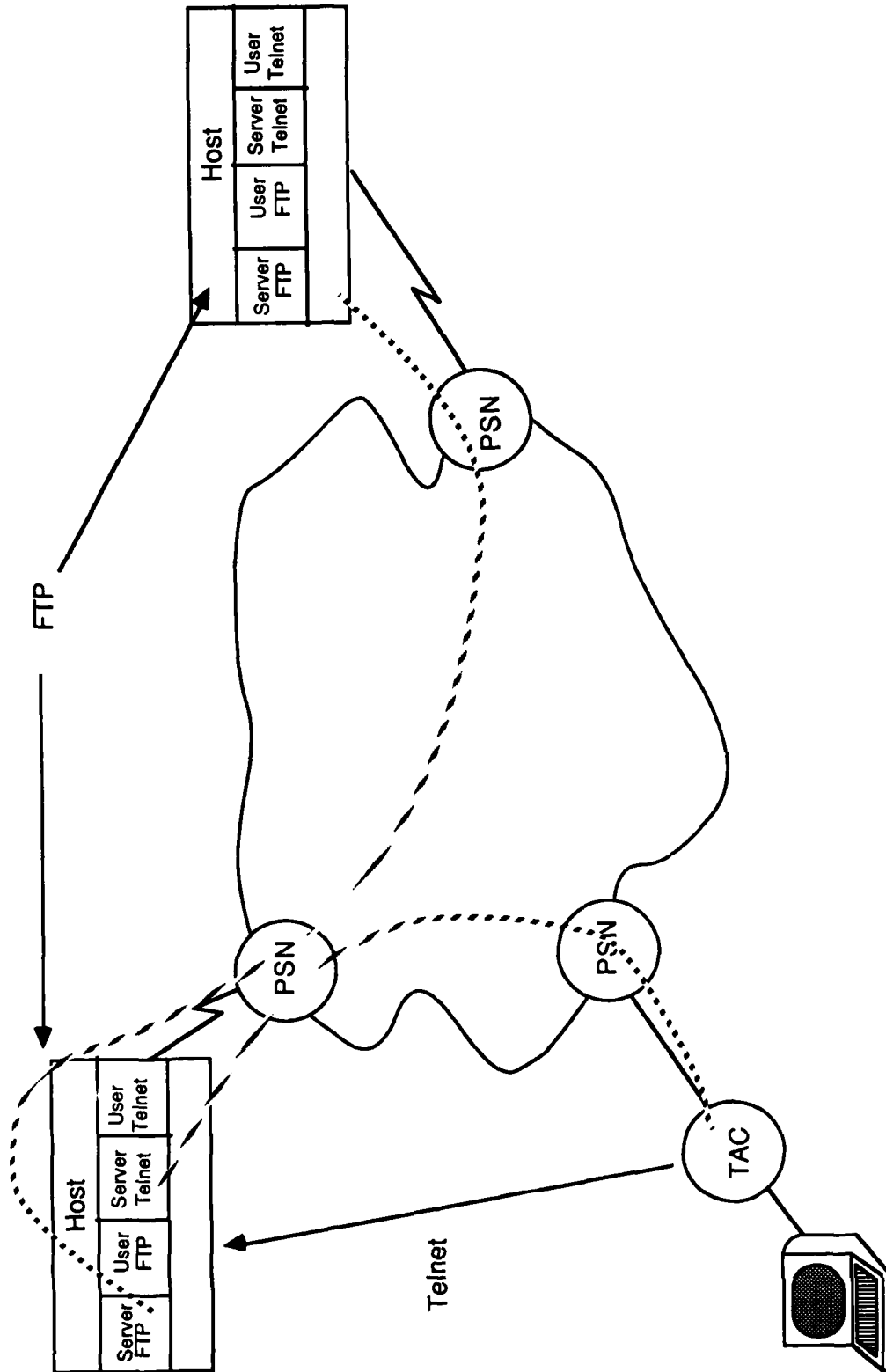
If both parties request an option simultaneously, each will see the other's request as a positive ack of its own request.

- Echo by host or terminal
- Suppress go ahead: for use with half-duplex locking terminals
- Status: allow user/process to verify status of an option
- Timing mark: mark data stream for changes to data
- Binary: receiver interprets data as 8 binary bits
- Extended options list: reserved for future use
- Terminal type: sent in response to request
- Terminal location number: for hosts in the same community
- TACACS user id Telnet: avoid double login at both TAC and host
- Output marking Telnet: support banners independent of application

4) References

- "Telnet Protocol Specification", RFC-854, May 1983.
- "Telnet Option Specification", RFC-855, May 1983.
- "Telnet Binary Transmission", RFC-856, May 1983.
- "Telnet Echo Option", RFC-857, May 1983.
- "Telnet Suppress Go Ahead Option", RFC-858, May 1983.
- "Telnet Status Option", RFC-859, May 1983.
- "Telnet Timing Mark Option", RFC-860, May 1983.
- "Telnet Extended Options - List Option", RFC-861, May 1983.
- "TACACS User Identification Telnet Option", RFC-927, December 1984.
- "Telnet Terminal Type Option", RFC-930, January 1985.
- "Output Marking Telnet Option", RFC-933, January 1985.
- "Telnet Terminal Location Number Option", RFC-946, May 1985.
- "Telnet Protocol", Mil-Std 1782, May 1984.

FTP



F. FILE TRANSFER PROTOCOL (FTP)

1) Introduction

- FTP promotes file sharing
- Facilitates use of remote computers
- Shields users from variations in file storage systems among hosts
- Transfers data reliably and efficiently
- Follows the specifications of TELNET for communication over the TELNET connection (for third party model to connect to FTP implementations)

2) Transmission Modes

- Stream
 - No restriction on representation type
 - Record structures are allowed
 - Passes data with little or no processing
- Block
 - Data blocks preceded by 1 or more header bytes with count field (length) and descriptor code (EOF, EOR, restart marker)
 - Formats data and allows for restart procedures
- Compressed
 - Compresses data consisting of replications or filler for efficient transfer
 - Allows for restart procedures

FTP SESSION

DDN2-> ftp nic

TCP trying nic (26.0.0.73)

Connections established.

220 SRI-NIC.ARPA FTP Server Process 5Z(25)-7 at Tue15-Oct-85 06:51-PDT

> log

Username: anonymous

331 ANONYMOUS user ok, send real ident as password.

Password:

230 User MILNET-FTP logged in at Tue 15-Oct-85 06:51-PDT, job 14.

> get

remotefile: < rfc>rfc949.txt

localfile: rfc.949

150 ASCII retrieve of <RFC>RFC949.TXT.1 started.

226 Transfer completed. 4130 (8) bytes transferred.

> quit

221 QUIT command received. Goodbye.

Transferred 4130 bytes in 1 seconds (33040 bps, 4130 bytes/sec)

3) Minimum Implementation Required

- Type
 - ASCII non-print
- Mode
 - Stream
- Structure
 - File
 - Record
- Command
 - User
 - Quit
 - Port
 - Type
 - Mode
 - Structure
 - Retrieve
 - Store
 - Noop
- Default values
 - ASCII non-print
 - Stream
 - File

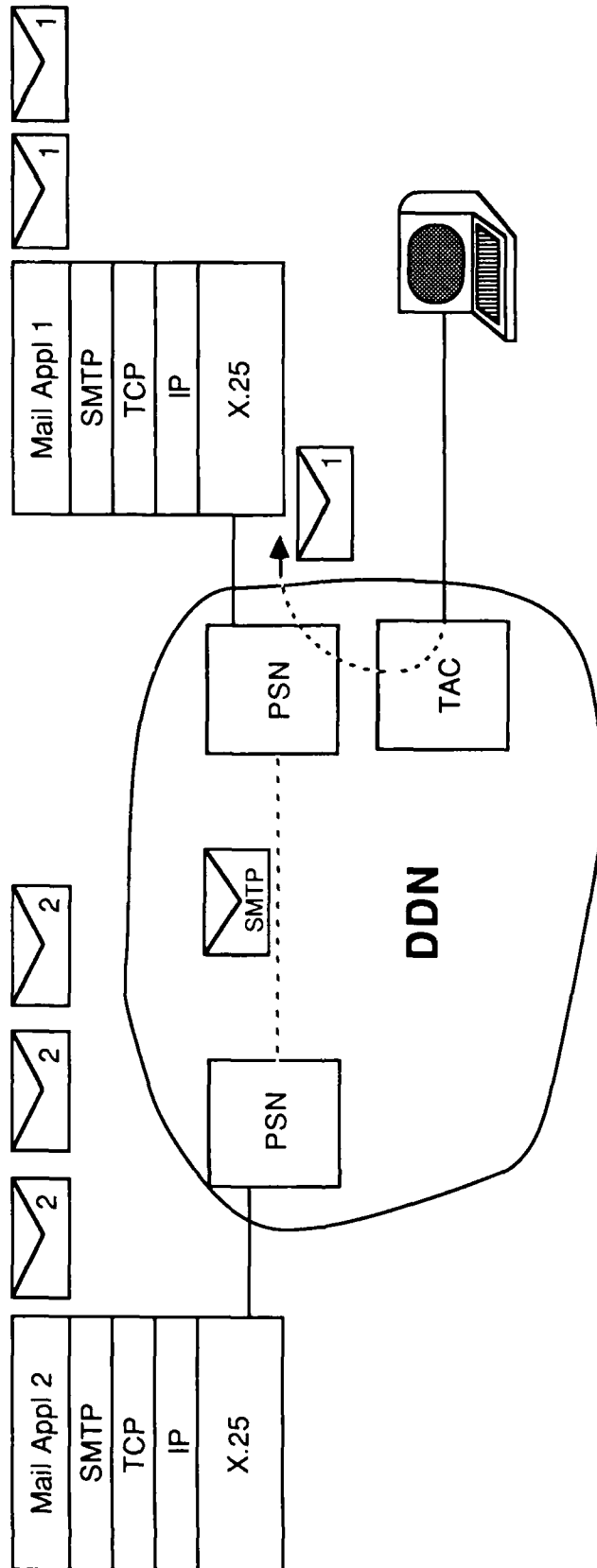
4) Establishing Data Connection

- Server receives transfer request
- Initiates data connection to the FTP port
- Connection is established
- Data transfer begins between server and user FTP processes
- Server protocol interpreter (server Telnet) sends confirmation to user protocol interpreter (user Telnet)

5) References

- "File Transfer Protocol", RFC-765, June 1980.
- "File Transfer Protocol", Mil-Std-1780, May 1984.

SMTP



G. SIMPLE MAIL TRANSFER PROTOCOL (SMTP)

1) Introduction

- SMTP is used to transfer mail reliably and efficiently
- To deliver messages to users' mailboxes
- Relay mail between hosts on different networks through a host on both of the networks

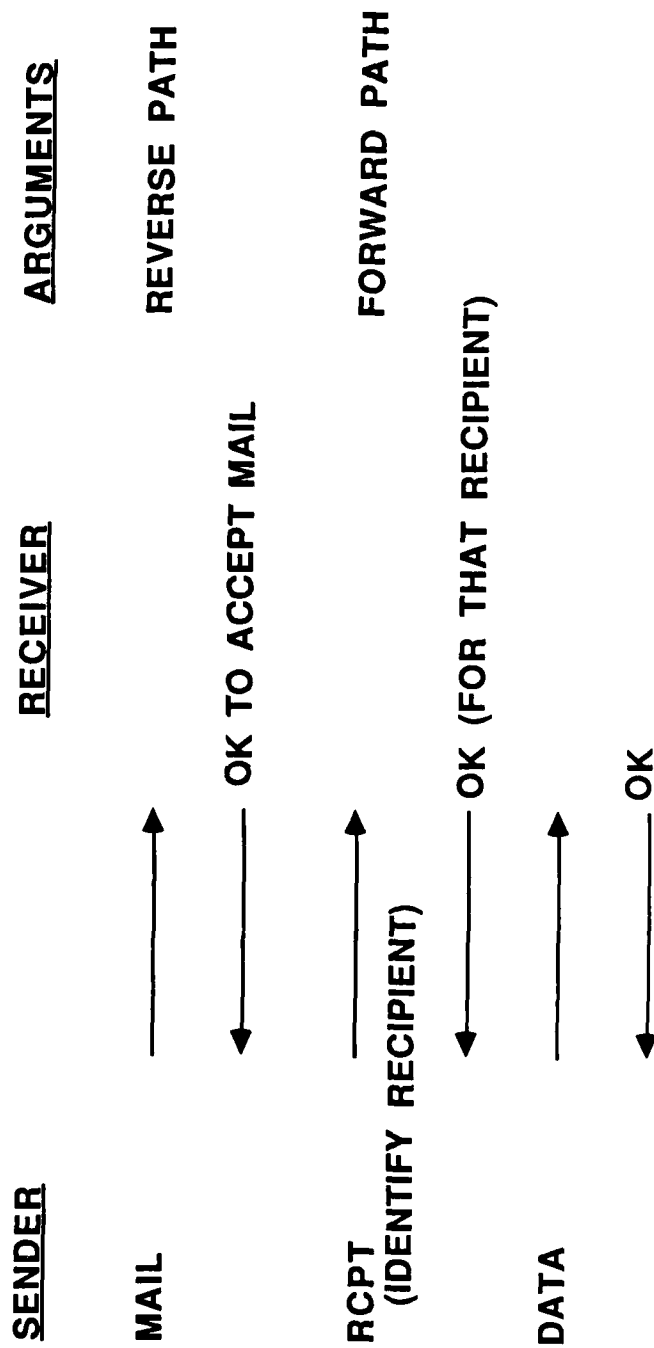
2) Mail Transmission Mechanisms

- Destination host, and destination mailbox name (name@host)
- Reverse-path, who mail is from; also called return route
- Forward-path, who mail is to; also called source route

3) Relaying

- Elements of the forward-path are moved to the reverse-path as the message is relayed from one server-SMTP to another.
- If a server-SMTP cannot deliver mail for any reason, it must build an "undeliverable mail" message and send it to the originator of the undeliverable mail.

SMTP SESSION



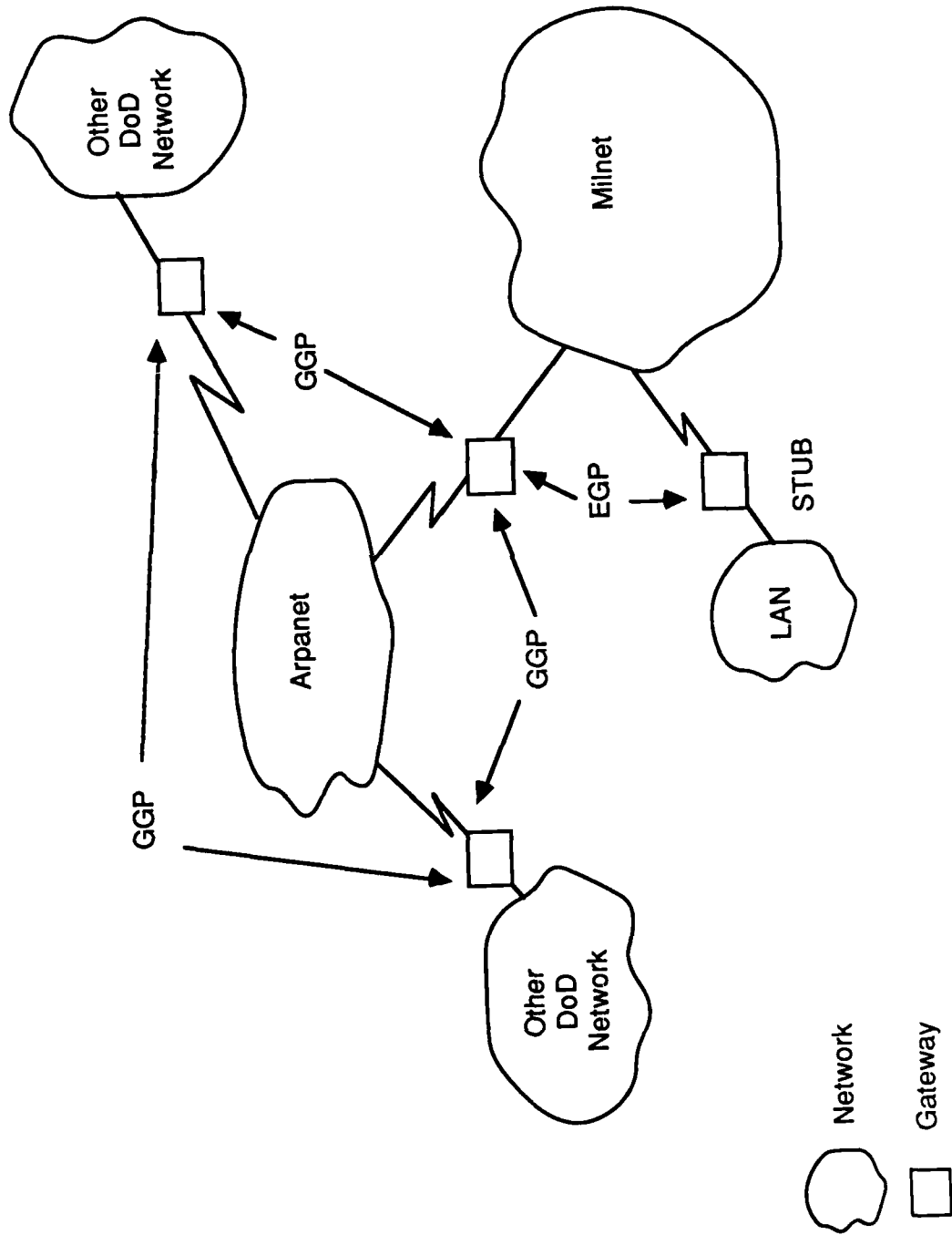
4) Domains

- Administrative entities to ensure responsible administration
- Divide name management of a central administration to sub-administrations
- Not based on geographical or technical constraints
- Administration requires controlling the assignment of names in a domain and providing access to those names

5) References

- "Simple Mail Transfer Protocol", RFC-788, November 1981.
- "Mail Header Format Standards", RFC-733, November 1977.
- "Simple Mail Transfer Protocol", Mil-Std 1781, May 1984.

GATEWAYS



H. GATEWAY PROTOCOLS

1) Overview

a) Introduction

- Enable communications between DoD networks
- Elements of a gateway system
- Act as loosely-coupled packet-switching communications systems
- Multiple sets of gateways which implement a composite single Internet System
- Homogeneous gateways under a single authority and control are best for maintainability and operability

b) Problem

- As more gateways were added, it became extremely difficult to keep updates current
- Other people wanted to write their own gateways
- Complexity and buffering requirements were beyond the capabilities of the hardware and software

c) Definitions

- **Autonomous system** — consists of a set of one or more relatively homogeneous gateways. The protocols and routing algorithm of these gateways will be a private matter and not necessarily implemented in gateways outside the particular system.
- **Internet** — set of autonomous systems, one of which consists of the DARPA gateways on ARPANET and SATNET (core system, used as transport or long-haul system)

- **Stub gateway** — interfaces a local network to the rest of the internet and only handles traffic originating or terminating on the local network. Could also be considered an autonomous system. Supports ICMP and EGP.
- **Interior neighbors** — part of same autonomous system (i.e., two core gateways on the same network)
- **Exterior neighbors** — not part of the same autonomous system (i.e., stub gateway and core gateway that share a network)

2) Gateway-Gateway Protocol (GGP)

a) Introduction

- GGP is used with the Internet Protocol (IP) to determine connectivity to networks and neighbor gateways
- Uses IP headers
- Is an example of an Interior Gateway Protocol

b) Functions

- Determine whether network interfaces are operational
- Determine if neighbor gateways are operational
- Build a table of networks reachable via neighbor gateways
- Add new neighbor gateways and new networks to its network table

c) Probe Packets

- The gateway sends itself "interface probe" packets every 15 sec to make sure it is still operational
- Sends "neighbor probe" packets to operational neighbors every 15 sec to make sure they are still operational

d) Update Messages

- Routing-update messages are sent to neighbor gateways when a change occurs in internet routing
- Routing update messages indicate the distance and address of the gateway on the shortest path to the network
- Cause the neighbor to recalculate its network table
- If a gateway goes down packets will be re-routed via an alternate gateway without disrupting host-to-host connections.

e) References

- "The DARPA Internet Gateway", RFC-823, September 1982.

3) Exterior Gateway Protocol (EGP)

a) Introduction

- Conveys network reachability information between neighboring gateways
- Has mechanisms to acquire neighbors, monitor neighbor reachability, and exchange update messages
- Used in gateways outside the core system
- Allows other gateways and gateway systems to pass routing information to Internet gateways
- Permits user to perceive all networks and gateways as part of one internal system even though 'exterior' gateways may use a routing algorithm not compatible with interior gateways

b) Messages

- Periodic polling Hello/I Heard You (I-H-U) messages monitor neighbor reachability and solicit update information
- Supports ICMP redirect and destination unreachable messages
- Neighbor acquisition — to pass routing information
- Neighbor reachability — decide if another gateway is up or down
- Network reachability information — pass routing information between gateways
- Gateway going down — messages sent to allow orderly going down

c) Network Reachability Information

- Each stub gateway has a list of networks reachable via that gateway including number of hops
- IP source address field of poll command specifies network common to each neighbor
- Update response includes a list of gateways on the common net

d) Gateway Lists

- Include gateways directly connected to the network specified in the IP source network field of the last received poll command
- Internal list
 - some or all of the gateways in the same autonomous system as the sender
 - nets reachable via these gateways
 - sending gateway is listed first
- External list
 - gateways in other systems known to the sender
 - EGP messages are designed to travel a single "hop", from one gateway to another one only
 - Hop counts are comparable between different gateways on the same system only, and are therefore on the internal list
 - Gateways belonging to designated core systems include the external list in their update responses

e) References

- "Exterior Gateway Protocol Formal Specification", RFC-904, April 1984.
- "Stub Exterior Gateway Protocol", RFC-888, January 1984.

SECTION IV

THE DDN: STRATEGIES FOR SUBSCRIBERS

**OBJECTIVES
OF
THE DDN: STRATEGIES FOR SUBSCRIBERS**

- **To understand the major interfacing issues concerned with connecting DoD systems to the DDN such as:**
 - **The different levels of interoperability obtainable through the DDN**
 - **Polled terminal protocol support on the DDN**
 - **Accommodating Local Area Networks and personal computers on the DDN and into the DoD architecture**

so that the student will be able to chose the best interface for his system.

- **To learn the procedures and time frame required to obtain DDN service to enable the student to initiate each step at the appropriate time so that all parties are prepared to complete the connection.**
- **To become familiar with the services provided by the Network Information Center so that the subscriber can make effective use of this network resource.**

9. Levels of DDN Interoperability

A. Definitions

1) DDN Network Services

The DDN provides a number of value-added network services to subscriber systems, including:

- **Transport** of data between any two subscriber locations, with both locations connected to the same network, or each location on a different subnetwork that is part of the DoD Internet (internetting)
- **Survivability** of communications, so that the network may continue to operate even in the event of multiple packet switching node or link outages. The DDN provides very high levels of communications availability. (This is one of the important distinctions between the DDN and typical commercial X.25 public data networks.)
- **Security** of data transmission, by using link encryption devices on selected links within the network, and end-to-end encryption (E3) devices such as Blacker on subscriber access links.

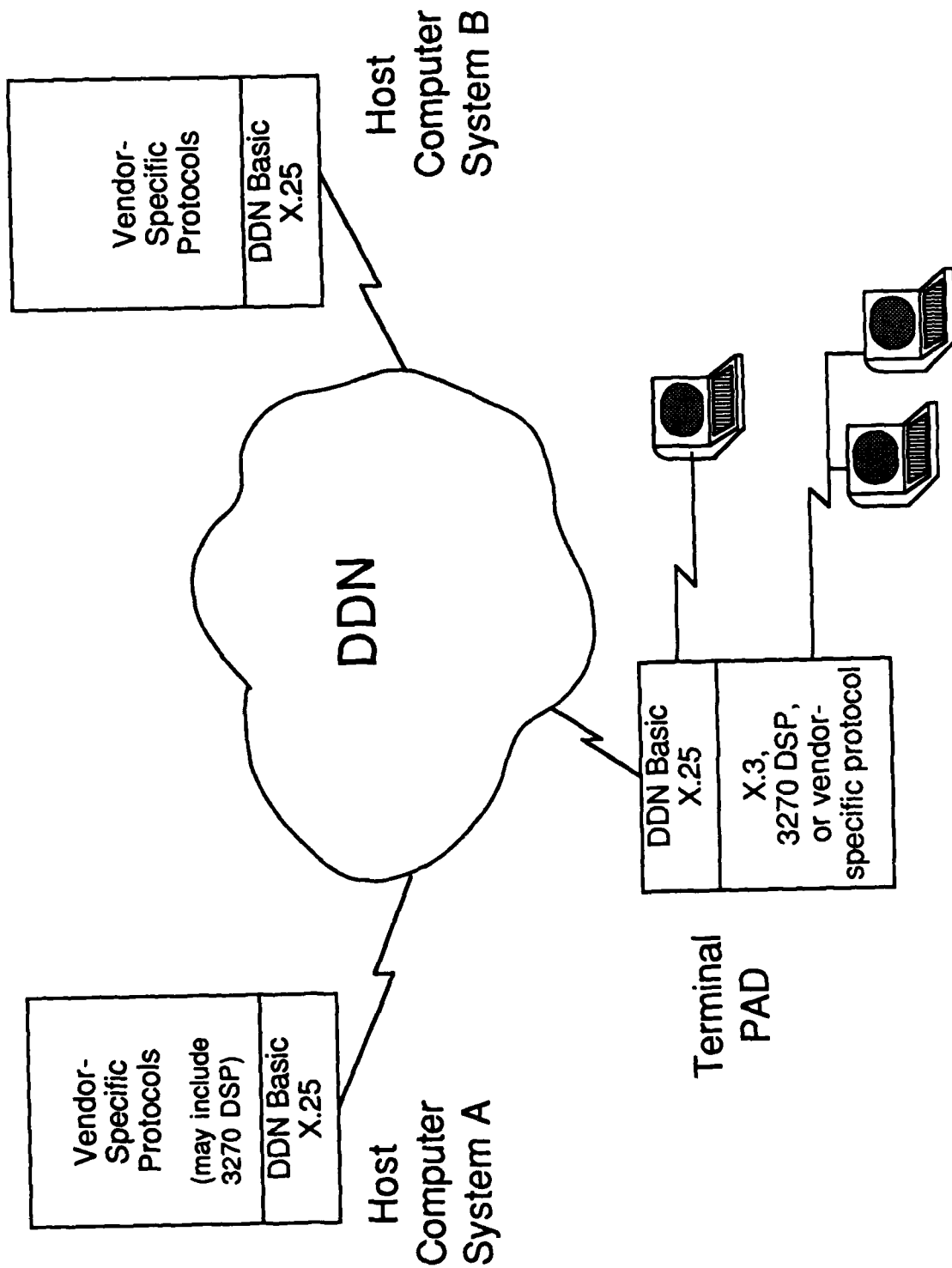
2) Interoperability

As a packet-switching network only, the DDN cannot guarantee interoperability.

Interoperability is the capability for two systems to communicate and actually "understand" each other, to permit useful work to be performed. Just because two subscriber systems are both connected to the DDN provides no assurance that these two systems can actually interoperate, or communicate. Unless both systems "speak the same language" (i.e., use common data communications protocols), interoperability is not guaranteed.

Depending upon the particular network interface used (described below), the DDN may provide all or some of the network services listed above. However, the services provided by the DDN do not by themselves provide **interoperability** between subscriber systems. Achievement of interoperability requires that subscribers implement the same end-to-end protocols in the subscriber's systems, *independent of service provided by the DDN.*

BASIC SERVICE



A good analogy is provided by the public phone system. An American in New York can pick up the phone, and by dialing the appropriate digits, call a Frenchman in Paris. However, unless the American knows French, or the Frenchman can speak English, the two persons cannot communicate (i.e., interoperate). The phone system provides transport of voice sounds between the two locations, but does not assure that real communications will take place between two people. Similarly, the DDN provides transport of data between two locations, but cannot guarantee interoperability.

B. DDN Host Interfaces

By using various DDN network service and subscriber system protocol implementation options, subscribers can implement the following host interfaces to the DDN:

- Basic Service Interface
- Full Service Limited Interoperability Interface
- Full Service Interoperable Interface
- Terminal Emulation Processor (TEP) Interface

1) Basic Service Interface

a) Description

- Implement X.25 only, with no use of TCP/IP or other DoD Internet protocol standards. Subscriber systems can utilize the DDN in virtually the same way that they would utilize a commercial X.25 public data network such as Tymnet, GTE Telenet, Uninet, etc.
- Uses 1980 CCITT Recommendation X.25 (Fed. Standard 1041), called "Basic X.25" by the DDN. (BBN does not support the CCITT 1984 Recommendation X.25.)
- Higher-layer protocols above X.25 are vendor-specific (e.g., SNA or DECnet)
- End-to-end message integrity is provided by use of the "D" bit (delivery confirmation) facility of X.25, or vendor-specific transport-layer protocols.

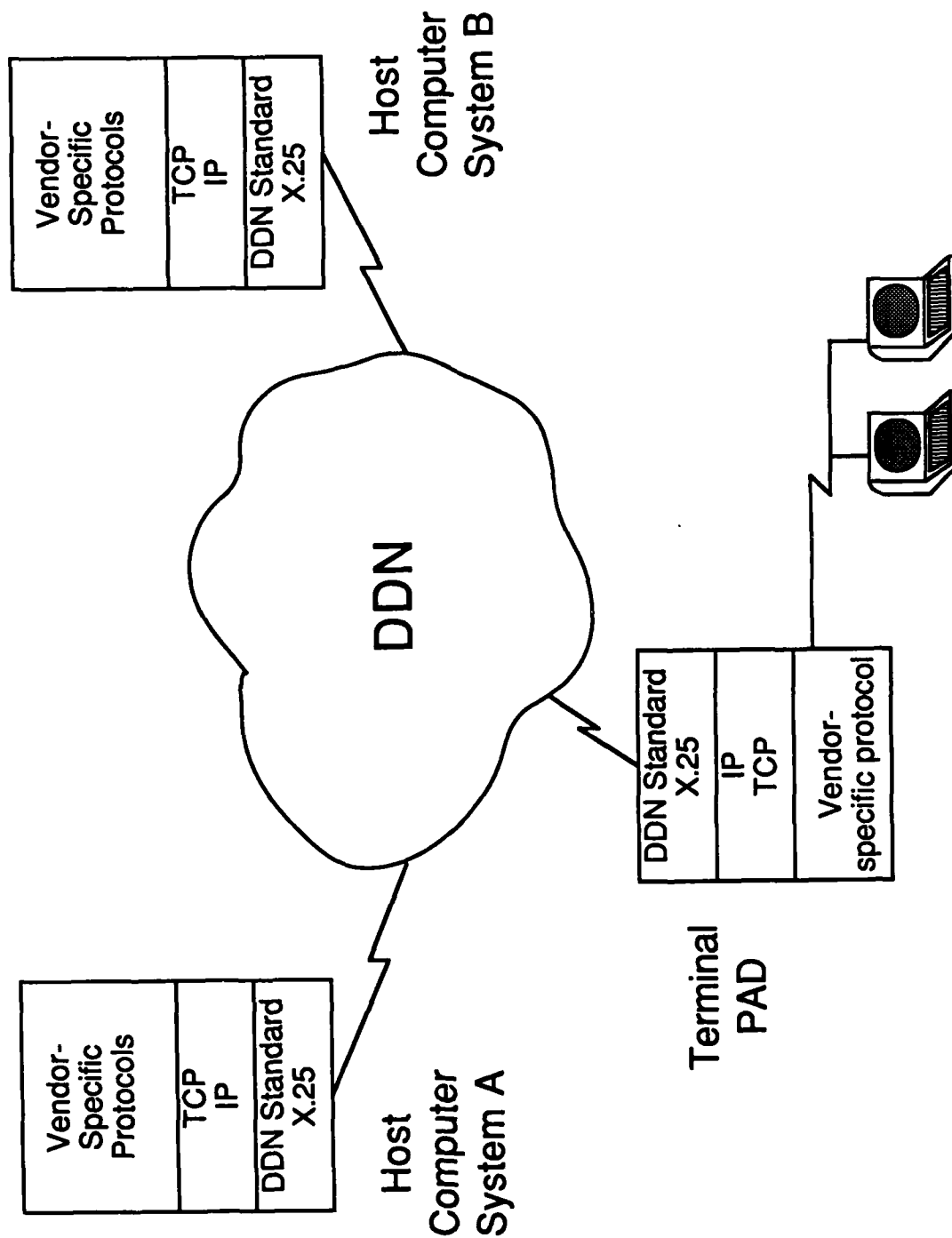
b) Advantages

- Standard commercial X.25 product implementations exist for virtually every type of computer system, and thus are readily available today. Subscribers can therefore utilize this type of DDN interface if TCP/IP implementations are unavailable (or until they become available) for their host system.
- Terminal X.25 PAD/protocol conversion devices are commercially available for terminals not supported by TACs or mini-TACs (e.g., SNA/SDLC 3270s, 2780 BSC RJE terminals, etc.)
- No impact on subscriber system application subsystems or user-written applications.

c) Disadvantages

- The use of vendor-specific high-level protocols above X.25 restricts interoperability to those subscriber systems that support these same protocols. For example, DECnet systems may be able to interoperate with each other, and SNA systems may be able to interoperate with each other, but DECnet and SNA systems cannot interoperate (unless the subscriber provides some other type of DECnet/SNA protocol converter).
- Subscriber systems are restricted to the Unclassified security level, since Blacker requires Standard X.25 and IP.
- Subscriber systems are restricted to a single subnet of the DDN (no internet capability), since their X.25 virtual circuits cannot communicate across DoD Internet gateways (IP would be required). Today the DDN is a single subnet of the DoD Internet, but this is expected to change in the future.
- Subscribers with remote terminal access requirements must provide their own X.25 PAD devices (to be paid for, controlled, and maintained by the subscriber organization) or wait for the mini-TAC.
- Monitoring Center cannot see Basic X.25 circuits for fault isolation.

FULL SERVICE LIMITED INTEROPERABILITY



2) Full Service Limited Interoperability Interface

a) Description

- Implement TCP/IP without use of higher-layer DoD Internet protocol standards such as Telnet, FTP, or SMTP.
- For the DDN network access protocol, subscribers would be expected to use a DDN-specific modified subset of the CCITT X.25 protocol, called "DDN Standard X.25". (This "non-standard" version of X.25 is required in order to permit interoperability with BBN's 1822 implementation in the C/30 PSN.)
- While DDN Standard X.25 is the recommended network access protocol, 1822 HDH will also be supported for ARPANET hosts.
- Higher-layer protocols above TCP are vendor-specific (e.g., SNA or DECnet).

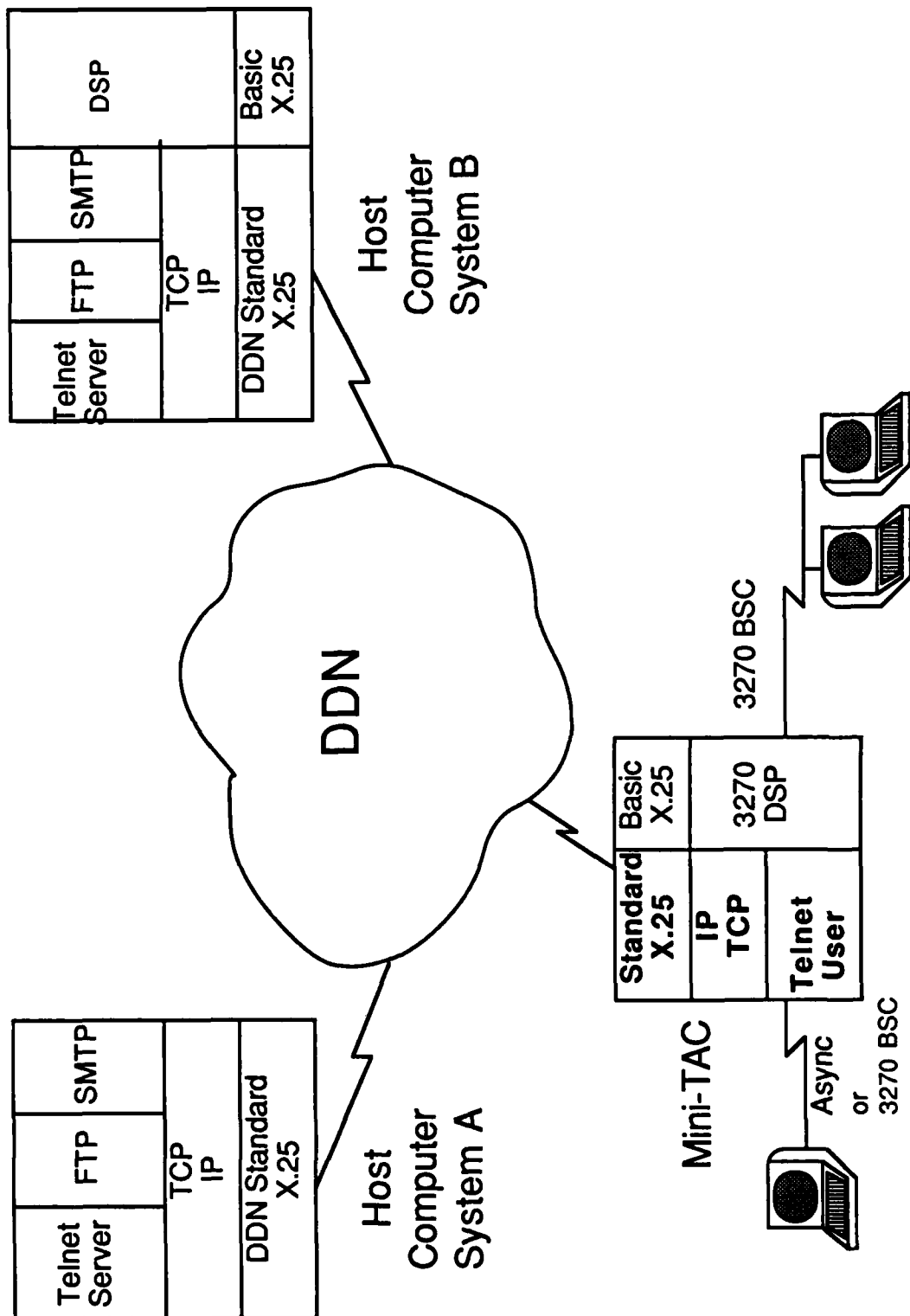
b) Advantages

- Support for TCP/IP allows multilevel security for subscriber systems that utilize DoD E3 devices (e.g., Blacker).
- Support for TCP/IP allows subscribers to communicate across multiple subnets of the DDN (or other DoD Internet subnets), since their TCP connections can cross IP gateways.
- Subscribers can continue to utilize vendor-specific protocols for higher layers, minimizing the impact on their applications. For example, forms-mode full-screen 3270 terminal sessions (unsupportable by the Telnet NVT protocol) can utilize SNA protocols on TCP connections.

c) Disadvantages

- The use of vendor-specific high-level protocols above TCP restricts interoperability to only those subscriber systems that support these same protocols. While TCP segments can be exchanged between subscriber systems, common higher-layer protocols must be used for interoperability.
- Vendor TCP/IP protocol implementations may be unavailable as standard products for specific subscriber systems. Much effort may be needed to integrate TCP into the host operating system.

FULL SERVICE INTEROPERABLE



3) Full Service Interoperable Interface

a) Description

- Implement TCP/IP and selected higher-layer DoD Internet protocol standards such as Telnet, FTP, or SMTP.
- For the DDN network access protocol, subscribers would be expected to use a DDN-specific modified subset of the CCITT X.25 protocol, called "DDN Standard X.25". (This "non-standard" version of X.25 is required in order to permit interoperability with BBN's 1822 implementation in the C/30 PSN.)
- While DDN Standard X.25 is the recommended network access protocol, 1822 HDH will also be supported for older ARPANET protocol implementations.

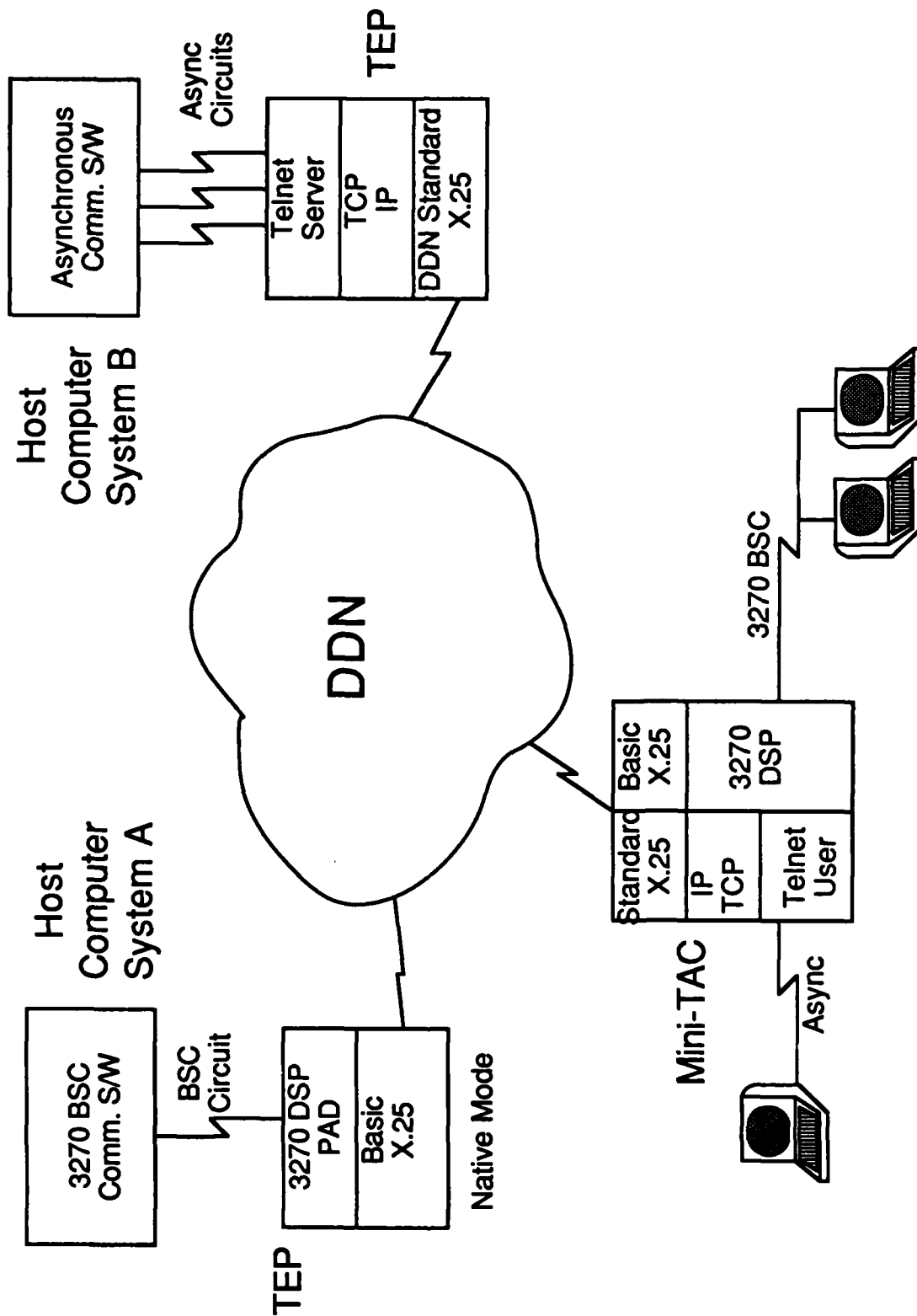
b) Advantages

- Support for TCP/IP allows use of DoD E3 devices (e.g., Blacker).
- Support for TCP/IP allows subscribers to communicate across multiple subnets of the DDN (or other DoD Internet subnets), since their TCP connections can cross IP gateways.
- Full interoperability with other subscribers on the DDN (or other DoD Internet subnets) who also have chosen to implement the complete DoD Internet Protocol Suite.

c) Disadvantages

- Vendor TCP/IP, Telnet, FTP, and SMTP protocol implementations may be unavailable as standard products for specific subscriber systems.
- Extensive modification of user-written applications is often necessary to use the higher-layer protocols of the DoD Internet Protocol Suite. It is sometimes very difficult (if not impossible) to modify these applications. For example, some applications written for forms-mode terminals cannot use the Telnet NVT protocol.

TEP INTERFACE



4) Terminal Emulation Processor (TEP) Interface

a) Description

- Implement DDN Standard X.25, TCP/IP, and Telnet Server in a Terminal Emulation Processor (TEP)
- Connect the host (or host FEP) to the TEP using one or more serial links, using asynchronous or 3270 BSC transmission.
- One serial link is required for each simultaneous asynchronous terminal session to the host.
- One serial link is required for each BSC multidrop line that is to be emulated to the host, with the number of lines determined by response time constraints.

b) Advantages

- No modifications are required to any subscriber host system software; use of the DDN is completely transparent to the host system. Consequently, a TEP interface may be appropriate for older systems that are going to be replaced soon, where the effort needed to develop (or the cost of) a Full Service DDN interface is not justified.
- Support for TCP/IP allows use of DoD E3 devices (e.g., Blacker).
- Support for TCP/IP allows subscribers to communicate across multiple subnets of the DDN (or other DoD Internet subnets), since their TCP connections can cross IP gateways.
- Full interoperability with other subscriber terminals on the DDN (or other DoD Internet subnets) who can access the TEP from any TAC.

c) Disadvantages

- All Telnet connections must be established from the terminal end, therefore, no files or electronic mail can be transferred across the DDN.
- Terminal sessions are restricted to those that can be supported by Telnet or the 3270 Display Systems Protocol (DSP).

3270 DATA STREAM

S B XX S_FY This is the header line
 A
 S B XX S_FY This is detail line 1
 A
 S B XX S_FY This is detail line 2
 A

This is the header line

This is detail line 1

This is detail line 2

SBA - Set Buffer Address
 XX - Screen Address
 SF - Start Field
 Y - Attribute Byte

10. Special Topics in DDN Interconnection

A. Polled Terminal Protocols and Full Screen Applications on the DDN

1) Introduction

- DDN, due to its Arpanet origins, was designed to support asynchronous terminals
- With the development of synchronous transmission, polling was usually required

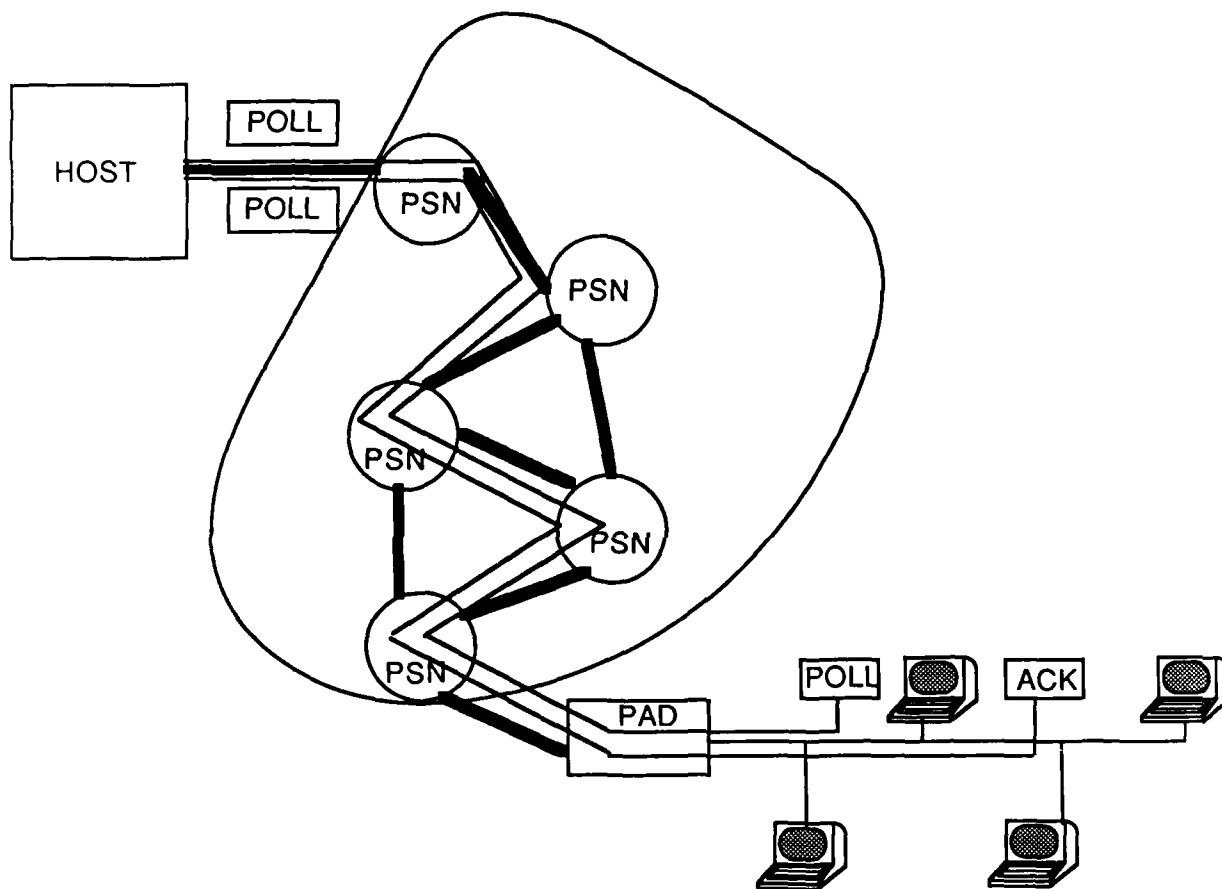
a) Terminal Characteristics

- Terminals became more sophisticated, supporting full screen and forms mode applications:
 - Protected fields or fill-in-the-blank application
 - Screen buffered
 - Read-modified capability
 - Special field oriented display characters - attributes
 - Highlighting
 - Reverse video
 - Intensity - regular, high, off
 - Color

b) Terminal Types Affected

- IBM 3270 terminal clusters using BSC or SNA/SDLC protocols
- Honeywell VIP terminals
- Sperry UTS terminals using Uniscope protocol
- Burroughs terminals using Burroughs' Poll / Select protocol
- 2780/3780 BSC

POLLING THROUGH A PACKET NETWORK



2) Problems with Polled Terminal Protocols on a Packet Switching Network

a) Response Time

User response time will increase due to the added delay associated with transmission of polling and selection messages across a packet network. The time required to go through the polling list will increase response time to unacceptable levels.

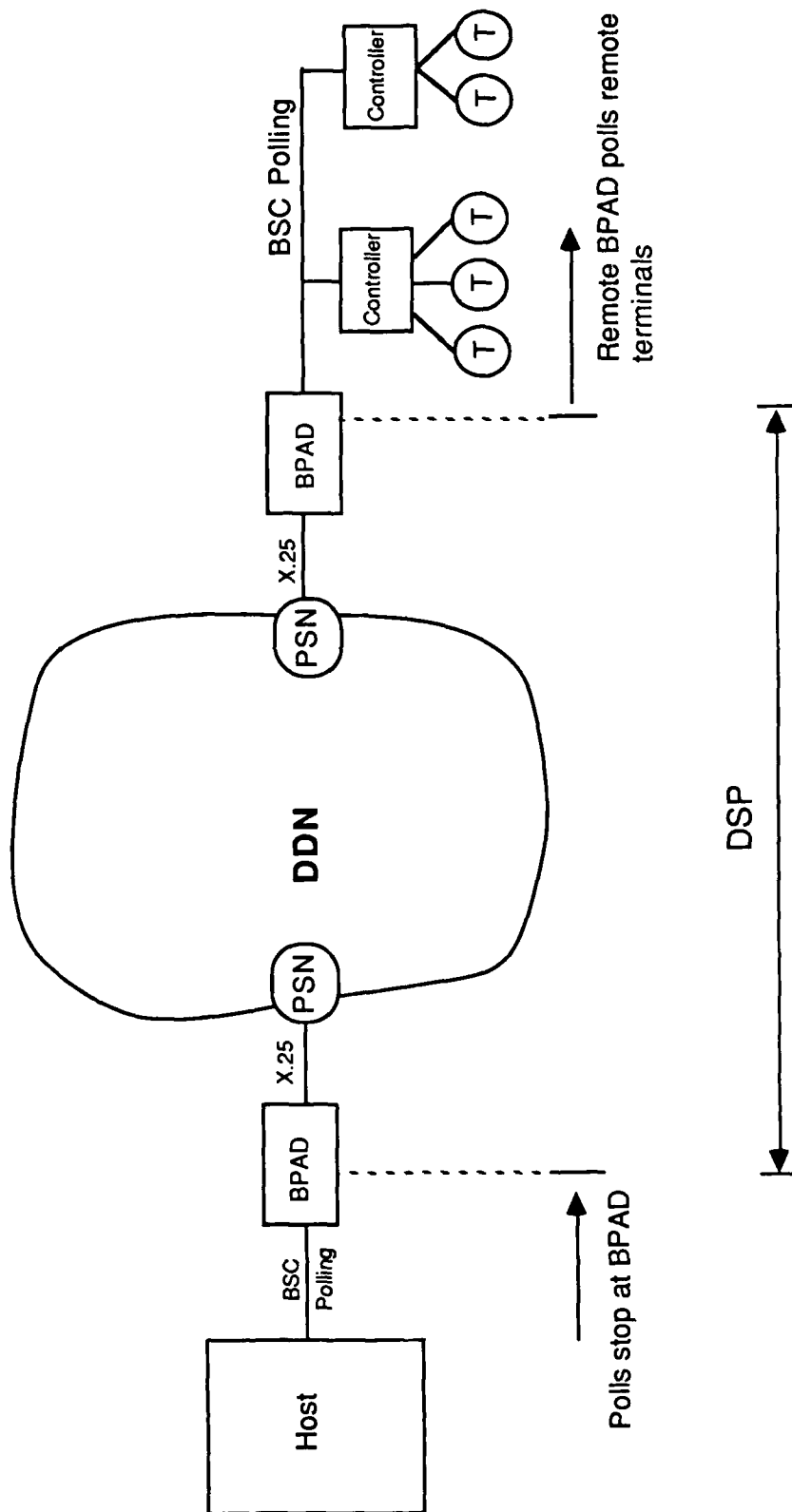
b) Network Overhead

Poll / select and ACK / NAK messages between hosts and terminals create a large amount of overhead traffic on a packet network.

c) Interoperability

Synchronous terminal protocols, of which polling protocols are a subset, are not provided for in the DoD protocol suite. The Telnet NVT cannot accommodate sophisticated screen features.

Protocol Converter



3) Solutions for Accommodating Polled Terminal Protocols on the DDN

a) Use a Protocol Converter to Perform Remote Polling of Terminals as Well as Conversion to X.25

Using a protocol converter such as a BSC PAD (BPAD) which uses a higher level protocol called Display System Protocol (DSP), the synchronous data stream can be converted to X.25 for transmission through the DDN.

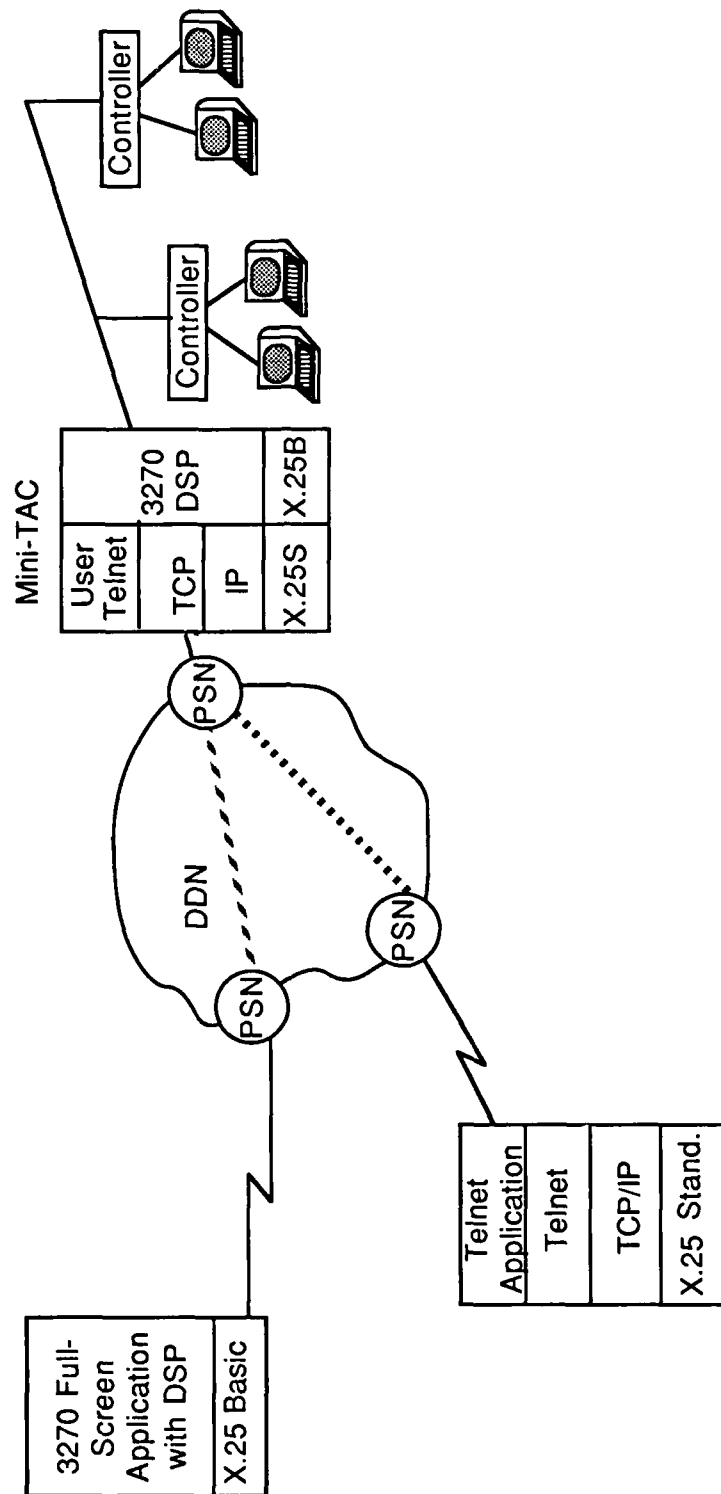
- Advantages

- Transparency to host and terminal — neither terminal nor host needs to be modified.
- Available today from multiple vendors.
- BPAD-like devices provide remote polling of terminals and thus do not create overhead traffic on the DDN.
- PADs with remote polling capability are currently available for virtually all IBM 3270 bisync devices.

- Disadvantages

- Does not allow interoperability with any other systems — Only those systems configured with similar devices will be able to interoperate.
- X.25-only connections cannot cross internet gateways — These systems will be limited to communication within a DDN internet network.

MINI-TAC



b) Incorporate Polled Synchronous Terminal Support in a Mini-TAC

Protocol will be converted in the mini-TAC to DSP protocol for transmission through the DDN.

- Advantages

- Full screen applications can still be used
- Allows complete interoperability with other synchronous DoD systems and terminals
- Transparent to host and terminal
- Allows internetwork communication
- TCP connections provide end-to-end error free communication.

- Disadvantages

- Forms mode full screen applications will not be interoperable with Telnet NVT
- Under development — Expected availability is first quarter 1987
- Will support IBM 3270 BSC terminals only

3270 BSC TERMINAL INTEROPERABILITY

	3270 Datastream Forms-Mode Application	Other Applications (Using ASCII)
Async Terminals	Telnet	No
3270 Terminals	Telnet	3270 DSP

c) Specify async terminals in any new systems procurements

d) Wait for International Standards

- Lead time required is too long for needs of current identified users
- No agreed upon standard exists regarding the type of NVT service which should be implemented
- Current DoD policy is to adopt commercial standards which meet military requirements
- Sensible to wait for and adopt commercial NVT standard (e.g., ISO VT)

B. Connecting Subscriber Local Area Networks to the DDN

1) Local Area Networks and the DDN

a) The DDN as a Collection of Networks

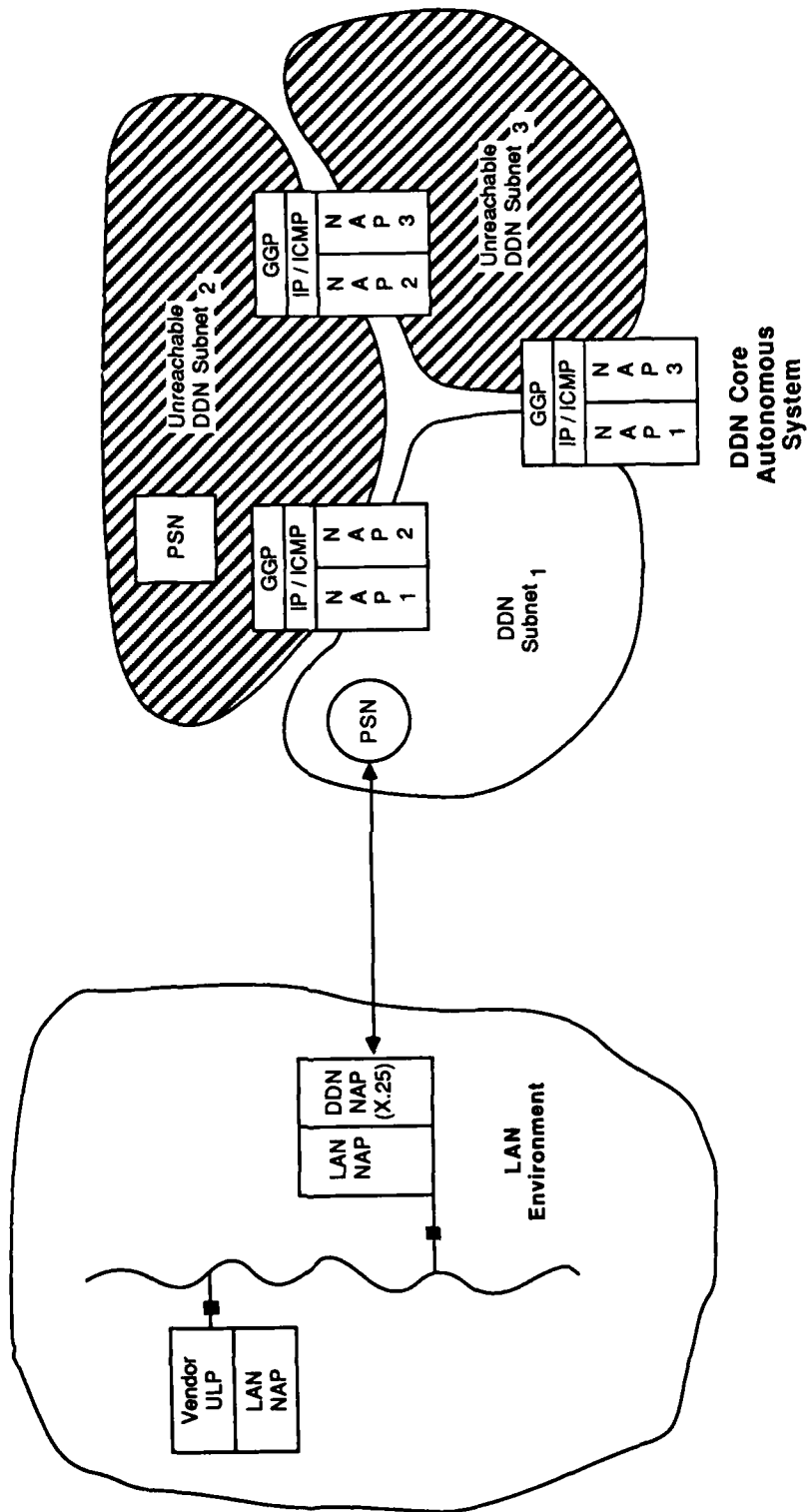
- The DDN is composed of several networks, which will be internetworked via DoD Internet Internal Gateways
- DoD Internet Gateways will implement the internal gateway protocol called GGP
- Subscriber LANs may be connected to the DDN by using a DoD Internet Gateway

b) Subscriber LANs

Subscriber Local Area Networks (LANs) connect to the DDN in one of three ways:

- X.25 Host Emulation "Gateway"
- TCP Host Emulation "Gateway"
- DoD Internet Gateway using EGP (i.e. , stub external gateway)

X.25 Host Emulation "Gateway"



2) X.25 Host Emulation "Gateway"

a) Gateway Protocol

There is no gateway protocol since the "gateway" is simply an X.25 host to the DDN, and a device on the LAN.

b) Description of Operation

- "Gateway" operates as a Network Access Protocol (NAP) translating device
- The "gateway" looks like an X.25 host to the DDN and to any user wishing to access the LAN from the DDN
- The "gateway" looks like a LAN device to all other devices on the LAN
- User information is passed from the LAN to the DDN with all vendor-specific upper layer protocols intact

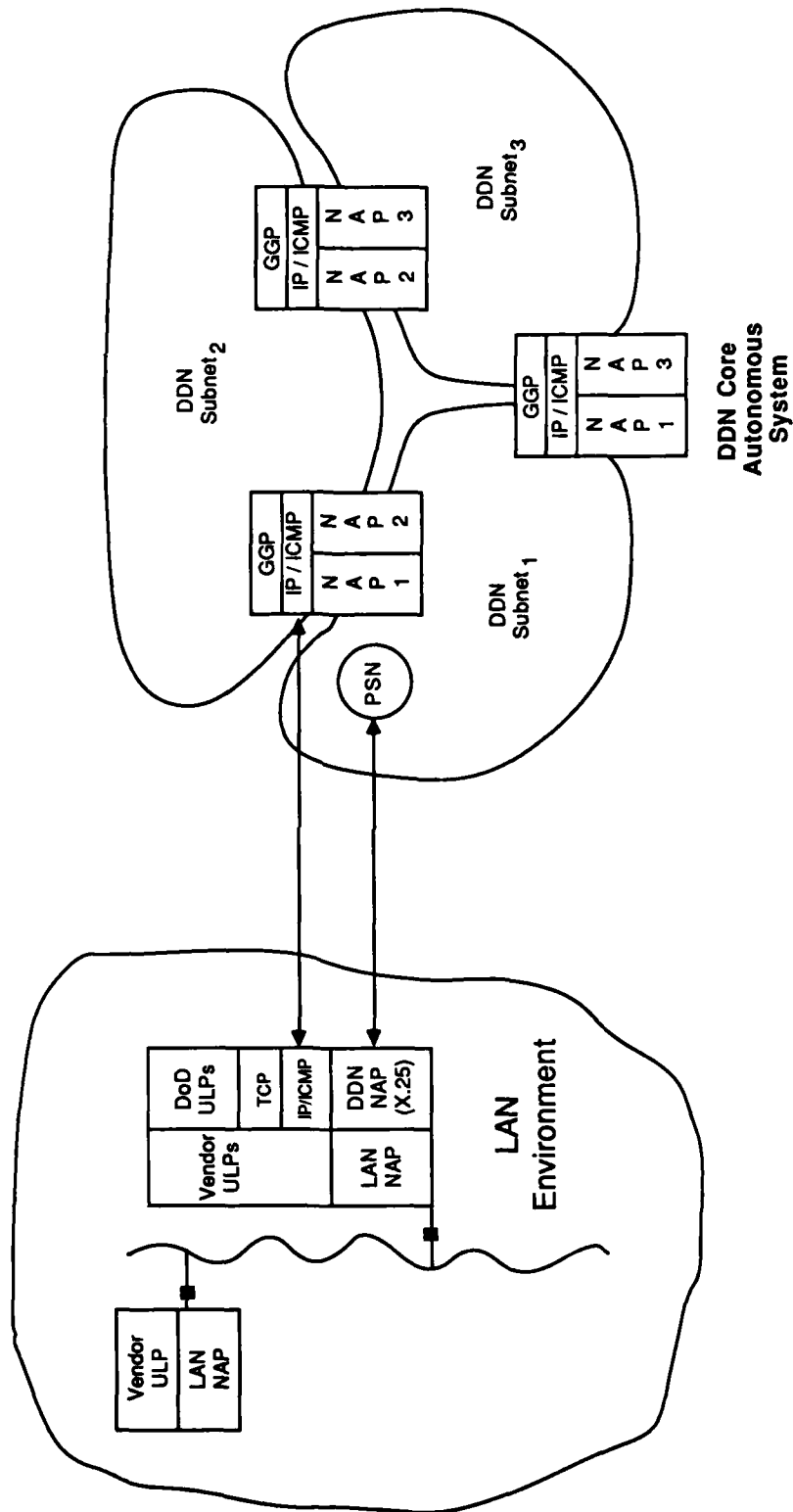
c) Advantages

- Simple to implement — little, if any, custom development
- "Gateway" is available today from multiple vendors, usually called a LAN communications server.
- No impact on current LAN applications

d) Disadvantages

- No interoperability with DDN hosts since upper layer protocols will be vendor-specific.
- No internetworking capability since there is no internetwork protocol such as IP.
- No end-to-end connection protocol unless supplied as a vendor-specific transport layer protocol.

TCP/IP HOST EMULATING "GATEWAY"



3) TCP/IP Host Emulation "Gateway"

a) Gateway Protocol

There is no gateway protocol since the "gateway" is simply a TCP/IP host on the DDN and a device on the LAN.

b) Description of Operation

- "Gateway" operates as a Network Access Protocol (NAP) and Upper Level Protocol (ULP) translating device
- The "gateway" looks like a TCP/IP host to the DDN
- The "gateway" looks like a LAN device to all other devices on the LAN
- User information is passed from a LAN device to the "gateway" which converts both upper layer protocols and network access protocols to the DoD equivalents
- Could require two logons for terminals accessing LAN hosts

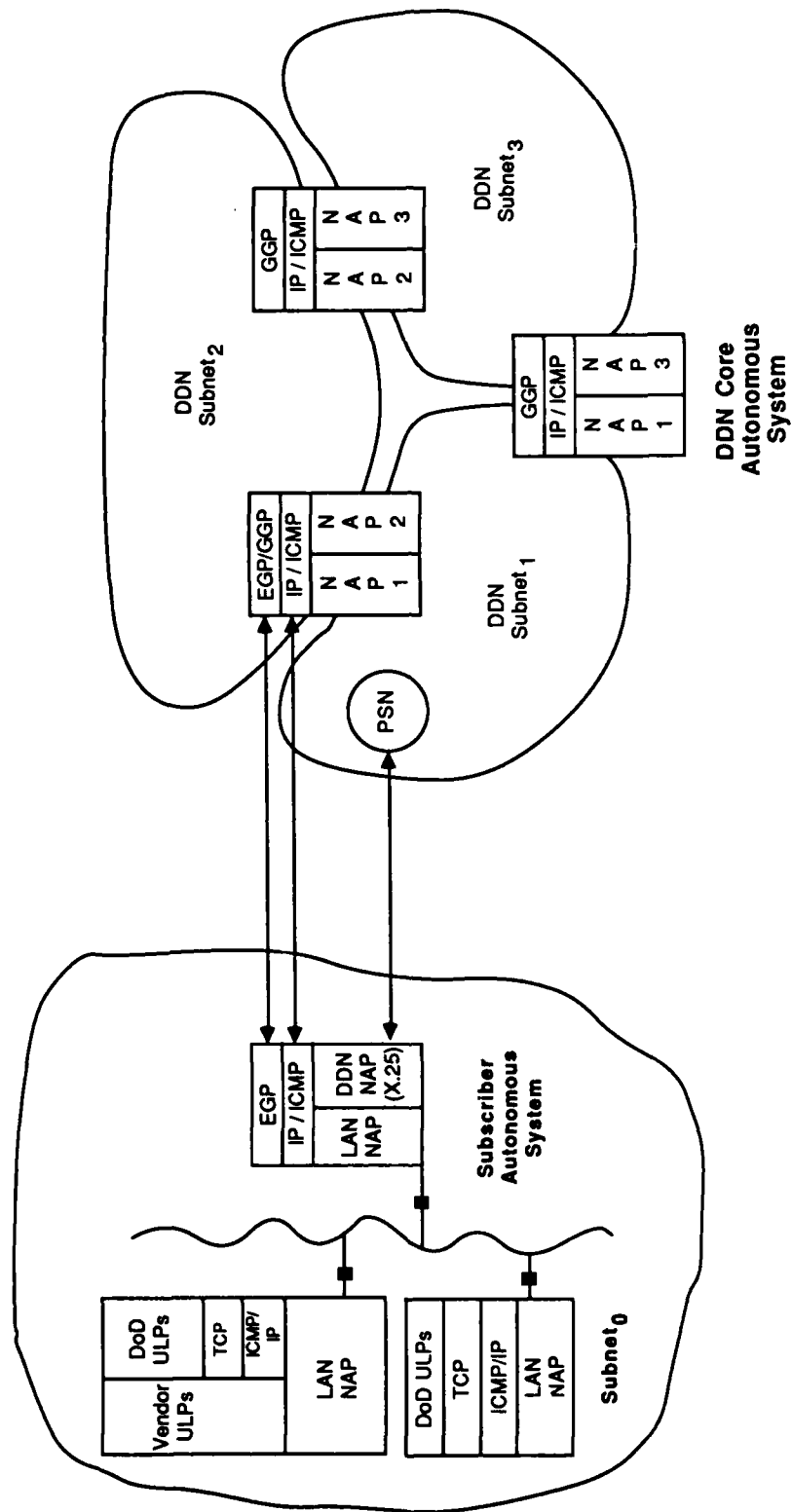
c) Advantages

- No impact on current LAN applications
- Provides an error-free TCP connection from the "gateway" to the DDN destination.
- Provides reachability to any user within the DoD internet.
- Provides interoperability between DDN hosts and terminals and the devices on the LAN because of the upper layer protocol translation in the gateway

d) Disadvantages

- Very few of these gateways exist as commercial products
- May be difficult to map all upper layer protocols from the DoD protocol suite into vendor-specific protocols without loss of some information (eg., forms-mode screen formatting)

DOD INTERNET GATEWAY



4) DoD Internet Gateway

a) Gateway Protocol

The gateway protocol used would be the Exterior Gateway Protocol (EGP). This protocol allows gateways within the DoD to communicate with the LAN gateway to exchange reachability information.

b) Description of Operation

- Gateway operates as a Network Access Protocol (NAP) translating device and as an external gateway to the DoD internet
- No upper level protocol translation takes place because all LAN hosts implement the DoD protocol suite
- The gateway is transparent to users and each device on the LAN is reachable from the DDN by its internet address
- The gateway looks like a LAN host and IP gateway to all other devices on the LAN
- Single logon required for interactive terminal access to LAN hosts

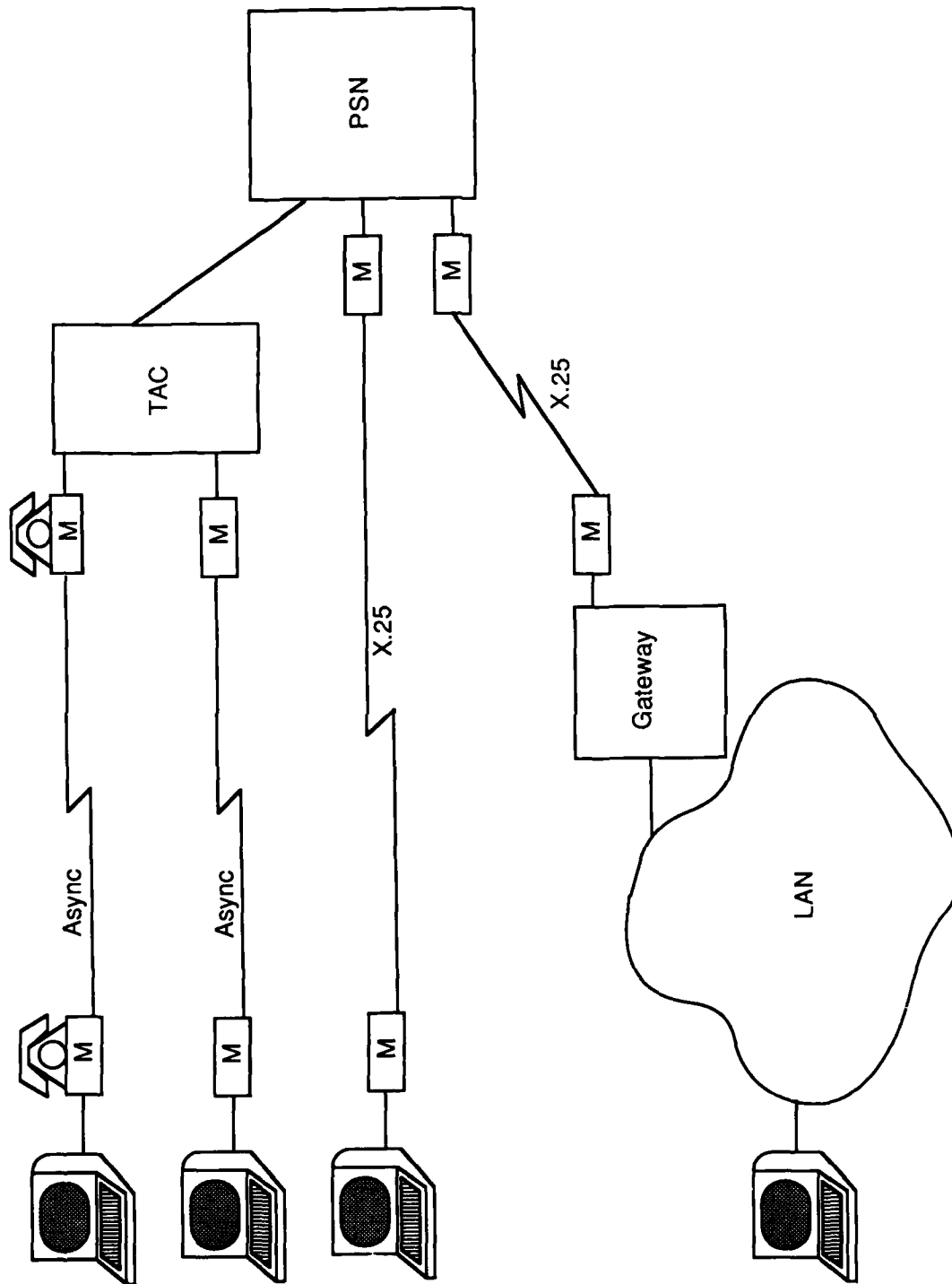
c) Advantages

- Provides error-free TCP connections, on a truly end-to-end basis, from LAN hosts to the DDN destinations.
- Provides reachability to any destination within the DoD Internet.
- Provides interoperability between DDN hosts and terminals and the devices on the LAN.

d) Disadvantages

- These gateways do not exist as commercial products yet.
- All LAN devices must support the DoD Internet protocol suite.

PC CONNECTION TO THE DDN



C. Personal Computers on the DDN

1) Methods of Connecting PCs to the DDN

a) Run asynchronous terminal emulation software and connect to a TAC

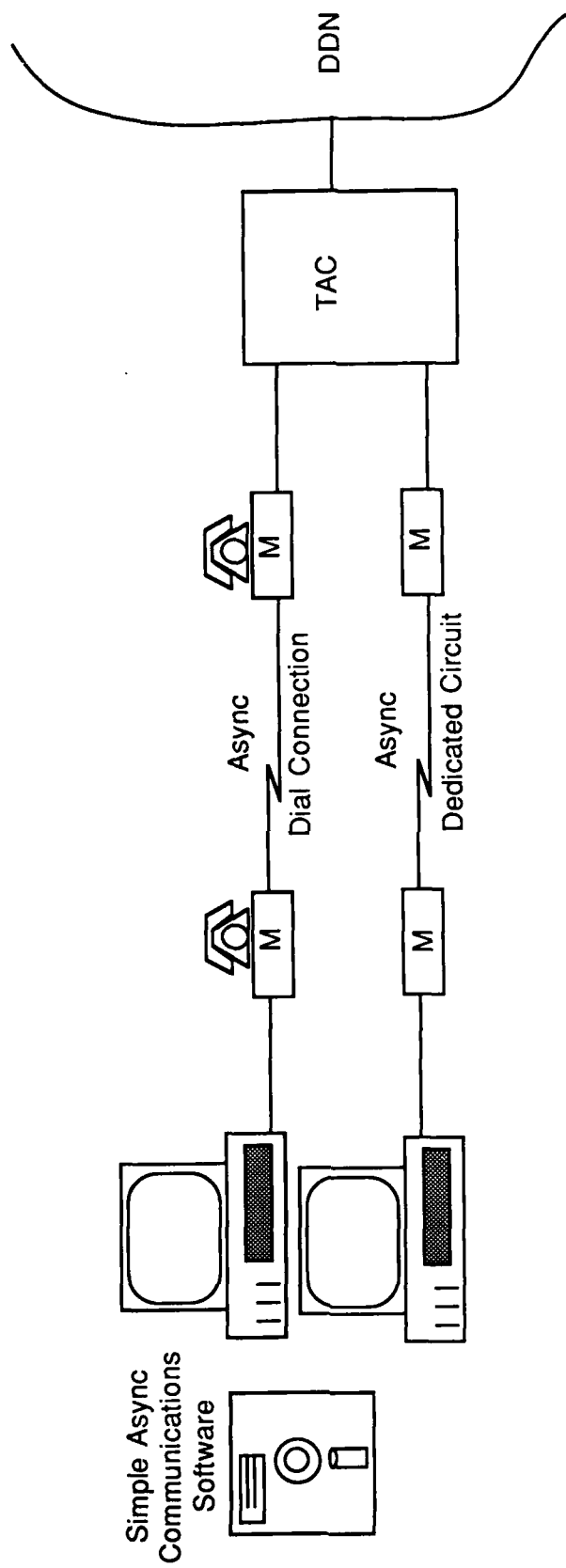
- Dedicated Line
- Dial-up Line

b) Connect the PC to a PSN as a Host Computer

- X.25-Basic Access to a DDN PSN

c) LAN Gateway

PCs CONNECTED AS ASYNC TERMINALS



2) Connecting PCs as Asynchronous Terminals

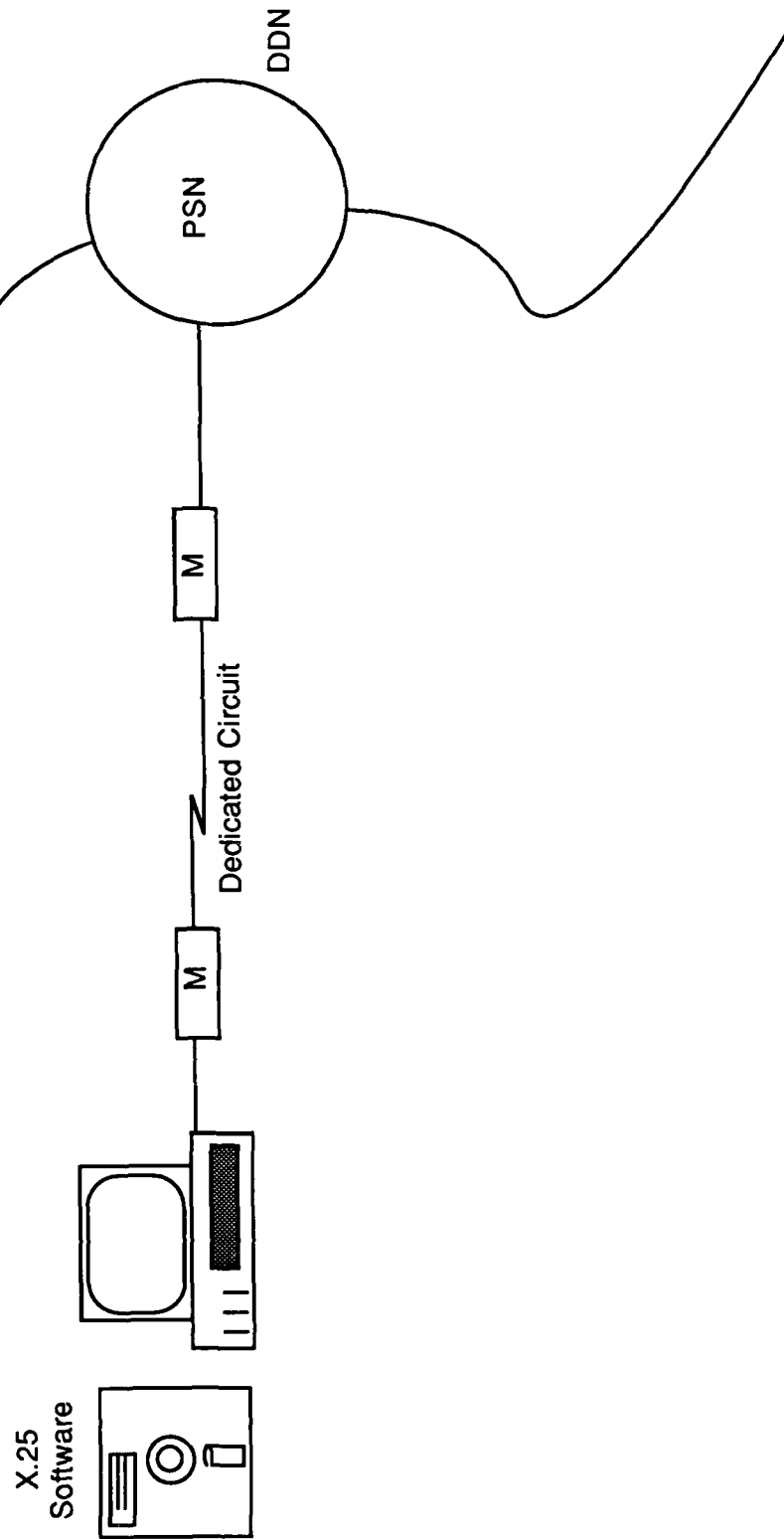
a) Requirements

- The personal computer must be able to emulate a simple asynchronous terminal (through use of communications software).
- The personal computer can be connected to a modem that can dial into a DDN TAC or the PC can be connected via a dedicated line to a TAC.

b) Implications

- The dial-up line can support up to 1200 bps, whereas the dedicated line can support up to 9600 bps of asynchronous traffic.
- Can connect to any DDN host and application program that supports Telnet.
- An asynchronous terminal cannot initiate a file transfer using FTP from a host to itself or vice-versa.

PC CONNECTED AS AN X.25 HOST



3) Connecting PCs as X.25-Basic Host Computers

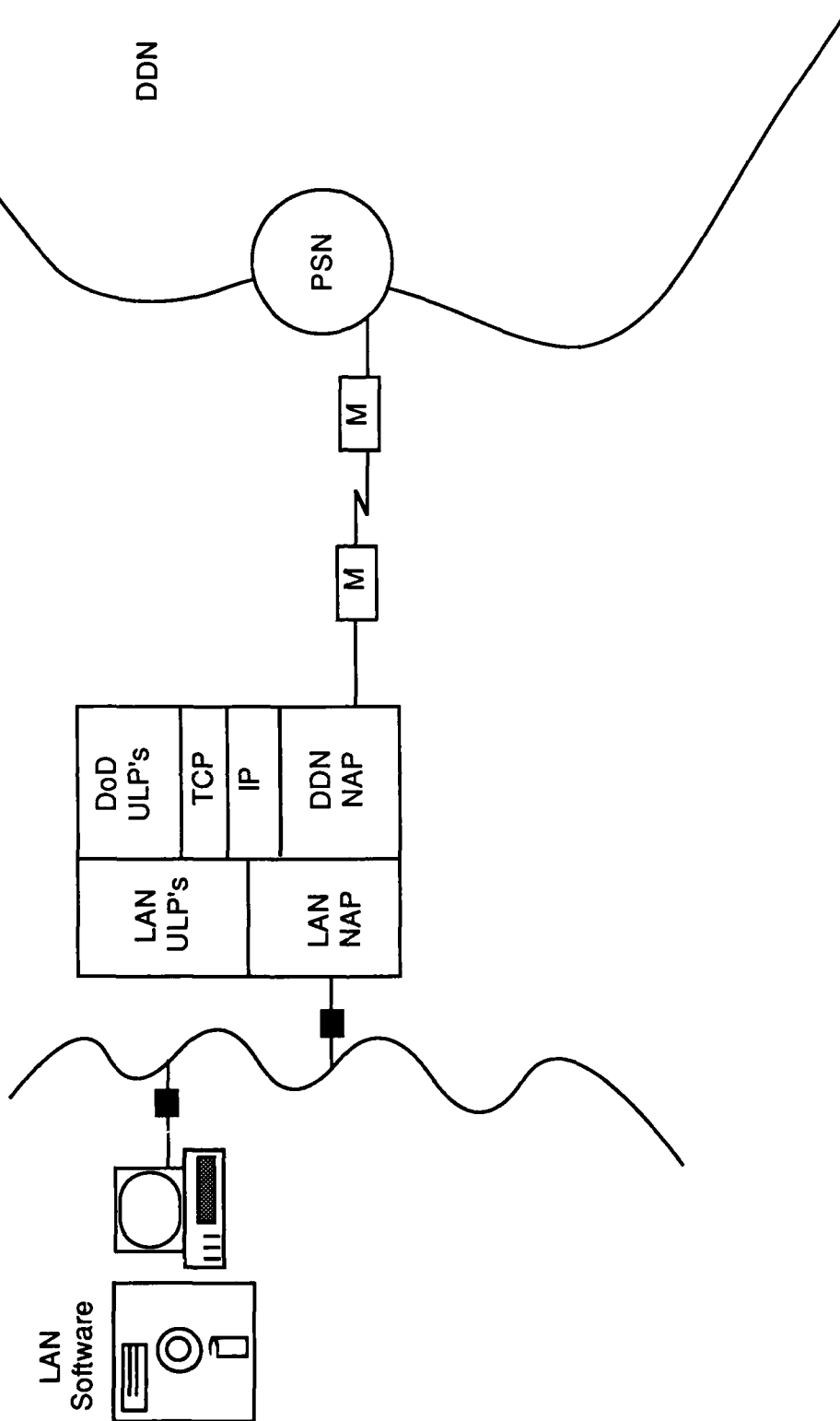
a) Requirements

- The PC must support at least Basic X.25 for service over the DDN.
- The PC must be able to support a dedicated line to the DDN PSN.

b) Implications

- Since PCs are generally single tasking machines with limited memory, they may not be able to run the X.25 and other application software (e.g., spread sheet, word processing, etc.) concurrently. This will severely limit the usefulness of a host connection to the DDN.
- PCs connected as X.25-basic hosts will not be able to perform the FTP file transfer functions.
- With a simple X.25 interface, the PC will only be able to access remote hosts that also use X.25-only access. The PC must be able to use the vendor-specific interfaces above X.25.
- PCs connected as hosts will necessarily divert large amounts of network resources by occupying host ports on the DDN PSNs. Although DCA does not encourage such PC host connections, extenuating circumstances will be reviewed on a case by case basis.

PCs CONNECTED THROUGH A LAN



4) Connecting PCs to the DDN Through Local Area Network "Gateways"

- Promising method of connecting PCs to the DDN since DDN connection maintenance will not monopolize PC processing resources.
- Many PCs may use the same DDN connection and thus PSN ports may not be vastly under utilized.
- May not require the LAN or PC applications software be changed (if all protocols are implemented in the "gateway" host)
- The "gateway" host will maintain the DoD connection
- The "gateway" host can be connected to the DDN on a full time basis and thus can act as a mail server or file server for all PCs connected to the LAN.
- The PCs can use the LAN protocols and applications for file transfer.

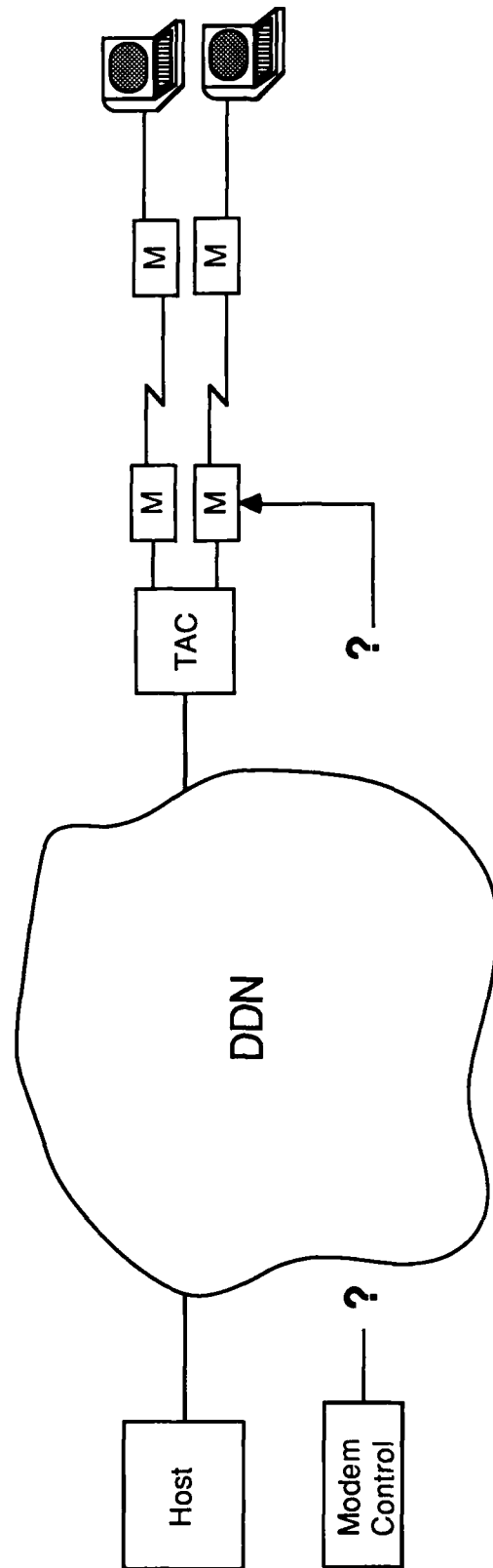
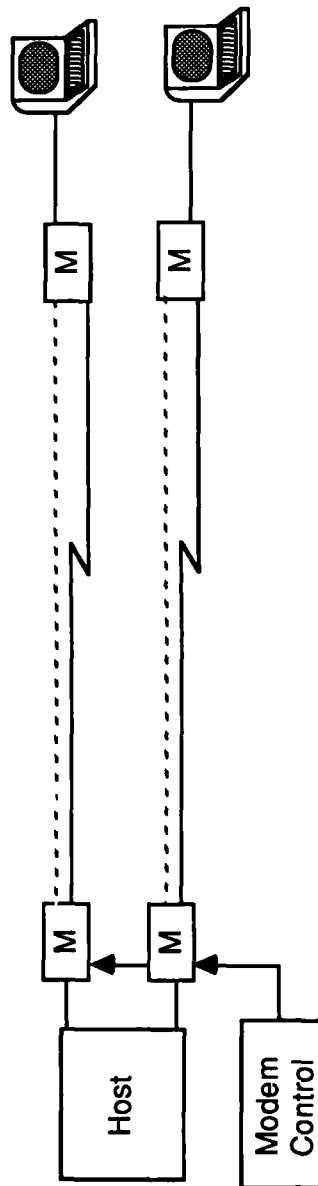
a) Requirements

- The LAN gateway must support at least X.25 protocol to access the DDN and may support the full DoD protocol suite.
- If upper layer protocols are supported in the gateway, then it must be able to convert them to the upper layer protocols used by the LAN and PCs.

b) Implications

- The gateway will look like a TCP/IP (or X.25 basic) host to other hosts and terminals on the DDN.
- The LAN software and PCs may be unaffected by the inclusion of a DDN gateway.
- The gateway can act as a mail server and file transfer device for all PCs on the LAN.

MODEM DIAGNOSTICS PROBLEM

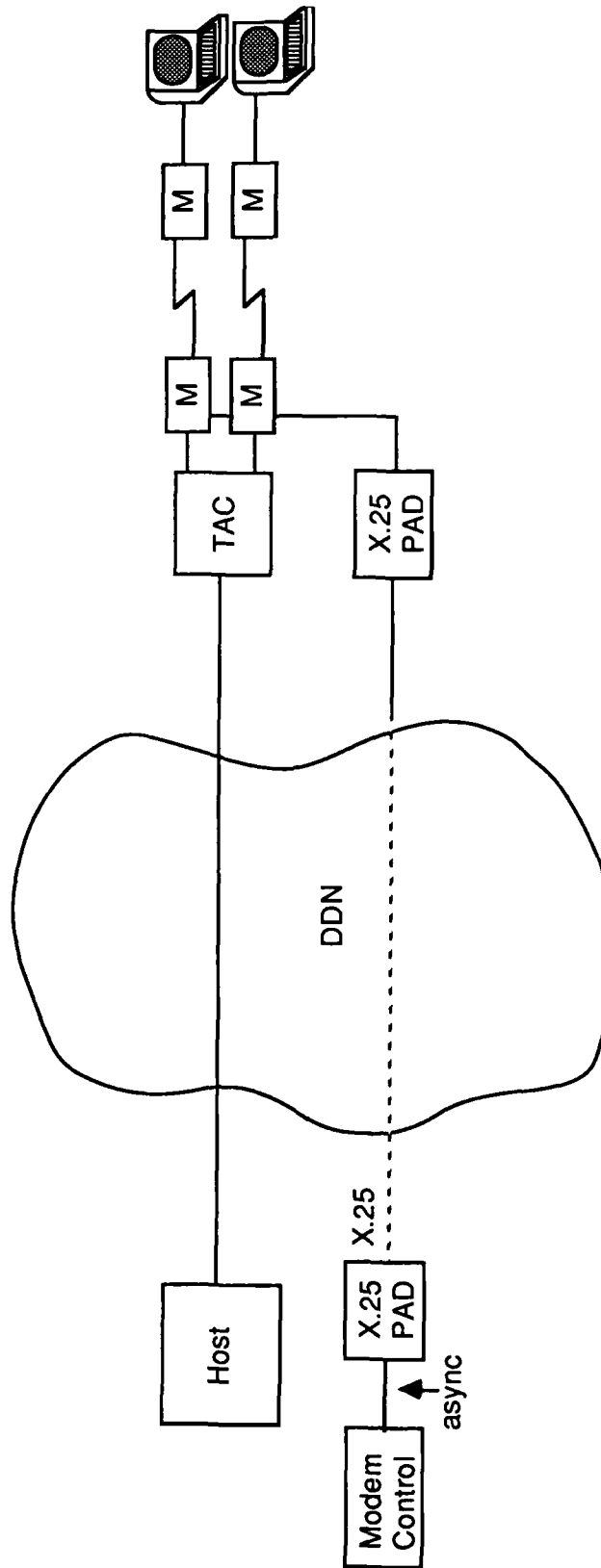


D. Subscriber Network Monitoring Systems on the DDN

1) Problem

- a) The maintenance of circuits not obtained through DCSDS is the responsibility of the subscriber.
- b) The DDN does not presently support a method for aggregating modem diagnostic information and passing it through the network to the subscriber's control location.

MODEM DIAGNOSTIC SOLUTIONS



2) Solution

The use of X.25 PADs to aggregate modem diagnostics at a remote location and at the modem control location. This method has been implemented on commercial networks but not on the DDN.

QUALIFICATION TESTING

- **Subscriber interfaces to the DDN
must be qualified**
- **Qualification testing performed by
DCSDS**
- **Individual vendors are responsible
for getting their DDN interfaces
qualified**

11. ADMINISTRATIVE ISSUES FOR DDN SUBSCRIBERS

A. QUALIFICATION TESTING

There are two aspects of qualification testing. The first is vendor qualification of X.25 and TCP/IP. The second is the subscriber system testing with the integration of the DoD protocols.

1) Protocol Testing

a) 1822

- As of April 1, 1986, new 1822 procurements must be qualified

b) Basic X.25

- X.25 is qualified up to level 3
- Vendor gets floppy disk containing test from DCSDS
- Vendor performs the test and sends an error file to DCSDS
- Formal test is scheduled
- DCSDS performs testing and analysis of the results

c) Standard X.25

- Qualifies X.25 up to level 3
- Checks two facility codes to see that X.25 can handle IP and TCP
- Full compliance with Federal Standard 1041 is required

d) TCP/IP

- Test scenarios are being developed by DCSDS.
- Test facilities will be available at the Defense Communications Engineering Center (DCEC)

2) System Testing

- Test system operation to ensure that any software modifications do not adversely affect functioning

HOST ADMINISTRATOR RESPONSIBILITIES

- Ensures network policies and procedures are observed
- Manages access control procedures & password system
- Coordinates with DCSDS changes to host system that may affect DDN
- Point of contact for escalating network related problems to MC

B. HOST SITE RESPONSIBILITIES

1) Host Administrator

- a) Should be assigned as soon as a firm Required Operational Date (ROD) has been established
- b) Performs the following duties:
 - Ensures that network policies and procedures are observed by the users. Administers TAC access control system (TACACS), which validates that all users have been authorized for DDN and TAC access, and are registered in the NIC User Registration database (WHOIS/NICNAME).
 - Manages the network access control procedures and password system, and is responsible for reporting network-related host break-ins and assisting with investigative effort as needed.
 - Coordinates with DCSDS installation of hosts or changes to, host software that has direct or indirect impact on the DDN. Provides DCA and NIC with required descriptive information for each new host addition or host change. Coordinates the host certification procedure with DCA prior to passing traffic on the network.
 - Responsible for proper implementation and maintenance of DDN protocols at the host level.
 - Serves as local point of contact for hosts and local users and coordinates suspected network-related problems directly with the network Monitoring Center (MC) .

2) Host Technical Liaison

- Provides technical assistance to DCSDS regarding the host
- Acts as troubleshooter/debugger for host

NODE SITE ADMINISTRATIVE RESPONSIBILITIES

- Primary point of contact for node site
- Liaison for the installation of node hardware, software, and circuits
- Coordinates/authorizes node site access

C. NODE SITE RESPONSIBILITIES

In some instances, a DDN packet switching node will be placed at a subscriber's location.

1) DDN Node Site Coordinator

The node site coordinator interfaces with the DDN MC, DCA, and the subscribers while managing the node site.

a) Responsibilities

- Interacts with DDN personnel and the MC
- Primary point of contact
- Authorizes and ensures personnel access to the DDN node
- Liaison for the installation of node hardware, software, and circuit

b) Functions

- Ensures the node site always has a primary point of contact
- Provides site coordination and authorizes personnel site access for installation, removal, and modifications to DDN hardware
- Provides local site assistance to the MC when corrective actions are required during hardware or circuit degradation or outages
- Ensures that DDN hardware, software, or circuits are not altered, moved, or tampered with

DDN NODE SITE SURVEY

- Survey of DDN node site by all participants
- Equipment installation & acceptance
- DCA Letter of Intent (LOI)
- Site engineering and documentation
- DCA site survey report and concurrence

2) DDN Node Site Survey

- Survey proposed node location
- Establish tasks/responsibilities
- Identify issues and who will respond to them
- Letter of Intent (LOI) will identify tasks and points of responsibility

3) Representatives Participating in the DDN Site Survey

a) Site Representatives

- local on-base communications personnel
- physical plant (Facilities Engineers) personnel
- on base security personnel
- site commander or local authority to sign the letter of intent
- node site coordinator

b) Service Representatives

- Service DDN Program Office (COMNAVTELCOM, ASPO, Ft. Monmouth)
- Engineering and Installation personnel, if necessary

c) DCA Representatives

- B642 - Installation Management Branch
- Network Strategies, Incorporated
 - Under contract to DCA to provide installation management assistance to DCA B642
- Primary engineer who will make red line drawings and draw up a bill of materials needed to install a node at the site
- BBN field service personnel who will be installing the node.

GENERAL NODE SCHEDULE & RESPONSIBILITIES

<u>ACTION</u>	<u>RESPONSIBILITY</u>	<u>TIMEFRAME</u>
Network Design	DCA	30 Months
Request for Sites	DCA	24 Months
Presurvey/Nomination	SERVICE	20 Months
Order Site Hardware Interswitch Trunks	DCA	18 Months
Site Survey	DCA/SITE	19 Month OCONUS 13 Months CONUS
Agreement/Tasking	DCA/SERVICE	18 Months OCONUS 12 Months CONUS
Complete Site Preparation	SERVICE	01 Month
Ship Node Hardware	DCA	01 Month
Complete Interswitch Trunk(s)	DCA	03 Weeks
Install Hardware/Software	DCA/SERVICE	02 Weeks
Test & Acceptance of Equipment	SERVICE	01 Week
Test & Acceptance of Node & Circuit Performance	DCA	01 Week
Initial Operating Capability	DCA	TARGET

3) DCA Provides Initial Connectivity to the DDN

- A minimum of 2 50Kbps or 56Kbps trunk circuits

4) Equipment Installation and Acceptance

a) Installation performed by DCA

b) Acceptance procedures

- Site personnel will test all power lines to the DDN equipment
- Site or service personnel will certify that node installation was performed in accordance with prescribed standards
- DCA will perform functional performance of node and communication services (circuit can pass traffic)

5) DCA Letter of Intent (LOI) Contents

- a) Specification of equipment location, placement and access
- b) Site preparation considerations for the DDN node
 - Space considerations and environmental requirements
 - Node power requirements
 - 3 20 amp dedicated power circuits
 - 2 L5-20R receptacles for communications and processor cabinets
 - Communications signal cables
 - 200 pair voice frequency signal cables for off base access (MILNET)
 - 100 pair voice frequency signal cables (DISNET)
 - Class 'A' telephone (with AUTOVON if available)
 - COMSEC requirements
 - Testing and acceptance requirements

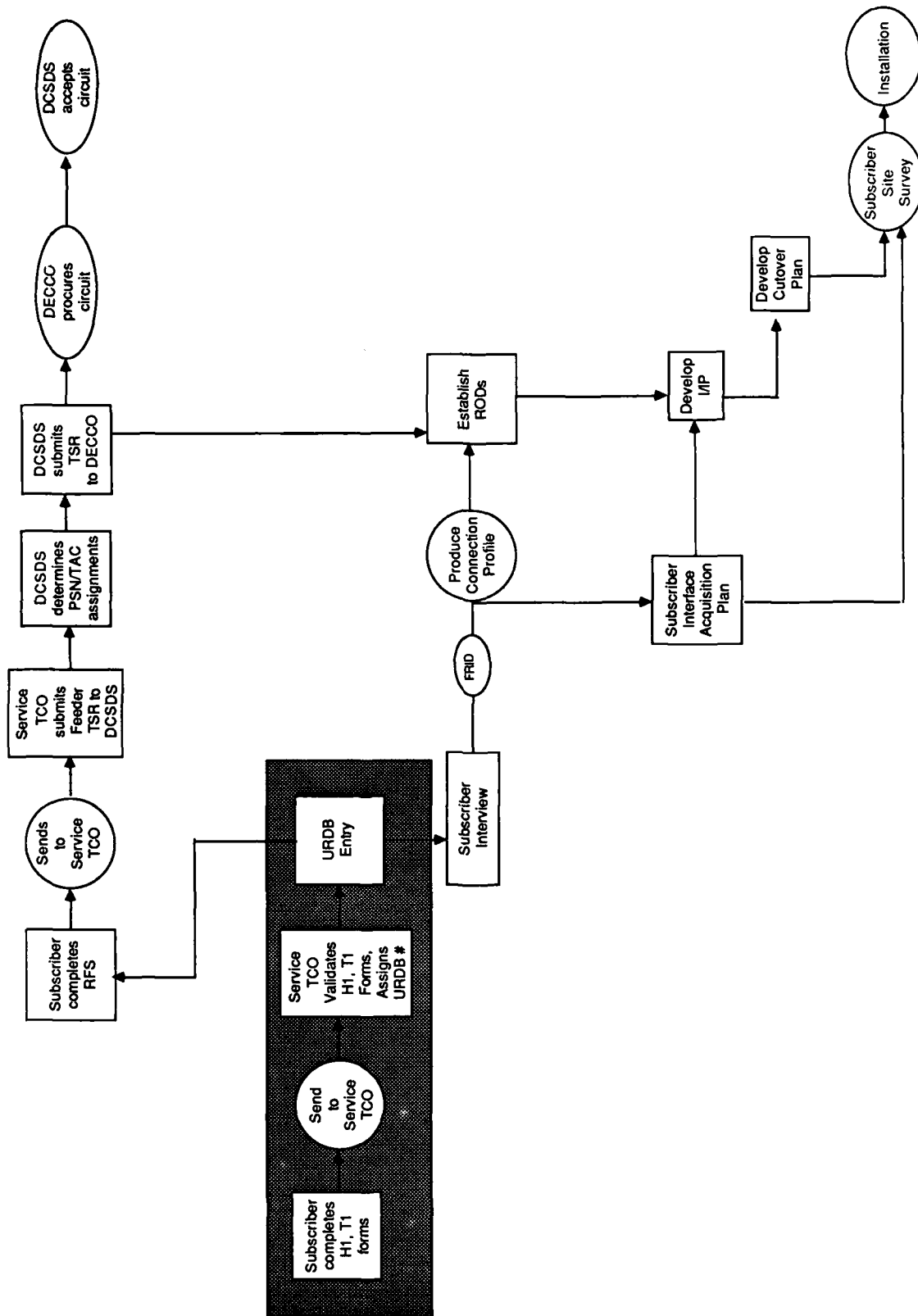
6) Site Engineering and Documentation

- a) Red line drawings done at initial site survey
- b) DDN provided connectivity documentation

7) Site survey Report

Formalizing of the LOI issued by DCA for concurrence by services

ORDERING DDN SERVICE



D. Ordering DDN Service

Defense Communications System Data Systems (DCSDS) requires accurate and complete system information to properly plan and implement the DDN. Therefore, all potential subscribers that need to order service must follow specified administrative procedures to supply DCSDS with the necessary information.

1) Requirements Analysis

a) User Requirements Data Base (URDB)

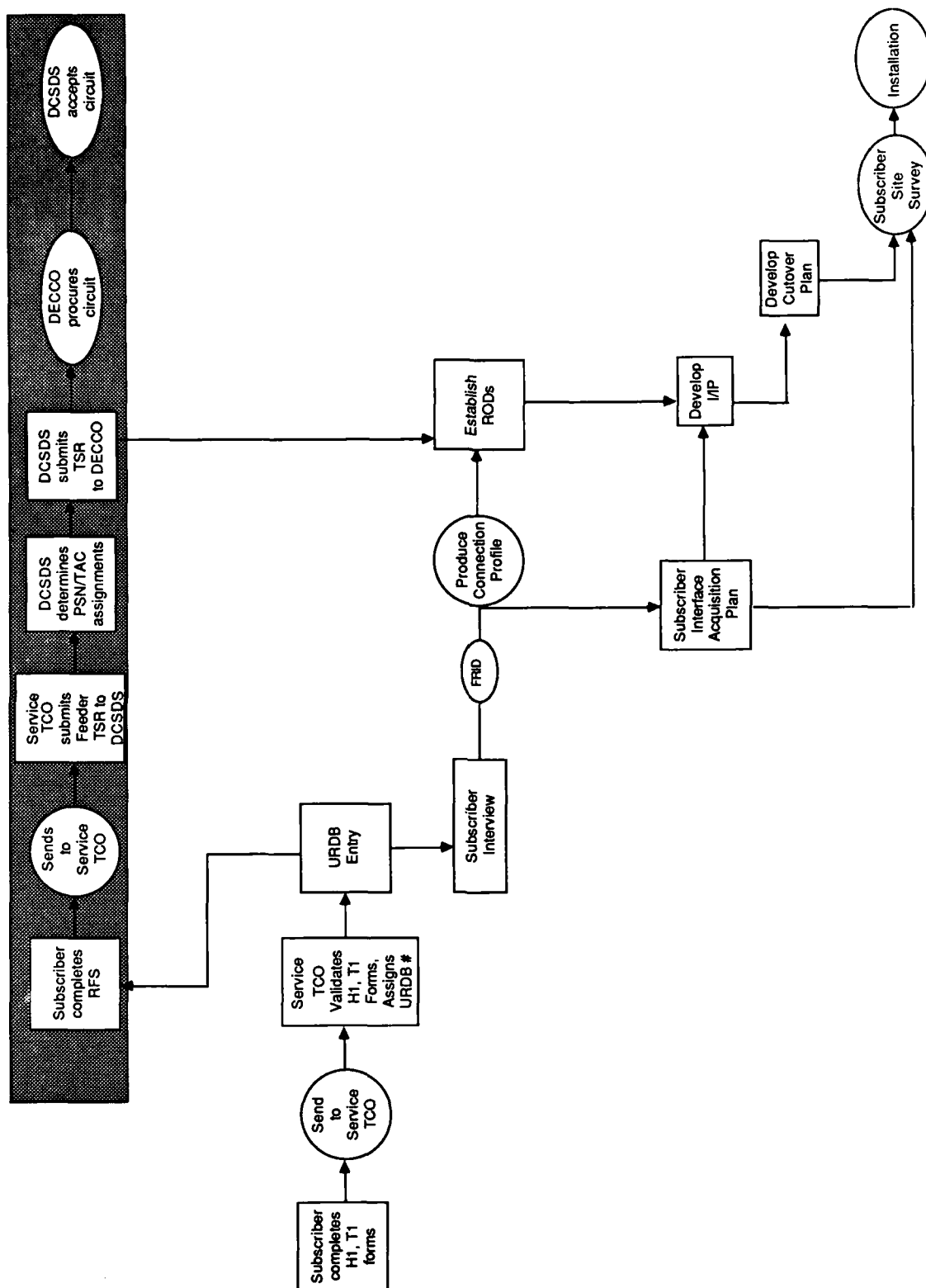
The URDB identifies all requirements of the subscriber hosts and dedicated terminals for connection to the DDN. The URDB also provides input for network modeling and serves as an initial DDN planning tool. DCSDS provides to the Telecommunications Certifications Office (TCO), URDB Questionnaires — Host (H1) and Terminal (T1) forms — to gather data for the URDB.

- Subscriber submits H1 and T1 forms to the Service/Agency (S/A) Telecommunications Certification Office.
- S/A TCO validates H1 and T1 forms, assigns URDB number and forwards forms to DCSDS.
- S/A TCO or DCSDS enters data from H1 and T1 forms into URDB.
- DCSDS is responsible for the URDB.

H-1 QUESTIONNAIRE FORM		DATE
TYPE SUBMISSION INITIAL _____ CHANGE _____	1. HOST SYSTEM IDENTIFIER _____/_____/____	
2. POINT OF CONTACT _____		POC PHONE NUMBER _____
3. GEOGRAPHIC LOCATION UNIT OR AGENCY _____ ADDRESS _____ CITY _____ STATE/COUNTRY _____ ZIP _____ APO OR FOREIGN ADDRESS _____		4. SITE AUTOVON PHONE NUMBER _____ SITE COMMERCIAL PHONE NUMBER _____
5. SECURITY/COMPARTMENT MODE OF OPERATION ____ UNCLAS ____ CONF ____ SECRET ____ TS-GENSER ____ TS-SIOP ____ TS-SCI		6. WAIVER NUMBER _____
7. DATE PROJECTED FOR SERVICE REQUESTED DATE (M/Y) ____/____/____ DATE ON DDN ____/____/____		
8. HOST COMPUTER MANUFACTURER _____ MODEL NUMBER _____ OPERATING SYSTEM _____ TERMINAL PASS-THROUGH REQUIRED? YES ____ NO ____ NUMBER OF DIAL PORTS _____ IS HOST A PC? YES ____ NO ____		
9. FRONT END PROCESSOR/TRANSMISSION CONTROL UNIT MANUFACTURER _____ MODEL NUMBER _____ OPERATING SYSTEM _____		
10. PRINCIPAL SYSTEM (S) ACCESSED SYSTEM ACRONYM _____ TYPE ACCESS ____ INTERACTIVE ____ QUERY/RESPONSE ____ BATCH/BULK ____ ELECTRONIC MAIL SYSTEM LEVEL SECURITY ____ UNCLAS ____ CONF ____ SECRET ____ TS-GENSER ____ TS-SIOP ____ TS-SCI ACCESSIBLE ON DDN ____ YES ____ NO		
11. HOST TO HOST COMMUNICATION LINK(S) DESTINATION HOST SYSTEM IDENTIFIER ____/____/____ LINESPEED (BPS) _____		
12. TELECOMMUNICATIONS SYSTEMS SOFTWARE NAME _____		

T-1 QUESTIONNAIRE FORM		DATE
TYPE SUBMISSION INITIAL _____ CHANGE _____		1. TERMINAL IDENTIFIER _____/_____/_____/_____
2. POINT OF CONTACT _____		4. POC PHONE NUMBER _____
3. GEOGRAPHIC LOCATION UNIT OR AGENCY _____ ADDRESS _____ CITY _____ STATE/COUNTRY _____ ZIP _____ APO/FOREIGN ADDRESS _____ _____		SITE AUTOVON PHONE NUMBER _____ SITE COMMERCIAL PHONE NUMBER _____ _____
5. SECURITY/COMPARTMENTATION MODE OF OPERATION ___ UNCLAS ___ CONF ___ SECRET ___ TS-GENSER ___ TS-SIOP ___ TS-SCI		6. WAIVER NUMBER _____
7. DATE PROJECTED FOR DDN SERVICE REQUESTED DATE (M/Y) ___/___/___ DATE ON DDN ___/___/___		
8. MANUFACTURER _____		
9. MODEL _____		
10. DATA LINE PROTOCOL ___ CHARACTER ASYNCHRONOUS ___ START/STOP ___ BSC (BINARY SYNCHRONOUS COMMUNICATIONS) ___ VIP ___ DDCMP ___ SNA/SDLC ___ OTHER _____ ___ HASP ___ BLOCK-MODE ASYNCHRONOUS		
11. CODE SET ___ ASCII ___ EBCDIC ___ BCD ___ BAUDOT ___ OTHER _____ ___ CORRESPONDENCE ___ SIX-BIT TRANSCODE		
12. TRANSMISSION SPEED (BPS) ___ 100 ___ 110 ___ 134.5 ___ 150 ___ 300 ___ 600 ___ 1200 ___ 1800 ___ 2400 ___ 4800 ___ 7200 ___ 9600 ___ 19.2 ___ OTHER (SPECIFY) _____		
13. PRINCIPAL SYSTEM(S) SYSTEM ACRONYM _____ TYPE ACCESS ___ INTERACTIVE ___ QUERY/RESPONSE ___ BATCH/BULK ___ ELECTRONIC MAIL SYSTEM SECURITY LEVEL ___ UNCLAS ___ CONF ___ SECRET ___ TS-GENSER ___ TS-SIOP ___ TS-SCI ACCESSIBLE ON DDN ___ YES ___ NO DESTINATION HOST ID ____/____/_____		

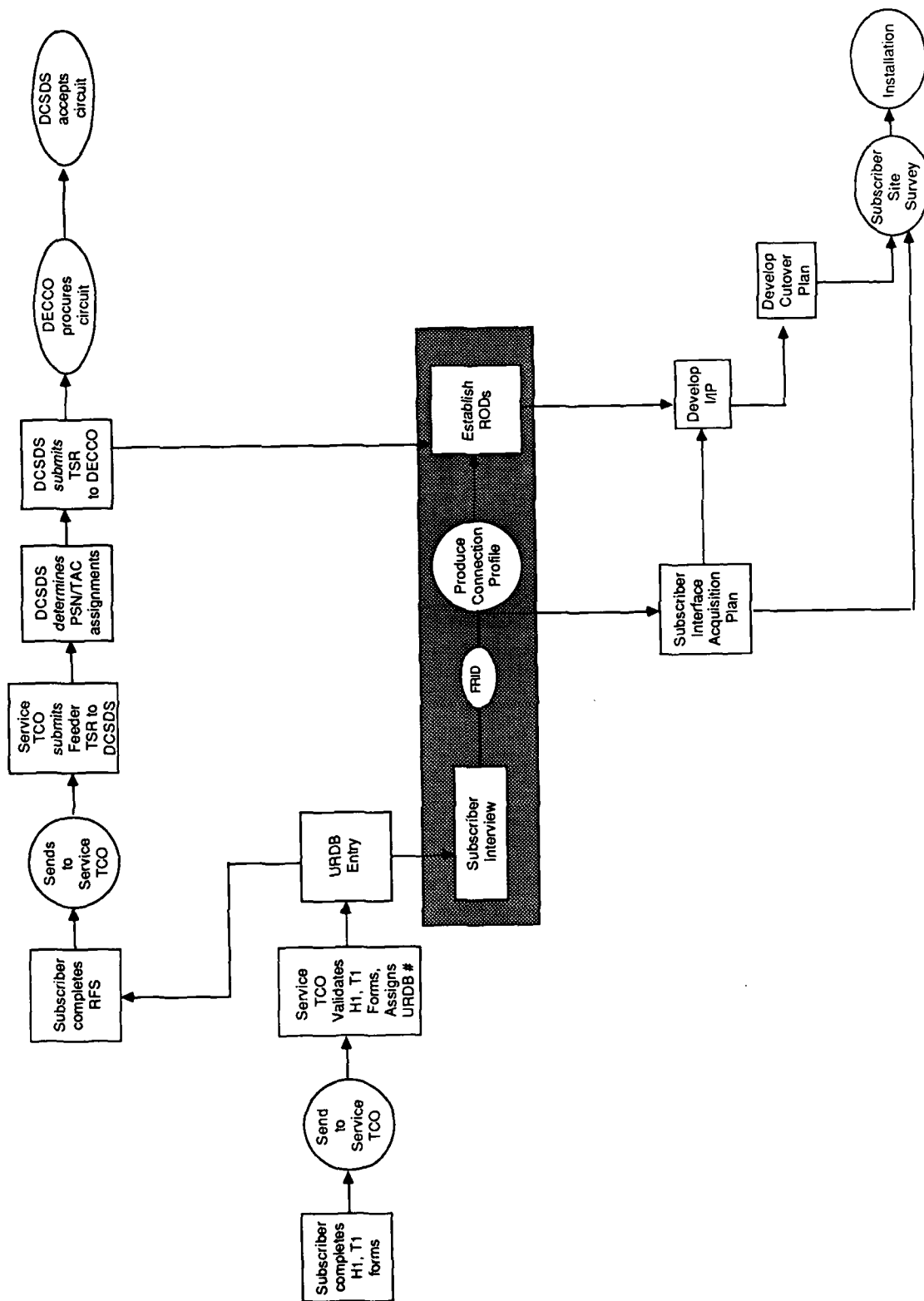
ORDERING DDN SERVICE



b) Request For Service (RFS)

- Subscriber will send RFS to the TCO.
- TCO will validate RFS and submit a Feeder Telecommunications Service Request (TSR) to DCSDS.
- DCSDS will submit TSR for DECCO to request circuits and modems.
- DCSDS determines PSN/TAC port assignments.
- DECCO issues Telecommunications Service Order (TSO) to solicit bids from the TELCOs to acquire required circuits and modems.

ORDERING DDN SERVICE



2) System Implementation

a) Subscriber Interviews

TCO and/or DCSDS selectively visit(s) or telephone(s) subscriber to collect additional data and discuss unique system configurations.

b) Functional Requirements and Interface Document (FRID)

DCSDS will produce a FRID if the system is expected to have significant network resource requirements. The FRID identifies the subscriber's current and future communications requirements. The FRID also describes subscriber interface alternatives and advantages and disadvantages of each alternative. DCSDS will include its acquisition recommendation with the document.

c) Connection Profile

DCA produces the Connection Profile based on information gathered from the subscriber interview, and FRID document. A Connection Profile is a compilation of the minimum set of data needed by DCSDS to plan for and reserve the network resources necessary to meet a subscriber's specific connection requirement.

d) Establishment of Required Operation Date (ROD)

- DCSDS, in coordination with the subscriber, establishes RODs for connecting the subscriber's hosts and terminals to PSN and TAC ports.
- Establishment of RODs is based on three factors:
 - The dictates of the subscriber's operational mission
 - Anticipated date that the subscriber will be ready to use the connection
 - Estimated leadtimes for circuit acquisition and deployment of network resources
- Realistic RODs help ensure that the availability of the subscriber interface corresponds to the availability of the network connection.

EXAMPLE OF TRANSITION PLAN OUTLINE

System Description

**Purpose, hardware, O/S, data comm requirements, URDB#s,
RODs**

Reason for Waiver

**Transition Plan is submitted as an attachment to waiver
request**

Transition Plan Details

URDB registration

**Interfaces — Milestones which correlate to projected
expiration date**

Acquisition strategy

Funding

Qualification

Submission of RFSs

Minimum lead time of 9 - 12 months

Effect on Application Programs

Which programs will be modified

Who will make the modifications

Time frame required

List dedicated leased lines, monthly cost and traffic volume

Schedule if connecting more than one system

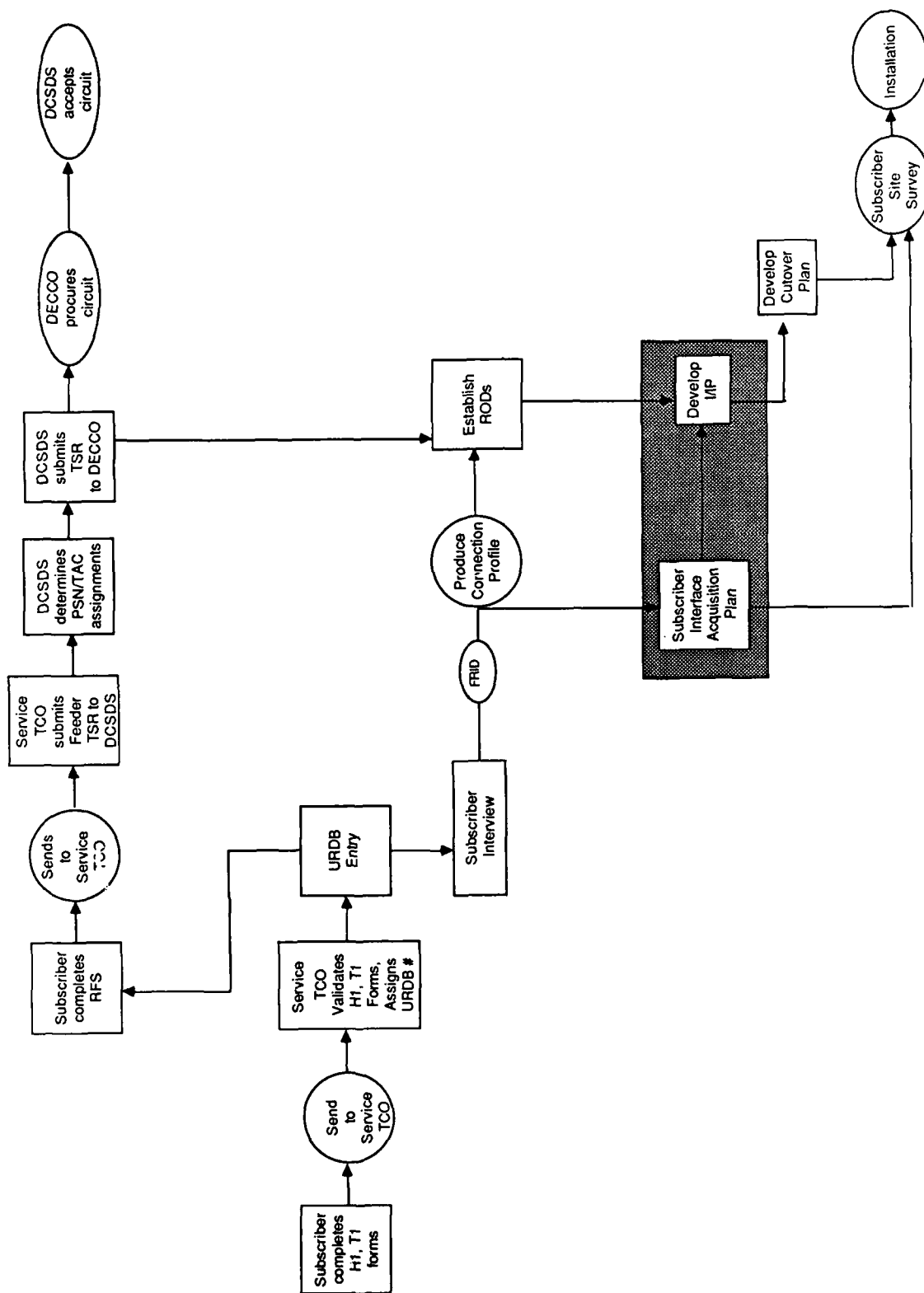
Date for completing DDN Cutover Plan

e) Waiver Procedures

If the subscriber and DCA jointly determine that the DDN cannot currently meet the subscriber's communications requirements, the subscriber may be granted a waiver.

- Waivers are generally not granted to subscribers with new systems.
- Waivers are generally temporary until capabilities are available to meet system requirements on the DDN.
- The following data processing requirements are exempted from the DoD policy on use of the DDN.
 - All exercise circuits
 - Temporary requirements with a life cycle of less than 12 months
 - Non-appropriated fund requirements
 - 150 BAUD and below circuits, except AUTODIN query response
 - AUTODIN narrative service requests including indirect AUTODIN circuits but excluding query response
 - Data requirements for a non-DoD host not connecting to the DDN, including NASA and Manned Space Agency
 - FEMA (exempted by DCA code B610 msg 231301Z SEP 83)
 - Intrafacility data communications whereby a facility is defined as a discrete entity such as a named post, camp, base or station or 20 miles or less point to point non long-haul circuits.
 - All circuit deactivations to include discontinuance of legs on existing multipoint circuits
 - Trunk actions (DCA channelized) that are in-house initiated actions and do not affect data service being provided
 - Trunk actions (DCA channelized) in response to certified TSRs
 - Defense Switched Network (DSN) including monitoring equipment access circuits
 - Data circuits that are used for Real-Time process control, e.g., full period telemetry, radar feeds

ORDERING DDN SERVICE



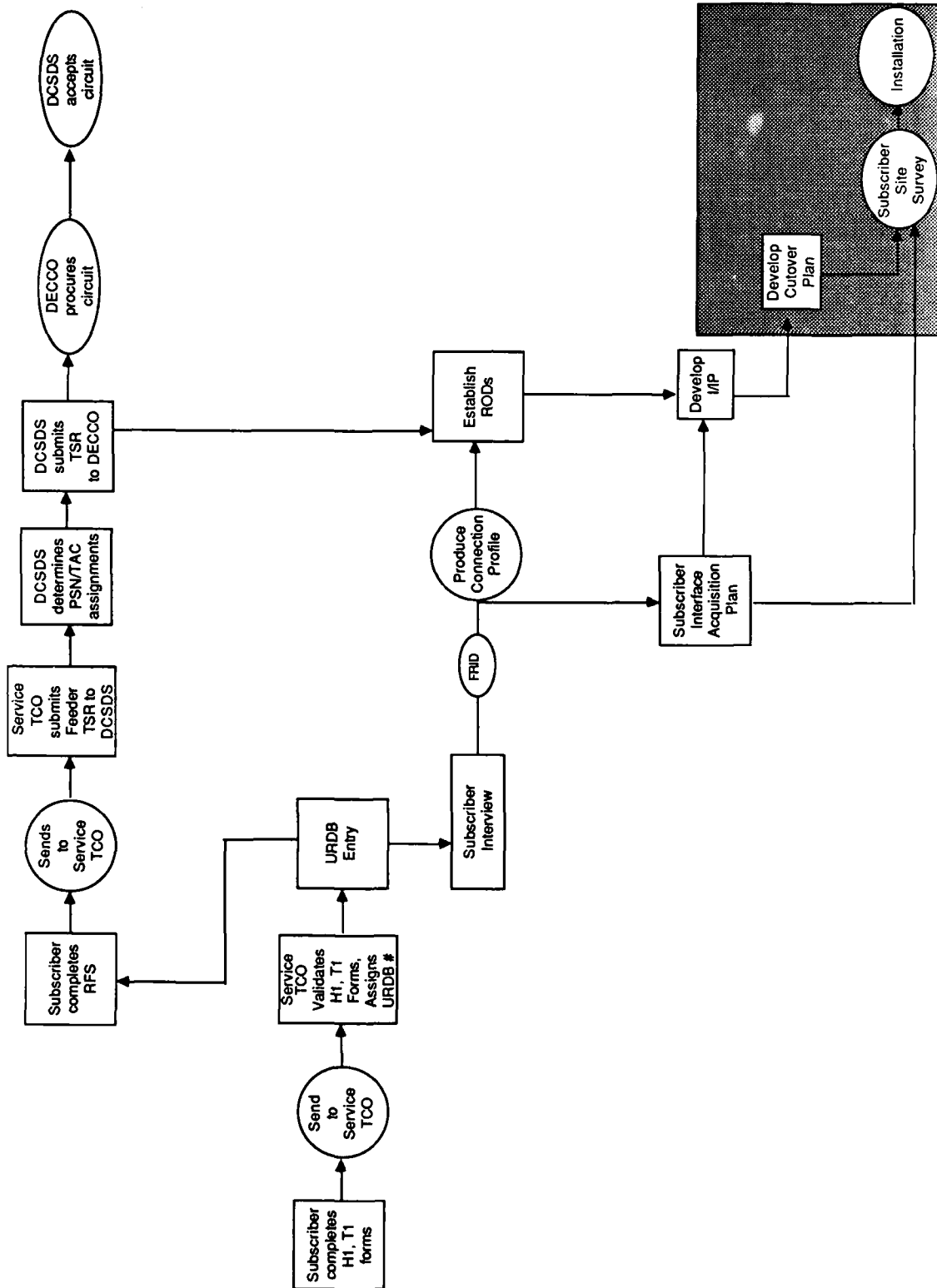
f) Acquisition of DDN Fully Qualified Interface

- Obtain a DDN fully qualified interface or provide a DDN fully qualified interface development strategy
- Identify a means of acquisition
- Procure fully qualified DDN interface

g) Subscriber Implementation/Installation Plan (I/IP)

- Subscriber to prepare I/IP which will serve as central planning tool and point of reference for all participants. Also used for tracking subscribers progress toward integration into the DDN.
- I/IP must address seven major topics. Plan must be structured according to specified outline, but in some cases not all of the sections may be applicable.

ORDERING DDN SERVICE



h) Cutover Plan

- Subscriber to develop cutover plan for each I/IP
- DDN Cutover Plan should address eight major topics. Additional topics may be included by the subscriber if desired.

i) Subscriber Site Survey

Service/Agency or subscriber to perform site survey to identify actions required to facilitate installation of subscriber equipment.

j) Subscriber Equipment and/or Interface Installation

Subscribers responsible for installation of any hardware and/or software to include the necessary DDN interface.

IMPLEMENTATION/INSTALLATION PLAN

- Statement of Requirements
 - verify functional user requirements
- Implementation
 - major milestones
 - incremental achievements
 - presentation
 - completeness
- Description of Facility
 - identify location
 - identify floorspace
 - interface mechanism
 - ancillary devices
- Support Construction
 - subscriber system construction program
 - subscriber system allied support construction
 - subscriber system construction organization
 - network construction
- Installation
 - subscriber system installation
 - network installation
- Logistics support
 - equipment maintenance
 - supplies
 - operator handbook
 - training
- Coordination
 - SSIC
 - coordination channels

DDN CUTOVER PLAN

- System Description
 - hosts
 - terminals
 - system connectivity
 - references
 - verification
- Operational Description
 - system functions
 - types of data transfer
- Cutover Organization
 - organization chart
 - team members
- Security
 - requirements
 - procedures
- Cutover
 - method
 - tasks
- Fallback Capability
 - method
 - task
 - criteria
- Subscriber Acceptance
 - criteria
 - discrepancies
 - testing
- Cutover Schedule
 - scheduling factors
 - schedule

GENERAL HOST SCHEDULE & RESPONSIBILITIES

<u>ACTION</u>	<u>RESPONSIBILITY</u>	<u>TIMEFRAME</u>
Submit H1	Subscriber	24 Months
Enter Data in URDB	TCO/DCSDS	23 Months
Conduct Subscriber Interview	DCSDS/TCO	22 Months
Develop FRID	DCSDS	20 Months
Develop Acquisition Plan	Subscriber	19 Months
Perform Site Survey	Subscriber	14 Months
Submit RFS to TCO	Subscriber	13 Months
Forward Feeder TSR to DCSDS	TCO	12 Months
Prepare I/IP	Subscriber	8 Months
Prepare Cutover Plan	Subscriber	8 Months
Submit TSR to DECCO	DCSDS	7 Months
Issue TSO	DCSDS	6 Months
Issue CLAM	DECCO	5 Months
Fully Qualified DDN Interface Acquired	Subscriber	3 Months
DDN Interface Installation	Subscriber	2 Months
Operational Test & Acceptance	Subscriber	2 Weeks
Cutover		Target

NETWORK INFORMATION CENTER

- **Funded by the DDN PMO**
- **Multiple methods of accessing**
- **Good source of general reference material for the network**
- **Provides network services for users**
- **Builds and Maintains Databases**
- **Registers users**

E. USING THE NIC

The Network Information Center (NIC) is responsible for providing information to the users of DoD networks, particularly MILNET and ARPANET. The NIC is funded by DCA.

1) How to Contact the NIC

a) Electronic Mail

- NIC@SRI-NIC.ARPA
- HOSTMASTER@SRI-NIC.ARPA
- REGISTRAR@SRI-NIC.ARPA

b) Commercial Telephone

- (800) 235-3155
- (415) 859-3695

c) U.S. Postal Service

Network Information Center
SRI International
Menlo Park, CA 94025

WARNING

AUG 1 DDN STARTS TAC AUDIT NIC NEWS #40 HAS INFO

NOTE YOUR TAC PORT BEFORE 1 AUG.

PROBLEMS: AV356 (703)285-5230

DARCOM TAC 112 #:15

@o 26.2.0.72

TAC Userid: XXX-XXXX

Access Code: XXXXXXXXX

Login OK

TCP Trying...Open

Welcome to DDN2 running BBN O/S BBNCC Release 5.3 23-Jan-1984

;login: XXXXXXXX

BBNCC Release 5.3 23-Jan-1984

WELCOME to DDN-2 MASSACHUSETTS 26.2.0.72

C Machine Release 5.3

***** THIS HOST IS A DDN MAIL SERVER *****

***** PLEASE RESTRICT USE TO INFOMAIL ONLY *****

TERM = (unknown) vt100

Erase set to Backspace

Kill set to Control-U

Welcome to InfoMail -- Version 2.5.1 -- Used under license from BBNCC

Password: XXXXXXXX

INBOX now opened

INBOX.

1 From:wjc @ ll-v /Subject: System V -- Help / Thu, 3 Oct 85 13:32:54

-->system

Type <cr> to return to InfoMail.

UNIX> nickname nic

[nic]

2) What the NIC does

a) Sources of General Reference Material

- The DDN Directory
- The DDN Protocol Handbook
- The DDN New Users Guide
- DDN Newsletter
- DDN Management Bulletin
- DDN News Flash
- DDN Protocol documents

b) Provider of Network Services

- NIC/Query program
- WHOIS
- NIC Hostname Server
- TACNEWS
- Online files
 - The official Internet DoD Hostnames table
 - The official DDN Host Administrators file
 - The official liaison files
 - Request For Comments (RFCs) file
 - Internet Experimental Notes (IENs)

c) Registers Users

- MILNET users
- Assigns TAC access id and password

SRI International (SRI-NIC)

**Telecommunications Sciences Center
Network Information Center
333 Ravenswood Avenue
Menlo Park, California 94025
Phone: (415) 859-3695**

**NetAddress: 26.0.0.73, 10.0.0.51
Nicknames: NIC**

Host Administrator:

**Feinler, Elizabeth J. (JAKE) FEINLER@SRI-NIC
(415) 859-3695**

Liaison:

**Neou, Vivian (VN) VIVIAN@SRI-NIC
(415) 859-4781**

DDN user assistance	(800) 235-3155	NIC@SRI-NIC.ARPA
Computer Operations	(415) 859-5921	ACTION@SRI-NIC.ARPA
WHOIS updates, user registration		REGISTRAR@SRI-NIC.ARPA
Host changes and updates		HOSTMASTER@SRI-NIC.ARPA
Suggestions		SUGGESTIONS@SRI-NIC.ARPA

UNIX>

-->quit

**Host closing connection
CLOSED**

@o 26.0.0.73

TCP Trying...Open

SRI-NIC, TOPS-20 Monitor 6(6401)-4

* For TACNEWS, enter: tacnews<RETURN>

* To find the host administrator for host xy-z, enter:whois xy-z

* Report system problems to Action@SRI-NIC or call (415) 859-5921

@tacnews

SRI-NIC TACnews 1.3(44)-2 on Thursday, 3-Oct-85 12:25pm-PDT

Send error reports to TACNEWS@SRI-NIC.ARPA and comments or
suggestions about the program to SUGGESTIONS@SRI-NIC.ARPA.

Stop output every 24 lines? (Y/N/# of lines/?) N

1. Announcements (updated 12-Aug-85)
- * 2. Dial-Ups (MILNET/ARPANET TAC phone numbers updated
13-Sep-85)
- * 3. Login (Help with TAC login, updated 24-Aug-84, 5K chars)
4. Newsletters (DDN News, updated 1-Jul-85)
5. Bulletins (DDN Management bulletins, updated 14-Jun-85)

Type a menu number ('HELP<CR>' for more info): quit

Killed Job 25, User ANONYMOUS.TACNEWS, Account QUERY, TTY 111

Host closing connection

Closed

AD-A173 472

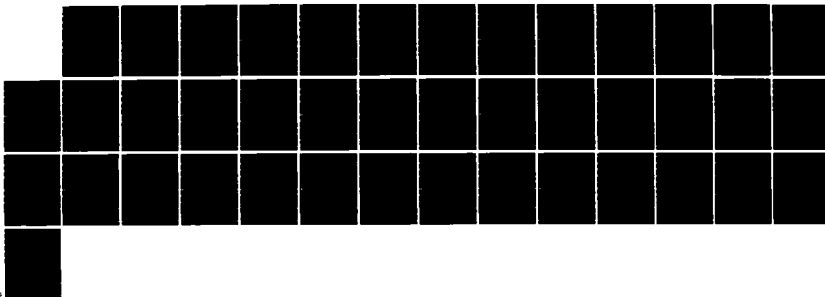
THE DDM (DEFENSE DATA NETWORK) COURSE(U) NETWORK
STRATEGIES INC FAIRFAX VA R DE VERE ET AL. APR 86
DCA100-83-C-0062

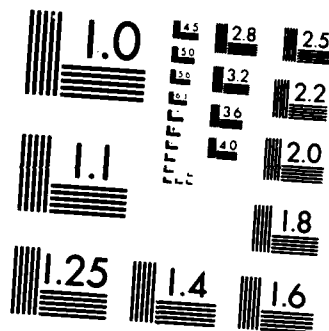
4/8

UNCLASSIFIED

F/G 17/2

NL





MICROCOPY RESOLUTION TEST CHART
NATIONAL BUREAU OF STANDARDS 1963-A

@o 26.0.0.73
TCP Trying...Open

SRI-NIC, TOPS-20 Monitor 6(6401)-4

- * For TACNEWS, enter: tacnews<RETURN>
- * To find the host administrator for host xy-z, enter: whois xy-z
- * Report system problems to Action@SRI-NIC or call (415) 859-5921

@whois nic

SRI International (SRI-NIC)
Telecommunications Sciences Center
Network Information Center
333 Ravenswood Avenue
Menlo Park, California 94025
Phone: (415) 859-3695

NetAddress: 26.0.0.73, 10.0.0.51
Nicknames: NIC

Host Administrator:
Feinler, Elizabeth J. (JAKE) FEINLER@SRI-NIC
(415) 859-3695

Liaison:
Neou, Vivian (VN) VIVIAN@SRI-NIC
(415) 859-4781

DDN user assistance	(800) 235-3155	NIC@SRI-NIC.ARPA
Computer Operations	(415) 859-5921	ACTION@SRI-NIC.ARPA
WHOIS updates, user registration		REGISTRAR@SRI-NIC.ARPA
Host changes and updates		HOSTMASTER@SRI-NIC.ARPA
Suggestions		SUGGESTIONS@SRI-NIC.ARPA

To see a list of users registered for this site, repeat the command,
preceding the argument with a star, e.g. "*nic" instead of
"nic".

@logout
Killed Job 25, TTY 111, at 3-Oct-85 12:27:44
Used 0:00:03 in 0:01:16
Host closing connection

@o 0/73
TCP Trying...Open

SRI-NIC, TOPS-20 Monitor 6(6401)-4

- * For TACNEWS, enter: tacnews<RETURN>
- * To find the host administrator for host xy-z, enter: whois xy-z
- * Report system problems to Action@SRI-NIC or call (415) 859-5921

@nic
TOP

NIC/Query is a database system containing information about the Defense Data Network (DDN), including MILNET and ARPANET. Each list of topics is presented to the user as a numbered menu of selections.

- To see more detail on any of the topics below, type its corresponding number followed by a carriage return, <CR>.
- To leave NIC/Query, type 'quit<CR>'.
- For more help and additional commands, type 'help <CR>'.
- Send error reports to NIC@SRI-NIC.ARPA. Send comments or suggestions about the NIC/Query program to SUGGESTIONS@SRI-NIC.ARPA.

1. INTERNET PROTOCOLS -- Describes Internet protocols
2. PERSONNEL -- Directory of DDN users
3. HOSTS -- Describes DDN hosts
4. RFCS -- Requests For Comments technical notes
5. IENS -- Internet Experiment Notes
6. NIC DOCUMENTS -- Documents available from the NIC

_ for back, ^ for up, + for top, or menu # (1-6): 6
NIC DOCUMENTS

1. PROTOCOL HANDBOOK
2. INTERNET PROTOCOL BOOKS
3. DDN DIRECTORY
4. OTHER DOCUMENTS
5. HOW TO ORDER DOCUMENTS

_ for back, ^ for up, + for top, or menu # (1-5): quit

Bye now!

Killed Job 25, User ANONYMOUS.NICGUEST, Account QUERY, TTY 111
Host closing connection

APPENDIXES

DDN INTERFACE AVAILABILITY

Host Vendor	Host/Term. Models	Oper. Sys. & Version	Vendor	Protocols	Hardware Required	Qual. Status	Availability Date
Burroughs	A Series	MCP 3.6	SDC	Full Suite*	CP 8201 Commun. Processor	not sched.	June 86
CDC	170, 180	NOS NOS / BE	CDC	Full Suite*	CDC Net	not sched.	May 86
DEC	VAX	VMS	Internet	Full Suite*	ACC ACP 625	X.25	Apr. 86
	11/xxx	VMS	Wollongong	Full Suite	ACC	X.25	Oct 85
Honeywell	DPS-6	GCOS 6 Mod 4	Honeywell	Full Suite*	CS/1-DDN	X.25	Nov 85
	DPS-8	GCOS 8 2300			Datanet 8 CS/1-DDN	X.25	Nov 85
	VIP Terminals	N/A	Protocom	X.25	X.25 PAD P-250 & P-2500	X.25	Now
Hewlett Packard	HP3000	MPE53	Hewlett Packard	X.25	Intelligent Network Processor	X.25 Basic	Dec 85
IBM	IBM Hosts	COS 2	NCR Comten	X.25	Comten FEP	X.25 Standard Basic	Oct 85
	370, 303x, 43xx, 308x	VM/SP	IBM	Full Suite*	Series 1, CSI	X.25	Jan. 85
		MVS 3.0	Network Solutions	X.25	37x5	Conditional	Dec 85
				Full Suite*	ACC IF/370-DDN	X.25	Feb. 86
	Bisync & SDLC Term.		Protocom	X.25	X.25 PAD P-250 & P-2500	X.25	Now
Sperry	1100	OS 1100	Sperry	Full Suite	DCP 10, 20, 40	X.25 Basic	Now
	1100	OS 1100	Internet	Full Suite*	DEC Micro Vax ACC ACP 625	X.25	Feb. 86
	Uniscopes Terminals	N/A	Protocom	X.25	X.25 PAD P-250 & P-2500	X.25	Now
Tandem	TNS-11	TNS-11 R A-06	Tandem	X.25	None	X.25	Now
Wang	VS-100	VS-TCI	Wang	Full Suite	None	X.25	Now

* - DCA Sponsored Host Interfaces

A - 1

as of 12/85

DDN INTERFACE - VENDOR SUMMARY

MANUFACTURER:	BURROUGHS CORPORATION
PRODUCT:	MIL/INT NETWORK
AVAILABILITY:	MARCH 1984
COST:	\$50,000 - \$100,000 depending on configuration
HARDWARE:	CP-8201 Host Network Front End, B1900 Mini-computer, Burroughs B1900 series, DEC
SOFTWARE:	DEC VAX UNIX and VMS, and DEC PDP-11 UNIX

BACKGROUND: All Burroughs' DDN development is being done by their wholly owned company Systems Development Corporation (SDC). SDC has developed the MIL/INT Network Products, their CP8000 series, specifically to interface to the Defense Data Network.

SYSTEM DESCRIPTION: The CP8201 is a generic Host Network Front End which supports TCP/IP, 1822J HDH, and the Host Front End Protocol (HFEP). It is designed to interface to any hardware running UNIX or VMS operating systems. The B1900, a 16-bit mini-computer, supports the upper level protocols, FTP, SMTP, Telnet, and the Host Front End Protocol. It is connected serially to the CP8201.

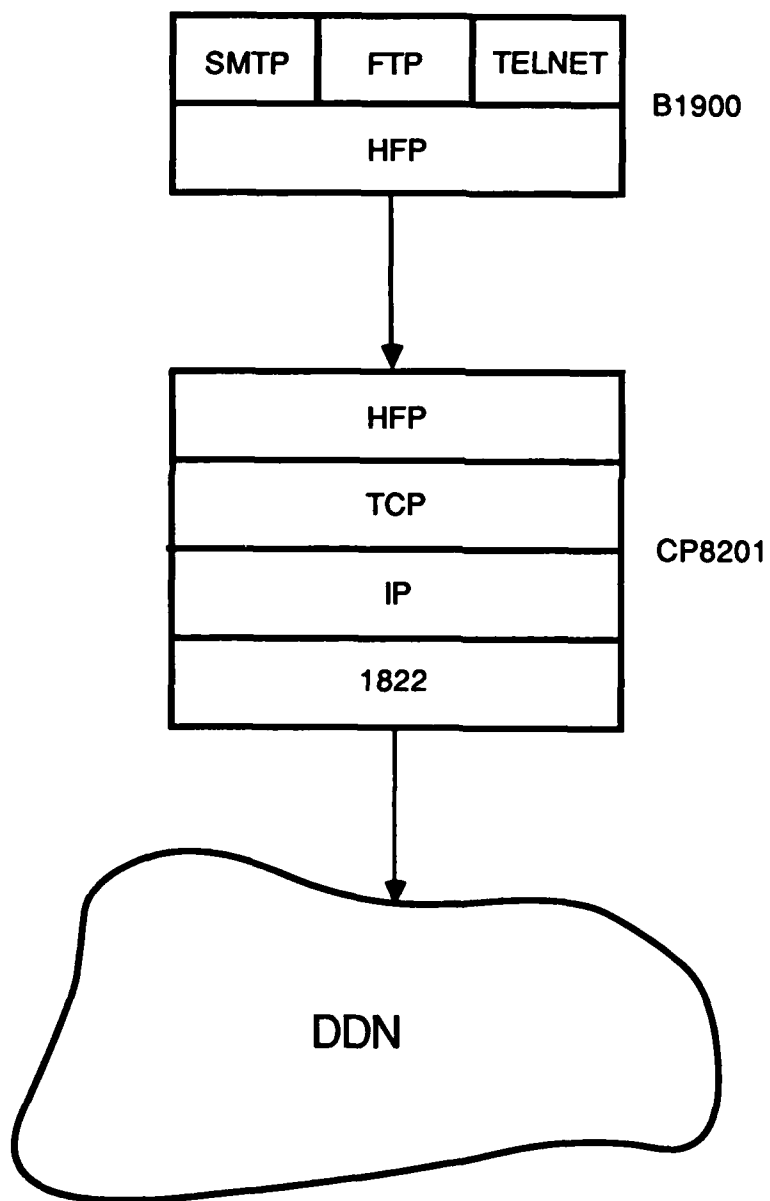
SDC is under contract to DCA to interface the CP8201 to Burroughs' A series of mainframes. Currently, A series products support X.25 basic only, and therefore, can connect only Burroughs equipment. There is no interoperability to other vendor's equipment. Under this contract, SDC plans to implement the upper level protocols in the mainframes, with the lower level protocols being off loaded in the FEP. The contract expires in June 1986. The proposal to interface to the CP8201 was presented in mid-1984, awarded a year later and in the meantime their product line changed.

FUTURE DEVELOPMENTS: SDC is now working on an as yet unannounced product, the CP2000 Communications Front End, which will be integrated into the Burroughs Network Architecture (BNA). TCP, IP and X.25 will be implemented here and the CP2000 will be connected to the A series products via a high speed channel interface. The CP2000 will also be able to function as a LAN gateway, and will support SNA.

SDC would not discuss this plan further without a non-disclosure agreement. They are working to renegotiate their contract with DCA to take advantage of their changing technology.

Burroughs

System Configuration



MANUFACTURER: DIGITAL EQUIPMENT CORPORATION (DEC)

PRODUCT: PACKETNET SYSTEM INTERFACE (PSI)
ADVANCED COMPUTER COMMUNICATIONS
(ACC) ACP625, ACP6250
Wollongong Group (TCP/IP, TELNET, SMTP,
FTP) DEC Unix Based Operating System

AVAILABILITY: Immediate

COST: PSI = \$2800 for each cpu software license,
\$1800 for distribution and documentation
ACC ACP625 = \$6,490; ACP6250 = \$7,650
Wollongong software = \$14,350 (GSA Pricing)
DEC Ultrix Operating System = No charge (DoD
suite of protocols inherent to Unix OS)

HARDWARE: VAX/PDP 11 System

SOFTWARE: VMS/Ultrix/TOPS-20 Operating System

BACKGROUND: Until this past year Digital promoted the use of "DECnet" exclusively, its proprietary networking software for interconnecting homogeneous DEC systems. Digital recognized the need to offer a solution for interconnecting heterogeneous systems and addressed this with the introduction of the DEC Unix based Operating System "Ultrix" which packaged TCP/IP, TELNET, FTP, and SMTP as an integral part of the operating system. In addition to Ultrix, DEC has announced support of the Wollongong software (The Wollongong Group took the University of California-Berkeley Unix BSD 4.1 and "ported" it to VMS).

SYSTEM DESCRIPTION: If a subscriber with a DEC system wishes to interface with the DDN using the "X.25 Basic Service," they need to purchase the ACC IF-11/X.25 interface board from Advanced Computer Communications. The IF-11/X.25 has been fully qualified to operate on the DDN. The "X.25 Standard Service" requires the DoD suite of protocols (i.e., TCP/IP, TELNET, FTP, SMTP); a DEC system running the Ultrix Operating system or the Wollongong software running under VMS would satisfy this requirement.

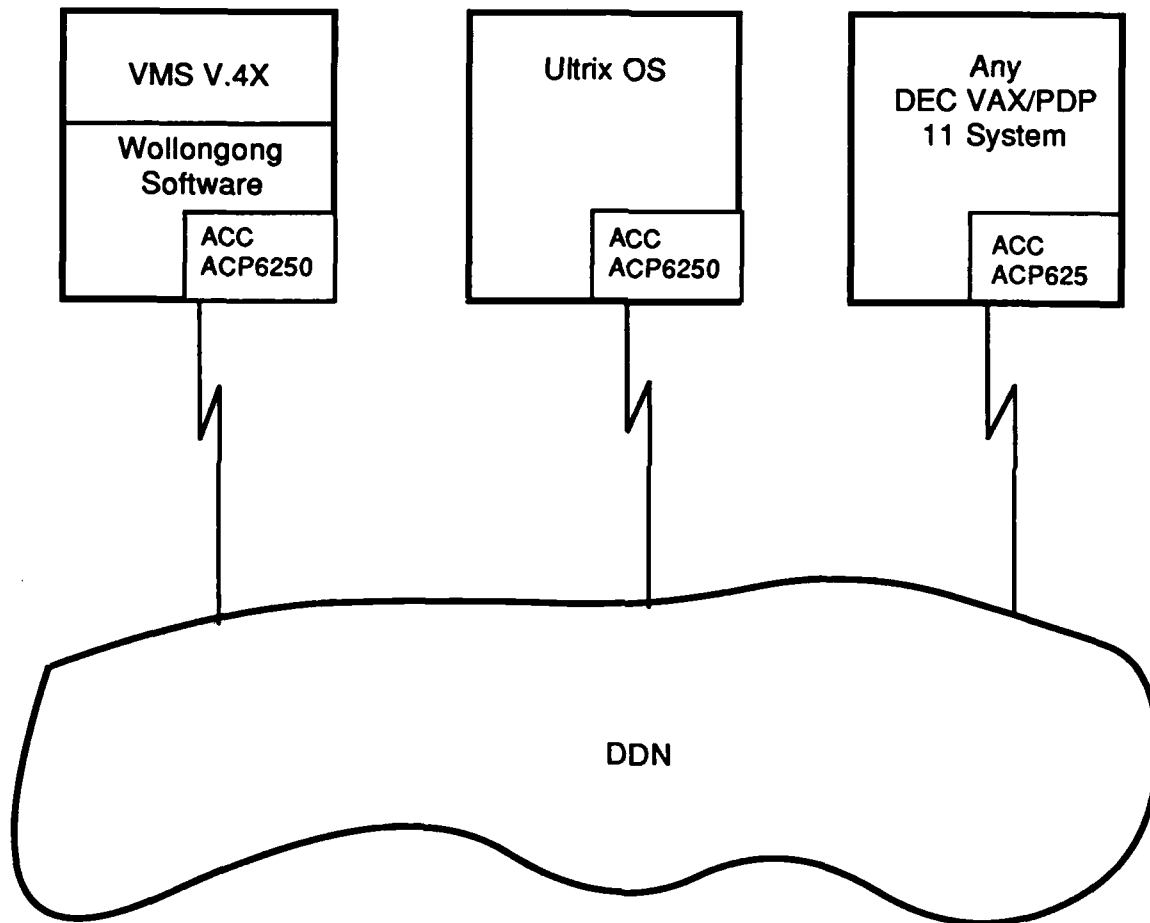
FUTURE DEVELOPMENTS: Digital is presently working on an OEM agreement with Advanced Computer Communications to market and support the LH/DH-11 (1822HDH) interface board. DEC is in the process of determining the feasibility of qualifying the PSI X.25 interface for use on the DDN.

Digital Equipment Corporation

System Configuration

"X.25 STANDARD SERVICE"

"X.25 BASIC SERVICE"



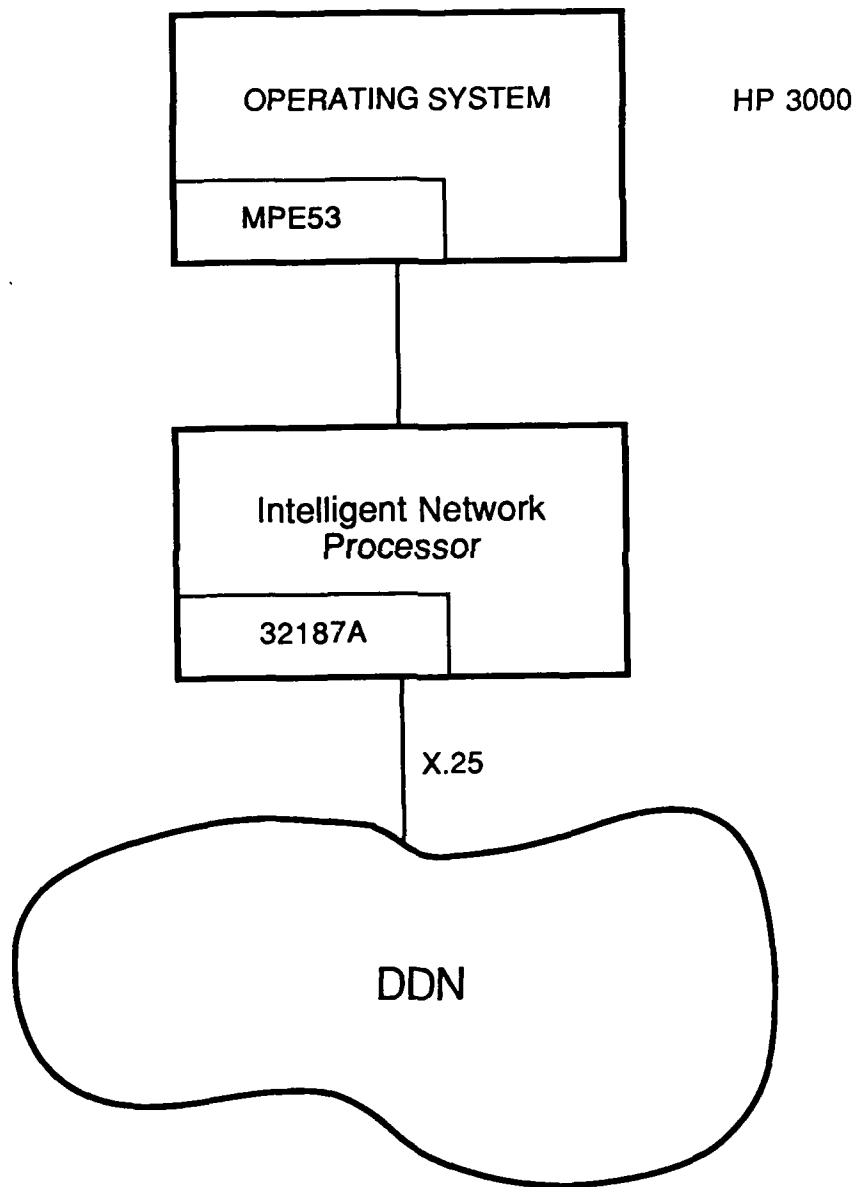
MANUFACTURER: HEWLETT-PACKARD
PRODUCT: INTELLIGENT NETWORK PROCESSOR
AVAILABILITY: Awaiting DDN qualification
COST: Pricing Not Available
HARDWARE: HP3000 host computer
SOFTWARE: MPE5E

BACKGROUND: HP currently has a 90 day conditional qualification for its X.25 interface to the DDN. The conditional qualification expires approximately the end of October 1985. HP has not yet scheduled further testing to obtain a fully qualified DDN X.25 interface. HP will be sending in another error file to the DDN for evaluation and will then schedule another qualification test.

SYSTEM DESCRIPTION: The initial qualification testing for a DDN X.25 interface will allow for interoperability among the HP3000 community of users. HP users must be running, at a minimum, the MPE5E release in order to support the DDN X.25 interface. This is the release level that the qualification testing was conducted on. The DDN X.25 interface is upward compatible with higher level HP releases. Subscribers must procure both hardware and software to run the DDN X.25 interface. The Intelligent Network Processor (INP) is the required hardware and the software is 32187A. These two products are bundled together and the price to the subscriber will vary depending upon the subscriber application. If the subscriber is connecting the INP to an HP host computer, the cost will be in the neighborhood of \$9,000. This includes the INP and the supporting software, 32187A. HP currently supports TCP/IP protocols between HP3000s running NS/3000 on an Ethernet LAN.

FUTURE PLANS: HP is currently developing prototypes of the full suite of DDN prototypes to include Internet Protocol (IP), Transport Control Protocol (TCP), Simple Mail Transfer Protocol (SMTP), File Transfer Protocol (FTP), and Telnet. These upper level protocols will run above the HP DDN X.25 protocol. These prototypes are not expected to be available until the fall of 1986. At that time, HP is planning to schedule DDN qualification testing for TCP and IP. (The DDN PMO plans to have TCP/IP qualification testing available in early 1986.).

Hewlett Packard System Configuration



MANUFACTURER: HONEYWELL

PRODUCT: HONEYWELL DDN PRODUCTS

AVAILABILITY: JANUARY 1986

COST: PRICING NOT AVAILABLE

HARDWARE: HONEYWELL DPS 8/20 with 4 MB of memory, a HONEYWELL DN-8 Communications Processor with 512 KB of memory and a HONEYWELL DDN Interface Unit (DIU) with a V.35 interface or HONEYWELL DPS 6/40 with 512 KB of memory and a HONEYWELL DIU with a V.35 interface.

SOFTWARE: DPS 8/20 with GCOS 8, Release 2300 Operating System, DPS 6/40 with GCOS 6 MOD 400, Release 2.6 Operating System, DN-8 with DNS, Release 3.1 Operating System and DIU with DIU Operating System.

BACKGROUND: Honeywell is developing and will provide the full "DDN protocol suite" via their DPS 8 and DPS 6 families of processing systems. The DDN protocol offering includes the following:

- (a) FED STD 1041 (X.25 Level-3)
- (b) Internet Protocol (IP)
- (c) Transmission Control Protocol (TCP)
- (d) Telnet
- (e) File Transfer Protocol (FTP)
- (f) Simple Mail Transfer Protocol (SMTP)

SYSTEM DESCRIPTION: The DPS 8 design uses 3 major pieces of hardware in its configuration; DPS 8, DataNet 8 and the DDN Interface Unit (See Attachment). The DPS 6 design uses 2 devices in its configuration; DPS 6 and the DDN Interface Unit. The protocol software is spread across each of these configurations.

The DDN Interface Unit (DIU) is a 68000 based microprocessor outboard unit built by Bridge Communication. Honeywell is modifying the software in an OEM agreement with Bridge and will be offering the DIU as a standard Honeywell product (i.e., with Honeywell logo).

Honeywell is offering a decoupled DDN interface. There will be 8 DDN products offered by Honeywell, 4 for each DPS configuration. The DDN products that will be offered for each Honeywell configuration are as follows:

- FTP
- SMTP
- TELNET
- DDN Interface Unit with TCP/IP

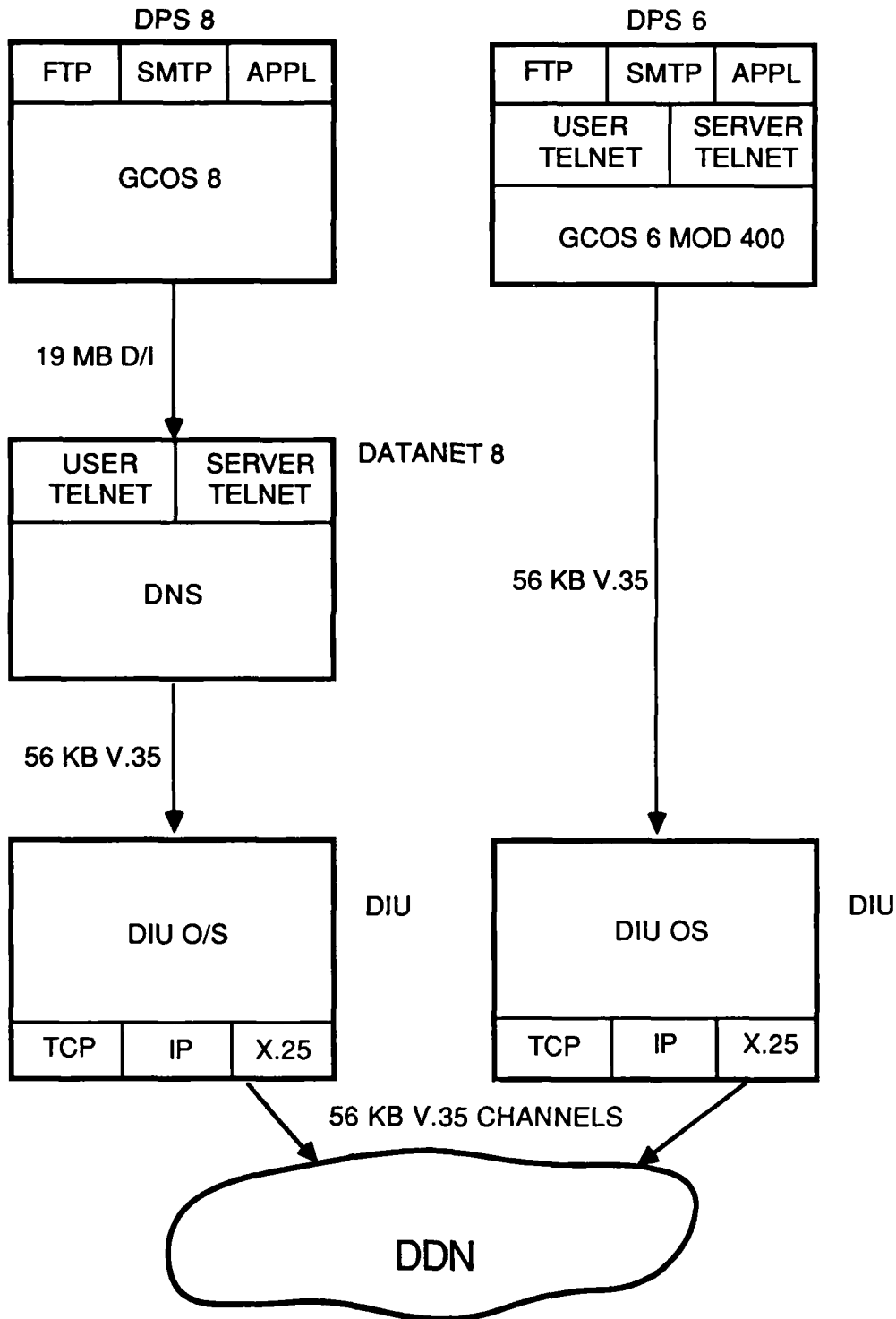
FUTURE DEVELOPMENTS: Honeywell is going through the final phase of their X.25 testing and waiting on receiving two DDN circuits to enable them to complete this phase. They expect to be ready for DCA qualification of their DDN X.25 by mid-September 1985.

Currently the TCP/IP interface is in unit testing and the high level protocols (TELNET, FTP, SMTP) are in the design phase.

Honeywell feels confident that they will have a complete set of products available for beta test by mid-January 1986. These products will be licensed and offered as standard Honeywell products.

Honeywell

System Configuration



MANUFACTURER: INTERNATIONAL BUSINESS MACHINES

PRODUCT: VM INTERFACE PROGRAM FOR TCP/IP

AVAILABILITY: 1822 HDH Currently available, X.25 will be available in January of 1986.

COST: This program is offered for a one time charge of \$17,000.

HARDWARE: Any 370 type CPU i.e., S/370, 303X, 43XX or 308X.
Series 1 Model 4956 with 512K
Channel Systems International M1 S1
Communications Line Attachment card
Channel Systems International Series/1-370
Channel Attachment card

SOFTWARE: VM Interface program for TCP/IP
IBM System Control Program VM/SP, Release 3, 5664-167

The Series/1 requires the following software:

Basic Supervisor and Emulator Version 4
CSI's Channel Attach and Arpanet HDH
Communications Line Attach Software

The Series/1 using the X.25 protocol must have the following software:

Realtime Programming System Version 5.2
Systems Macros
Realtime Programming System Generation
Facilities
Series/1 - System 370 Channel Attach Program
Realtime Programming System Packet Network
Support Program

Note: Subsequent versions or releases of the above software may affect the functions of this program offering.

BACKGROUND: Currently there are IBM 370 type systems that have been grandfathered onto the DDN from Arpanet using 1822 HDH.

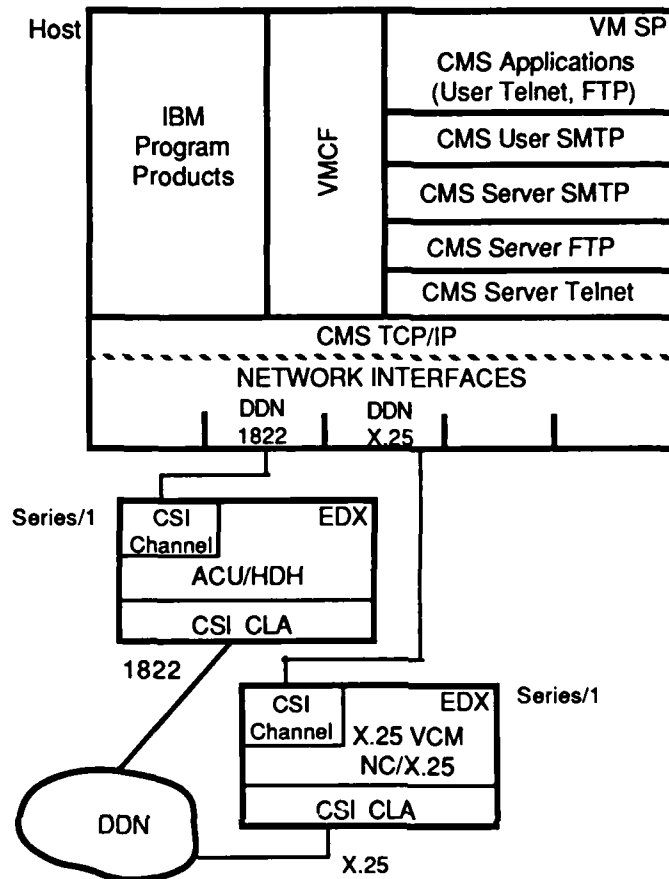
SYSTEM DESCRIPTION: The VM Interface Program for TCP/IP uses a 370 channel attached to a front-end Series/1 running the Event Driven Executive which allows a subscriber to access the DDN via X.25 or 1822 HDH. The Interface Program can reside on any 370 type architecture CPU, i.e., S/370, 303X, 43XX or 308X. The Program Offering supports three user services: file transfer to remote terminals using the File Transfer Protocol, electronic mail to remote terminals using the NOTE as a user interface to the Simple Mail Transfer Protocol and remote terminal access using TELNET. These higher level protocols utilize Transmission Control Protocol, Internet Protocol and Internet Control Message Protocol. One disconnected virtual machine handles all TCP/IP initiations.

The VM software is written almost entirely in PASCAL, with a small amount of assembler-language support. Some assembler code is found on the Series/1 X.25 interface: Standard IBM release software is implemented throughout.

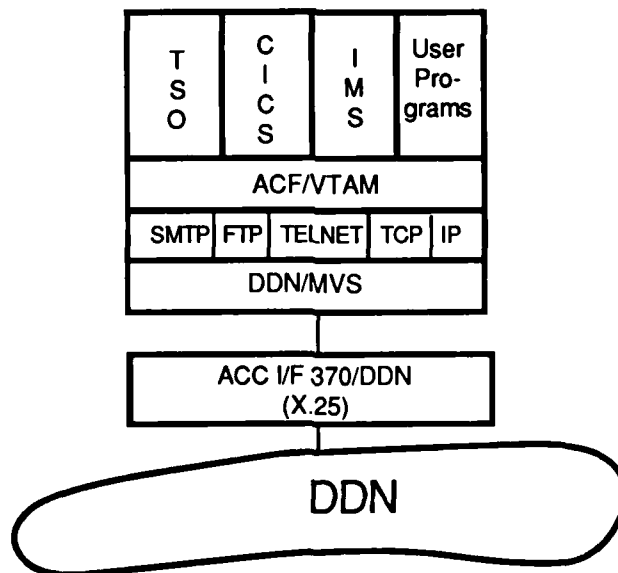
The Series/1 minicomputer is used as a front-end/protocol converter supporting either the X.25 or 1822 host interface protocols. In the case of the X.25 configuration, Internet Protocol datagrams are converted to X.25 logical channels within the X.25 VC manager. The X.25 interface currently supports 64 logical channels.

The basic hardware configuration as recommended by IBM for the Series/1 is the model 4956 with at least 512K of addressable memory. The 4956 also requires three Channel System International I/O cards. Two cards are used for channel control to and from the CPU and one is used for the Series/1 to the X.25 network interface. Upgrading from an 1822 HDH interface to a X.25 interface requires no additional hardware.

IBM VM System Configuration



Network Solutions MVS System Configuration



MANUFACTURER:	NCR COMTEN
PRODUCT:	DEVELOPMENT OF DDN PROTOCOL SUITE
AVAILABILITY:	FIRST QUARTER 1987
COST:	PRICING NOT AVAILABLE
HARDWARE:	COMTEN 3690, 3670, or 3650
SOFTWARE:	COMTEN Operating System (COS) for the full suite of DDN protocols.

BACKGROUND: NCR is committed to developing and marketing the full suite of DDN protocols and is actively testing and staging the DDN's requirements.

The project is of high priority and the appropriate channels, Vice Presidents of Marketing, Finance, Development, Sales and Software Development have been briefed.

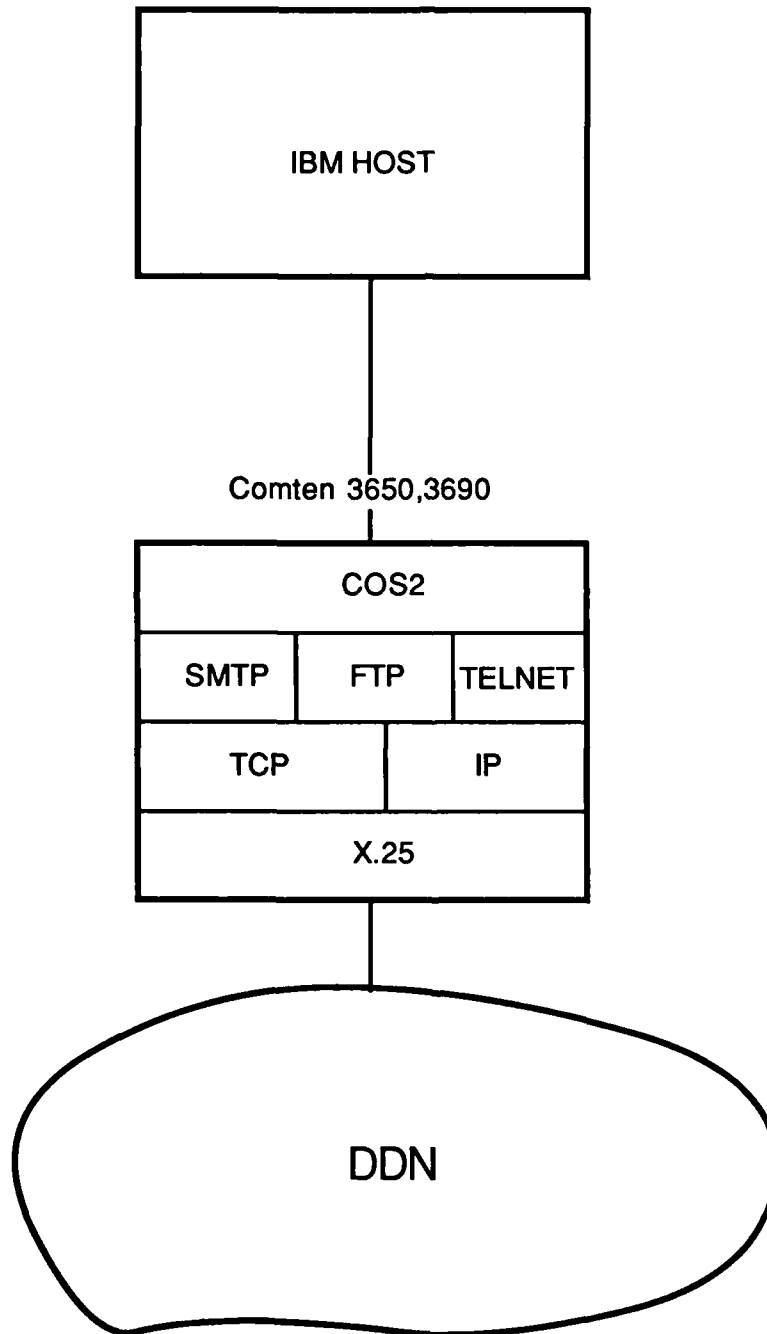
TESTING: The preliminary X.25 testing from St. Paul to Kansas City, Comten to Comten, has been scheduled several times but has yet to happen. The testing will involve Comten to Comten communications only using the 3690 or 3650 over the Marine Corps Data Network (MCDN). The problem which has caused the delay is the inability to get a circuit installed.

Additional steps are being pursued to test with the Army's Vertical Integration of Automated Data Base Level (VIABLE) system.

The second phase of NCR's testing will focus on testing TCP/IP with the cooperation of either the Air Force or Army, followed by additional testing for SMTP, TELNET, and FTP.

FUTURE DEVELOPMENTS: The development and testing of TP-4 is under serious consideration.

NCR COMTEN SYSTEM CONFIGURATION



MANUFACTURER: SPERRY COMPUTER SYSTEMS

PRODUCT: SPERRY OS1100 TO DDN

AVAILABILITY: OCTOBER 1985

COST: PRICING NOT AVAILABLE

HARDWARE: SPERRY 1100/60/70/80/90 mainframe
SPERRY DCP/40 Communications Processor
(FEP)

SOFTWARE: Series 1100 EXEC level 39r2a or higher
Communications Delivery 2r1 or higher
IPF1100 level 3r2 or higher
OS1100 to DDN level 2r1 or higher

BACKGROUND: In December of 1984 Sperry received DDN X.25 Basic service qualification. Sperry has been developing IP/TCP for their product line on and off over the past few years. According to information received from Sperry, the information obtained below is accurate.

SYSTEM DESCRIPTION: The SPERRY OS1100 TO DDN is only one element of several software products required to gain telecommunications access to the Defense Data Network (DDN). The OS1100 TO DDN interface itself consists of three products. The first, X.25 INTERFACE FOR DDN, provides X.25 capabilities to TELCON. The second component provides IP/TCP capabilities to TELCON. The third resides in the host and is DDP1100 with enhanced features for FTP, SMTP, and TELNET. Other software products required are Communications Delivery level 2r1 (CD 2r1) or higher, IPF1100 level 3r2 or higher, and DMS 1100. CD 2r1 provides TELCON and CMS1100. TELCON is the operating system for the DCP/40 and requires CMS1100 as the software interface in the 1100/XX mainframe. The product CMS1100 requires Sperry 1100 EXEC level 39r2a or higher as the Operating System in the mainframe. The TELCON X.25 INTERFACE FOR DDN is currently qualified on DDN.

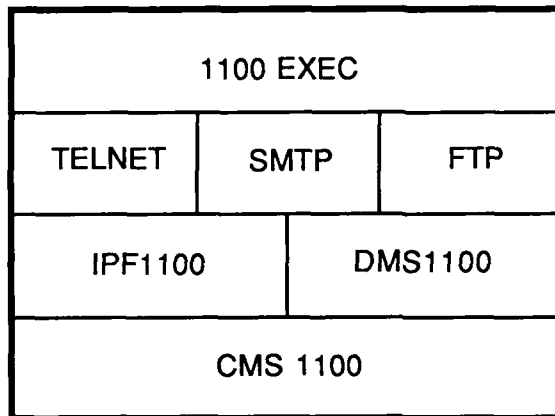
Internet Systems Corp. uses a DEC Micro-VAX II to front end Sperry 1100 series or System 11 mainframes. The Micro-VAX II supports X.25, and TCP/IP. The upper level protocols, SMTP, FTP and Telnet, reside in the host.

FUTURE DEVELOPMENTS: Sperry is currently working on an 1822 and 1822L interface which is scheduled to be available in mid 1986.

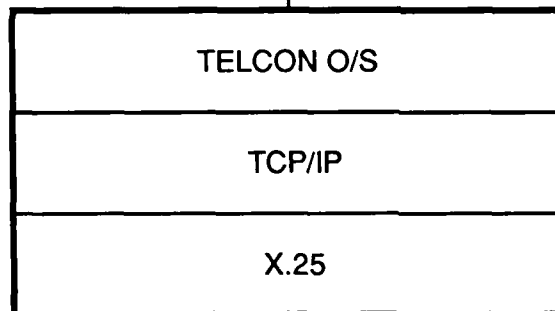
Sperry is also developing LAN capabilities which will utilize their DCP/40 as a Gateway to DDN. Current work in this area is focusing on development of GGP, and IGP protocol software for the DCP/40. There is no projected availability date for this product.

Sperry System Configuration

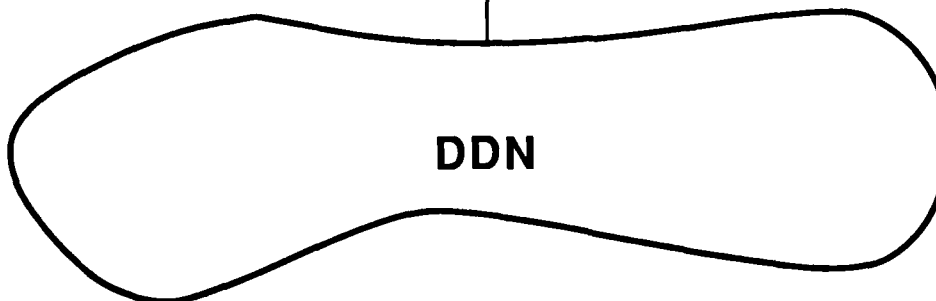
1100/XX Mainframe



DDN 1100

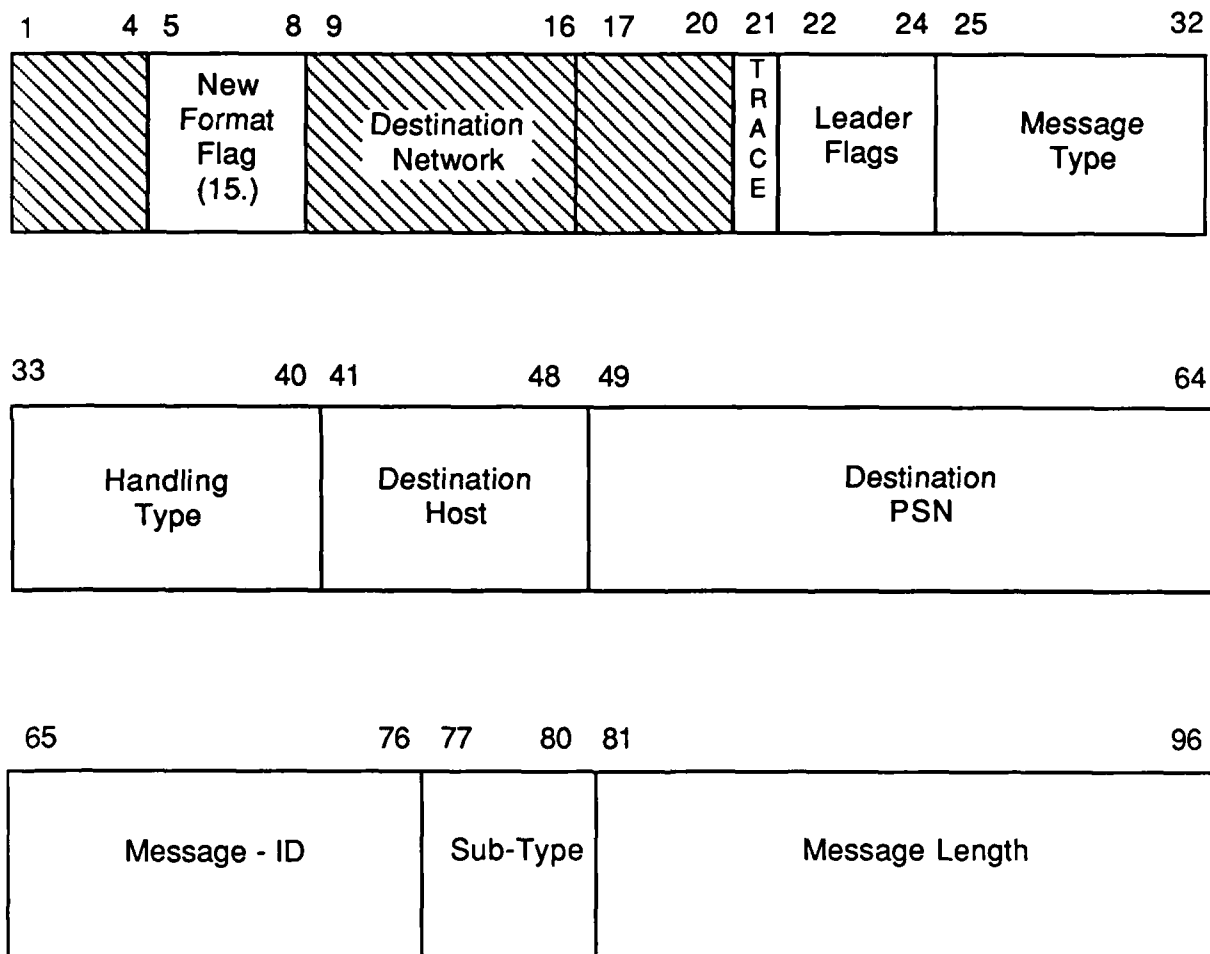


DCP/40

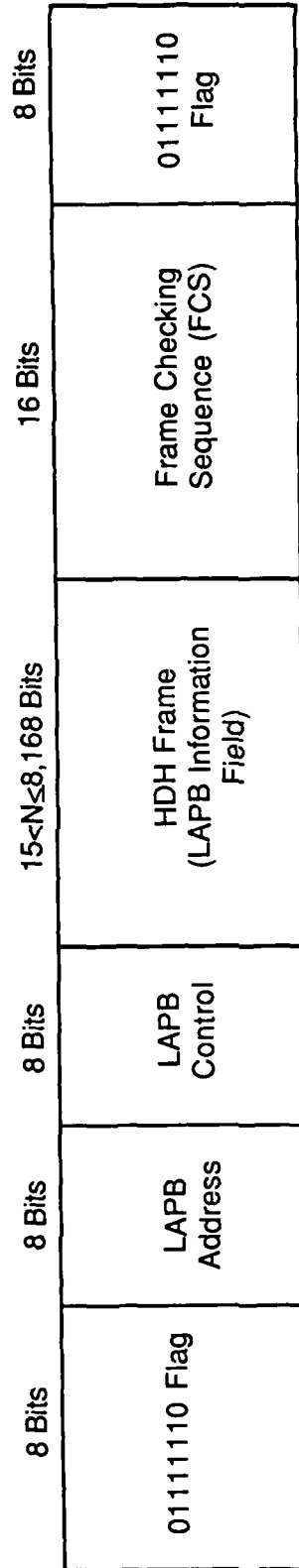


PROTOCOL HEADERS

1822 HDH HOST-TO-PSN LEADER FORMAT



1822 HDH FRAME WITHIN A LAPB INFORMATION FRAME



HDLC FRAME FORMATS

Bit order of
transmission

1 2 3 4 5 6 7 8 1 2 3 4 5 6 7 8 16 - 1 1 2 3 4 5 6 7 8

Flag	Address	Control	FCS	Flag
F	A	C	FCS	F
01111110	8-bits	8-bits	16-bits	01111110

8 - 3

HDLC Supervisory Frame

Bit order of
transmission

1 2 3 4 5 6 7 8 1 2 3 4 5 6 7 8 16 - 1 1 2 3 4 5 6 7 8

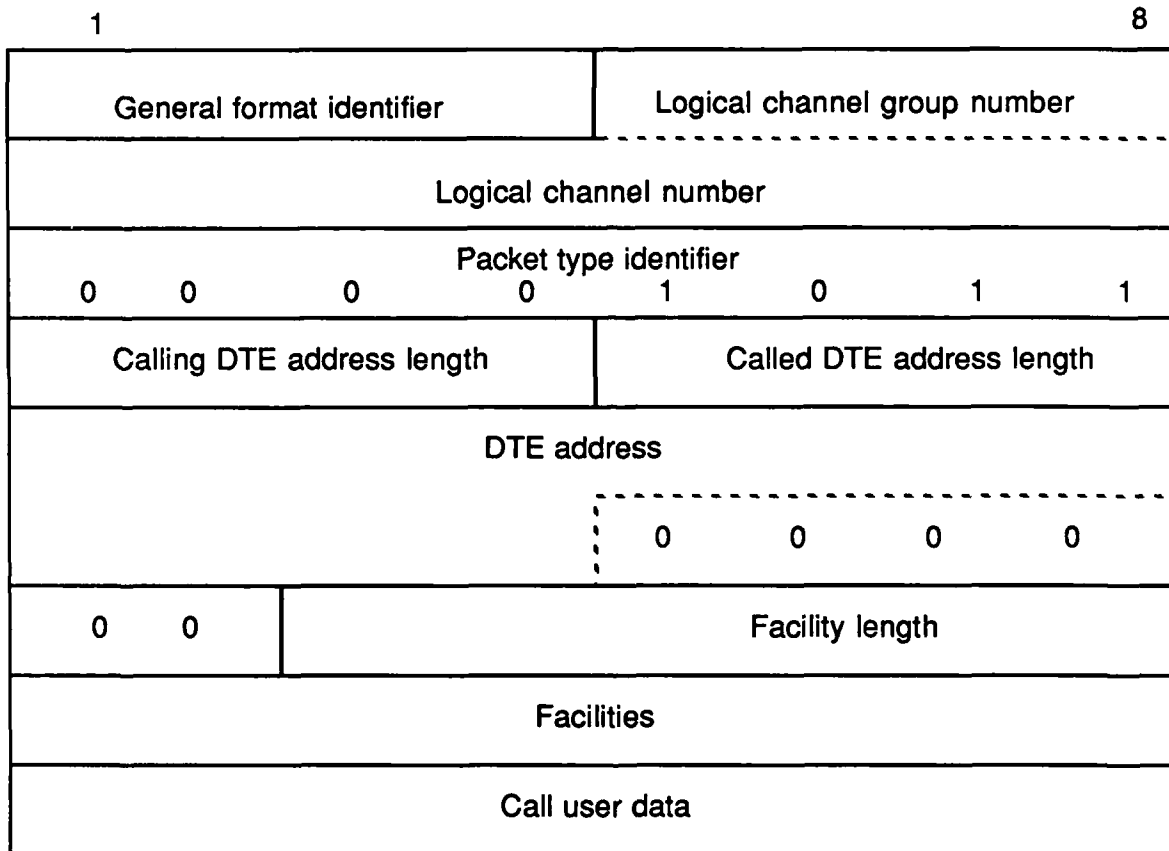
Flag	Address	Control	Information	FCS	Flag
F	A	C	I	FCS	F
01111110	8-bits	8-bits	N-bits X.25 Packet	16-bits	01111110

HDLC Information Frame

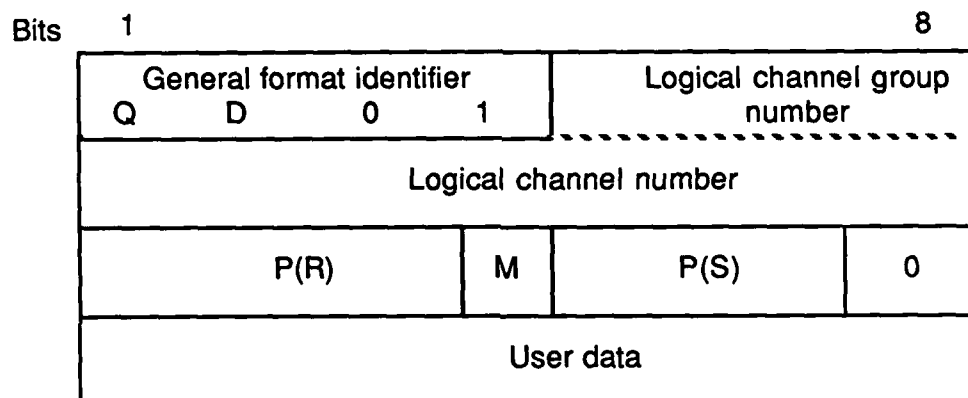
X.25 HDLC COMMANDS AND RESPONSES

		Bit Position								
		1 2 3 4 5 6 7 8								
Format	Commands	Responses	Control Field							
Information transfer	I (Information)		0	N(S)			P	N(R)		
Supervisory	RR (receive ready)	RR (receive ready)	1	0	0	0	P/F	N(R)		
	RNR (receive not ready)	RNR (receive not ready)	1	0	1	0	P/F	N(R)		
	REJ (reject)	REJ (reject)	1	0	0	1	P/F	N(R)		
Unnumbered	SABM (set asynchronous balanced mode)		1	1	1	1	P	1	0	0
	DISC (disconnect)		1	1	0	0	P	0	1	0
		UA (unnumbered acknowledge ment)	1	1	0	0	F	1	1	0
		FRMR (frame reject)	1	1	1	0	F	0	0	1
		DM (Disconnect mode)	1	1	1	1	F	0	0	0

X.25 CALL REQUEST PACKET



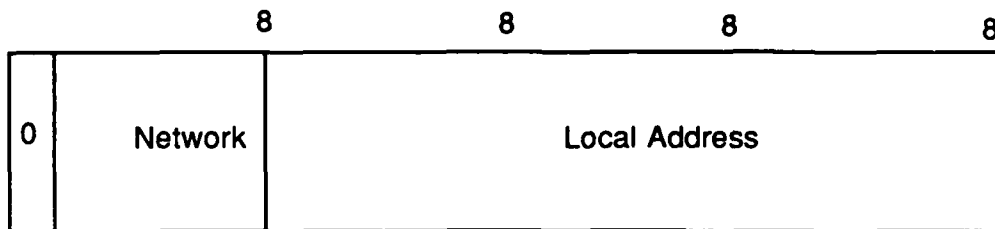
X.25 DATA PACKET



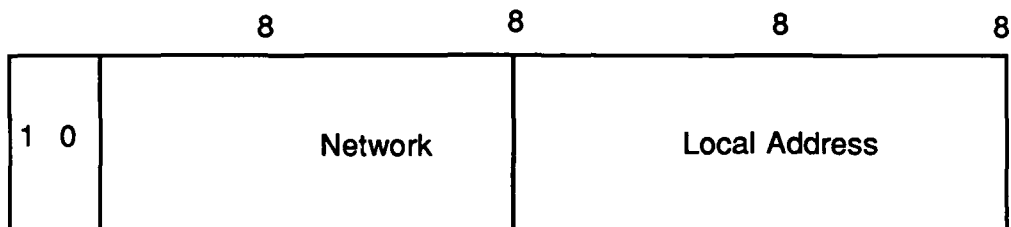
IP DATAGRAM HEADER

8		8		8		8	
Version	IHL	Type of Service		Total Length			
Identification				Flags	Fragment Offset		
Time to Live		Protocol		Header Checksum			
Source Address							
Destination Address							
Options						Padding	

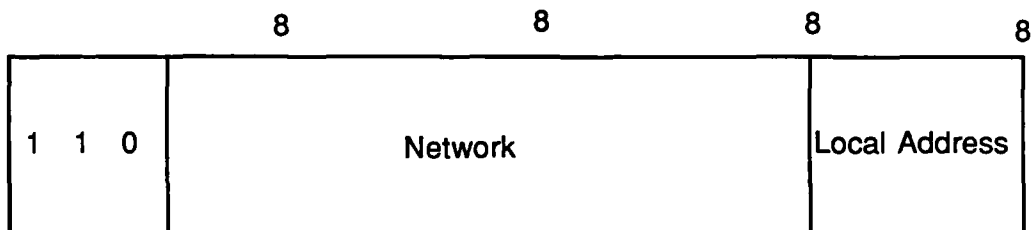
IP ADDRESS MAPPING



Class A Address



Class B Address



Class C Address

ICMP

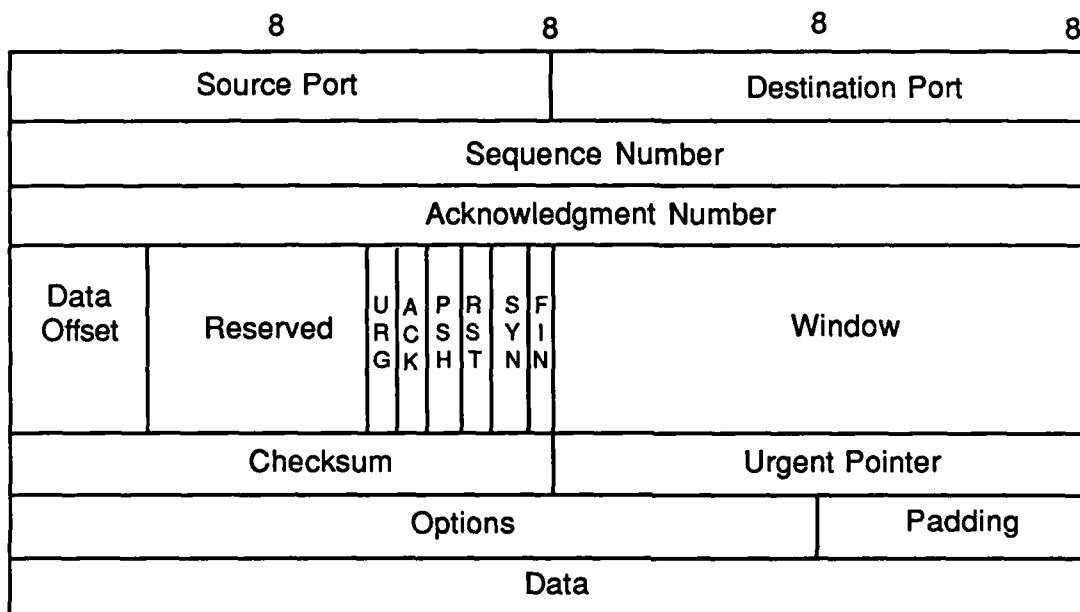
Destination Unreachable Message

8	8	8	8
Type	Code	Checksum	
unused			
Internet Header + 64 bits of Original Data Datagram			

Code

- 0 = net unreachable
- 1 = host unreachable
- 2 = protocol unreachable
- 3 = port unreachable
- 4 = fragmentation needed and Don't Fragment bit set
- 5 = source route failed

TCP HEADER



EGP MESSAGE FORMAT

8	8	8	8
EGP Version	Type	Code	Status
Checksum		Autonomous System #	
Sequence #			

EGP NEIGHBOR ACQUISITION MESSAGE

8	8	8	8
EGP Version #	Type	Code	Status
Checksum		Autonomous System #	
Sequence		Hello Interval	
Poll Interval			

GLOSSARY

ACF	Advanced Communications Function
ACC	Access Control Center
ADP	Automatic Data Processing
AED	Allocation Engineering Division
AHIP	Arpanet Host Interface Protocol
ANSI	American National Standards Institute
ARPANET	Advanced Research Project Agency NETwork
ASCII	American Standard Code for Information Interchange
BBN	Bolt Beranek and Newman
BCD	Binary Coded Decimal
BER	Bit Error Rate
BFE	Blacker Front End
BPAD	Bisynchronous Packet Assembler Disassembler
BSC	Binary Synchronous Communications
CCITT	International Telegraph and Telephone Consultative Committee
CONUS	Continental United States
CRC	Cyclic Redundancy Check
CSMA/CD	Carrier Sense Multiple Access with Collision Detection
CSU	Channel Service Unit
DARPA	Defense Advanced Research Projects Agency
DCA	Defense Communications Agency
DCE	Data Circuit-terminating Equipment
DCEC	Defense Communications Engineering Center
DCSDS	Defense Communications Systems Data Systems
DDCMP	Digital Data Communications Message Protocol
DDN	Defense Data Network
DDS	Digital Data System

DECCO	Defense Equipment Commercial Communications Office
DES	Data Encryption Standard
DH	Distant Host
DoD	Department of Defense
DSP	Display Systems Protocol
DSU	Data Service Unit
DTE	Data Terminal Equipment
E3	End-to-End Encryption
EBCDIC	Extended Binary Coded Decimal Interchange Code
ECMA	European Computer Manufacturers Association
ECU	Error Correction Unit
EGP	Exterior Gateway Protocol
EIA	Electronics Industry Association
FCS	Frame Check Sequence
FDM	Frequency Division Multiplexing
FEP	Front End Processor
FRID	Functional Requirements and Interface Document
FIPS	Federal Information Processing Standard
FTAM	File Transfer, Access, and Management
FTP	File Transfer Protocol
GGP	Gateway to Gateway Protocol
H1	Host Form
HDH	High-level Data Link Control Distant Host
HDLC	High-level Data Link Control
HEMP	High-altitude Electro-Magnetic Pulse
HFEP	Host Front End Processor
HFP	Host to Front End Protocol
ICMP	Internet Control Message Protocol
IEEE	Institute for Electrical and Electronic Engineers

IEN	Internet Experimental Notes
I/IP	Implementation/Installation Plan
IMP	Interface Message Processor
IP	Internet Protocol
IPLI	Internet Private Line Interface
ISO	International Organization for Standardization
IST	InterSwitch Trunk
JCS	Joint Chiefs of Staff
KDC	Key Distribution Center
LAN	Local Area Network
LATA	Local Access and Transport Area
LEAD	Low-cost Encryption and Authentication Device
LH	Link Header
LT	Link Trailer
LU	Logical Unit
MC	Monitoring Center
MILNET	Military Network
MILDEP	Military Department
MINET	Movement Information Network
MODEM	Modulator-Demodulator
NAC	Network Access Components
NAU	Network Addressable Unit
NBS	National Bureau of Standards
NCP	Network Control Protocol
NSA	National Security Agency
NSC	Node Site Coordinator
NSP	Network Services Protocol
NIC	Network Information Center
NU	Network Utilities

NVT	Network Virtual Terminal
OCONUS	Outside the Continental United States
OSI	Open Systems Interconnection
PAD	Packet Assembler Disassembler
PC	Personal Computer
PDN	Public Data Network
PH	Packet Header
PMO	Program Management Office
PNS	Packet Node Software
PPDU	Presentation Protocol Data Unit
PSN	Packet Switch Node
PTT	Postal Telegraph and Telephone
PU	Physical Unit
RFC	Request For Comments
RFS	Request For Service
RJE	Remote Job Entry
ROD	Required Operation Date
SACDIN	Strategic Air Command Digital Network
SATNET	Satellite Network
SCINET	Sensitive Compartmented Information Network
SDLC	Synchronous Data Link Control
SH	Session Header
SMTP	Simple Mail Transfer Protocol
SNA	Systems Network Architecture
SNI	SNA Network Interconnection
SPDU	Session Protocol Data Unit
SPF	Shortest Path First
SSIC	Subscriber System Implementation Plan
SSCP	Systems Services Control Point

STDM	Statistical Time Division Multiplexing
STE	Signalling Terminal Equipment
T1	Terminal Form
TAC	Terminal Access Controller
TACACS	TAC Access Control System
TCO	Telecommunications Certification Office
TCP	Transmission Control Protocol
TDM	Time Division Multiplexing
TDMA	Time Division Multiplex Access
TEP	Terminal Emulation Processor
TH	Transport Header
TPDU	Transport Protocol Data Unit
TSO	Telecommunications Service Order
TSR	Telecommunications Service Request
TTL	Time To Live
UDP	User Datagram Protocol
ULP	Upper Level Protocols
URDB	User Requirements Data Base
VAN	Value Added Network
VC	Virtual Circuit
VDH	Very Distant Host
WINCS	WWMCCS Intercomputer Network Communication Subsystem
WWMCCS	World Wide Military Command and Control System

END

12-86

DTIC