86 pgs

DEPARTMENT OF THE NAVY
OFFICE OF THE CHIEF OF NAVAL OPERATIONS
WASHINGTON, DC 20350-2000

IN REPLY REFER TO
OPNAVINST 2800.3
OP-945
06 OCT 1988

OPNAV INSTRUCTION 2800.3

From: Chief of Naval Operations

Subj: NAVY DATA COMMUNICATIONS PROGRAM

Ref: (a) OPNAVINST 2070.4 of 7 Mar 84
(b) OPNAVINST 2800.2 of 2 Jan 80 (NOTAL)
(c) DONIRM ltr ser 155 of 18 Dec 86 (NOTAL)
(d) NAVTELCOMINST 2066.1 of 3 Nov 87 (NOTAL)

Encl: (1) Navy Data Communications Control Architecture
(2) Data Communications Steering Committee Charter

1. Purpose. To establish the Navy Data Communications Program and assign responsibilities.

2. Scope and Applicability

a. This instruction applies throughout the Navy with regard to data communications requirements of decision and mission support information systems.

b. The basic data communication requirement is the need to transfer information. References (a) and (b) are applicable for all long haul and afloat requirements covered by this instruction. Enclosure (1) implements the Navy Data Communications Control Architecture (NDCCA), based on the guidance contained in references (a) through (c).

c. As the program evolves, this instruction will also include the overall architectural segment concept, provide Navy-wide goals and objectives, establish specific guidance, and reference other documents which provide additional details applicable to individual information and communication system elements.

3. Background

a. Information systems are becoming increasingly dependent upon data communications capacity and capabilities. Emerging technologies elicit different designs and economies. Major support problems have been encountered by Navy information systems. Local, unique solutions applied to specific bases or information systems have surfaced the critical data communications requirements: a problem in one system or area of a country causes a whole information system or geographic area degradation. Reference (c) directed the formation of a broad program to address the issue of data communications support for information systems in the Navy.

b. The NDCCA describes the architecture and summarizes the architectural segments needed as a baseline for enhancing the transfer of decision and mission support data between afloat and shore-based information systems and information systems users. The Navy mission can suffer unless each element of the comunications system works together to move information quickly and effectively to decision makers. Careful planning and management are necessary to ensure the individual system elements fit within an overall systems framework.

4. Definitions. Enclosure (1) contains a glossary of terms applicable to this instruction.

5. Data Communications Steering Committee. To ensure the Data Communications Program is meeting the emerging needs of resource sponsors, a Data Communications Steering Committee will convene periodically to review the NDCCA and subarchitectures outlined in enclosure (1). The steering committee (enclosure (2)) will be composed of representatives from Space and Naval Warfare Systems Command, Naval Telecommunications Command, Naval Data Automation Command, and the Office of the Chief of Naval Operations (OPs- 094, 44, 941, 942, 943, and 945). OP-094 will chair this steering committee.

6. Responsibilities

a. CNO (OP-094) shall:

(1) Act as overall manager of the Navy Data Communications Program and related sub programs.

b. Commander, Space and Naval Warfare Command shall:

(1) Ensure interoperability of enclosure (1) with mission architectures, including warfare and command and control architectures.

c. Commander, Naval Telecommunications Command shall:

(1) Provide support to bases to implement communications plans consistent with enclosure (1). Ensure that specifications for procurement incorporate provisions of enclosure (1).

(2) Ensure interoperability of enclosure (1) with mission architectures including the Naval Telecommunications Systems.

(3) Ensure provisions of enclosure (1) are submitted to DCA for consideration in common user systems, including DDN and DSN.

d. Commander, Naval Data Automation Command shall:

(1) Maintain the overall data communications architecture (enclosure (1)).

(2) Ensure that data communications plans (enclosure (1)) are prepared for all bases and stations, and include provisions for cost benefit analysis for projects and local user chargeback.

(3) Ensure that the Navy is adequately represented at DOD and national protocol and network security standardization bodies and that appropriate provisions of enclosure (1) are submitted for inclusion in emerging standards efforts.

(4) Demonstrate feasiblity of enclosure (1) through extensive operational testing and rapid prototyping.

e. Commander, Naval Facilities Engineering Command shall ensure that base master planning includes provision of enclosure (1).

7. Action. Addressees shall ensure:

a. All Information Systems acquisitions which require data communications include the architectural provisions of this instruction and local implementations are incorporated into the base communications plan.

b. Base Telecommunications, Long haul and afloat communications requirements are submitted to COMNAVTELCOM in accordance with references (a), (b) and (d).

c. Data communications strategies for individual Information Systems are developed in accordance with the architectural guidelines in enclosure (1).

d. Architectures developed for specific mission areas use enclosure (1) for continuing interoperability.

8. Report. The reporting requirement contained in enclosure (2) is exempt from reports control by OPNAVINST 5214.7.

Laurence Layman
LAWRENCE LAYMAN
By direction

Distribution:
SNDL A (Navy Department) (Less A6)
W (Department of the Navy Echelon 2 Activities)

Copy to:
SNDL FL1 (COMNAVDAC) (Code 813, only) (35)
MARCORPS Code H plus 7000067 (20)
CNO (OP-09B)

Stocked:
CO, NAVPUBFORMCEN
5801 Tabor Avenue
Philadelphia, PA 19720-5099 (100 copies)

Navy Data Communications Control Architecture

Enclosure (1)

TABLE OF CONTENTS

TABLE OF CONTENTS (Continued)

LIST OF FIGURES

TABLE OF CONTENTS (Concluded)

1.0 INTRODUCTION

Information systems are becoming increasingly dependent upon data communications capacity and capabilities for survival. Emerging technologies elicit different designs and economies. The data communications components of information systems are becoming more important as information systems have evolved from largely stand alone operation, where data communications costs were less than 5% of total system cost, to the large networks of today where data communications costs are in the range of 30% to 50% of total system cost. The end-to-end reliability of information systems is governed more by the communications network environment than by equipment used to provide end user services.

Major support problems have been encountered by Navy information systems. Local, unique solutions applied to specific bases or information systems have surfaced the critical data communications requirements: a problem in one system or area of a country often causes a whole information system or geographic area degradation.

To address this problem, Department of the Navy Information Resource Management (DIRDONIRM) directed the formation of a broad program specifically to address data communications support for information systems in the Navy. The goal of the program is to provide a robust information network available across the Navy, ship and shore alike. Anyone needing Navy information can literally "plug into" the network and get access to information or computer capacity regardless of geographic location. DIRDONIRM called together all Navy commands with a primary interest in providing that support to develop a data communications architecture.

An architecture is a world view or picture that is commonly accepted by all parties. As a document, this architecture contains the present coordinated picture of the technical and managerial resources, and facilities to be provided in the 1995 and beyond timeframe. The most critical dynamic surrounding the architecture is the process; i.e., how it is to be used. Some aspects such as international standard protocols and use of the Defense Data Network (DDN) have been mandated by higher authority. Other aspects such as common base cable plant and standard building wiring are commonly accepted. Major problem areas or "holes" such as security and network management become apparent and cause projects to be started to develop specific areas of the architecture. Information systems also start modifying their approaches to getting data communications support. As these processes unfold, the architecture must be updated and changed to the emerging world view. New "holes" appear and projects start to address the emergent issues.

The world of data communications has been divided into four parts based upon the responsibilities: base, long haul, ship-to-shore, and shipboard. The base communications environment is made up of several component systems. The DON base telecommunications systems, to include the DON NTCCs, are the management responsibility of NAVTELCOM. Both NAVTELCOM and NAVDAC have planning responsibilities associated with their respective missions, a part of which is the identification of the base commander's requirements. In order to provide a complete and integrated picture of the total information system/data communications/telecommunication requirements of the base commander and to maximize economies of scale, a Base Information Transfer System (BITS) Requirements Identification and Planning Program has been initiated. Under this program NAVDAC has the management responsibility of identifying and planning for the base commander's requirements associated with NAVDAC's mission area and, as an agent for and in coordination with NAVTELCOM, the requirements associated with NAVTELCOM's mission area. Once identified, NAVTELCOM will determine the system design necessary to meet the requirements within the confines of the architecture. The DDN which connects bases together for long haul data communications is managed by the Defense Communications Agency (DCA) with Navy coordination performed by NAVTELCOM and interfaces by NAVDAC. Ship-to-shore is managed by NAVTELCOM with shipboard equipment provided by the Space and Naval Warfare Systems Command (SPAWAR). The shipboard equipment is provided by SPAWAR with Naval Sea Systems Command (NAVSEA) participating especially in ship construction issues. This architecture looks to these commands to provide assistance and authority.

The initial architecture effort has developed a baseline. An initial examination of each environment indicates radically different problems and perceptions. For example, voice and data upgrade requirements for base and pier support continue to be identified for integration into BITS. although DDN connectivity is available, a Navy implementation plan to support fleet data communications requirements and capabilities needs to be addressed. In ship-to-shore area, there is no common consensus on requirements or concepts so the architecture concentrates on developing issues. Shipboard capabilities to significantly upgrade pier support and directly connect to the Navy Telecommunications System (NTS) are encouraged. The ship-to-shore section will drive many information systems of the future and needs immediate attention.

The Navy Data Communications Control Architecture (NDCCA) will become the baseline for enhancing the transfer of decision/mission support data between afloat and shore-based information systems and information systems users. This section of the report provides an overview of the situation and the purpose, scope, and objectives of the NDCCA. Also provided are a brief outline of the background leading to development of the NDCCA, and the responsibilities for accomplishing this effort. Section 2.0 provides a description of the control architecture. Sections 3.0 through 7.0 provide a brief summary of the NDCCA architectural segments (Afloat, BITS, Long Haul Communications, Security, and Protocols).

1.1 Overview

Naval units must be continually ready to achieve their assigned mission whether it be on land (Marines), at sea (Surface or Sub-Surface), or in the air (Navy Air). One of the keys to mission success is providing accurate and meaningful information to the right person at the right time in order to make effective decisions. Information systems are critical tools in today's command and management environment for providing the data upon which decisions can be formulated. They help to:

a. Maintain control over weapons and forces.

b. Provide intelligence about enemy intentions and capabilities.

c. Provide warning of attacks or hostile actions.

d. Aid in countless other tasks such as decision/mission support (the principal topic of this architecture) which are needed to sustain today's Navy.

The mission can suffer unless each element of the communications system works together to move information quickly and effectively to decision makers. All of the communications circuits, computers, terminals, people, and other elements must work in a cohesive fashion. Cohesiveness doesn't just happen. Careful planning and management are necessary in order to ensure that individual system elements fit within an overall systems framework.

One view of the overall Navy information system data communications picture is that of a set of operational environments which must interoperate in order for information to pass among the spectrum of Navy information systems and information system users. As shown in Figure 1-1, these operational environments include the Navy base/port facilities both in Continental United States (CONUS) and overseas, the Navy tactical forces, and the Navy usage of the long haul Defense Communications System (DCS).

Currently, the lack of interoperability between these environments causes significant bottlenecks and hampers the flow of decision/mission support data. Building cohesive, interoperable systems is a difficult technical challenge which is further complicated when the systems must withstand the stresses of crisis and conflict. The responsiveness and effectiveness of Navy information systems can be improved by:

a. Increasing system interoperability by reducing the barriers between system components which hamper the timely and effective flow of information.

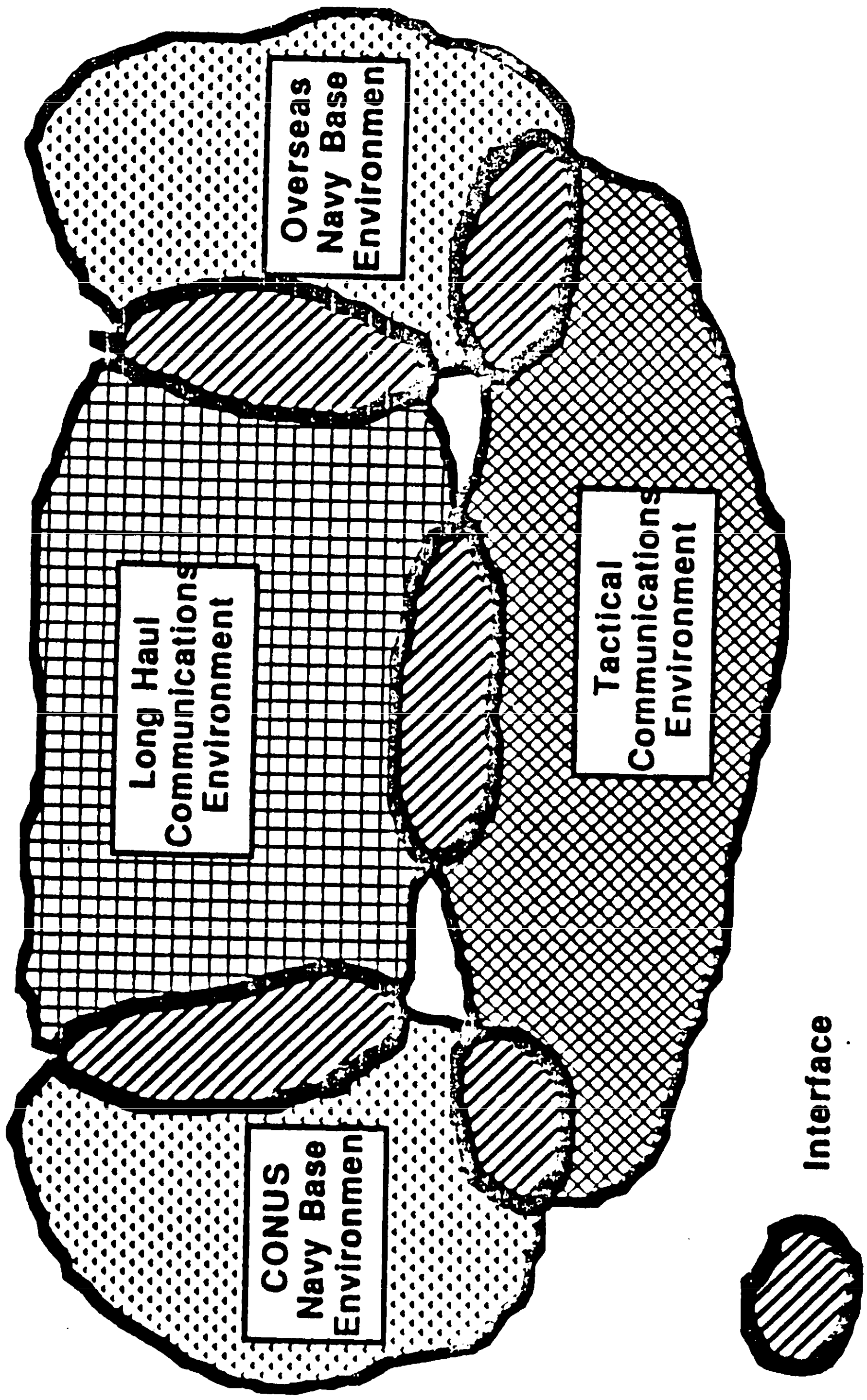


Figure 1-1
Operational Environments

b. Exploiting technology by developing a clear framework to shape technology introduction while effectively using the capabilities of existing systems.

c. Achieving cost savings by reducing duplication of effort and achieving more effective use of common-user systems.

Currently, there are several architectural efforts on-going within the Navy, as shown in Figure 1-2, which are closely inter-related: the Department of Navy Information Resource Management (DONIRM) sponsored NDCCA with its Afloat, BITS, Long Haul, Security and Protocol Sub-architectures; the SPAWAR Warfare C^2I Systems Architecture, with its Communications Support System (CSS) Sub-architecture and the NAVTELCOM Telecommunications System Architecture.

It might appear at first that these architectural efforts are separate and distinct, however, upon more detailed examination it has been identified that both the C^2I and decision/mission support information systems share common data communications resources over the telecommunications system. Another facet of the situation is that the NTS was designed to provide voice and data communications for the fleet including ship/shore exchange. The limiting factor has been transmission capacity to meet all the needs. Finally, the designated DOD data communications system, DDN, is continuing to evolve and expand to meet an ever increasing number of users. There are significant issues associated with capacity, cost, rate of expansion, and, in some cases, ability to properly fulfill the requirement. Continued examination of this situation will be accomplished.

1.2 Purpose

The purpose of the NDCCA is to provide:

a. A top down framework for developing the relationships and interfaces between key elements.

b. A unifying concept for influencing near term programs and long term evolution.

c. A vehicle for developing policies, standards and guidelines which apply to subordinate programs and systems.

d. A reference source for Navy managers as well as information and communication system planners and developers.

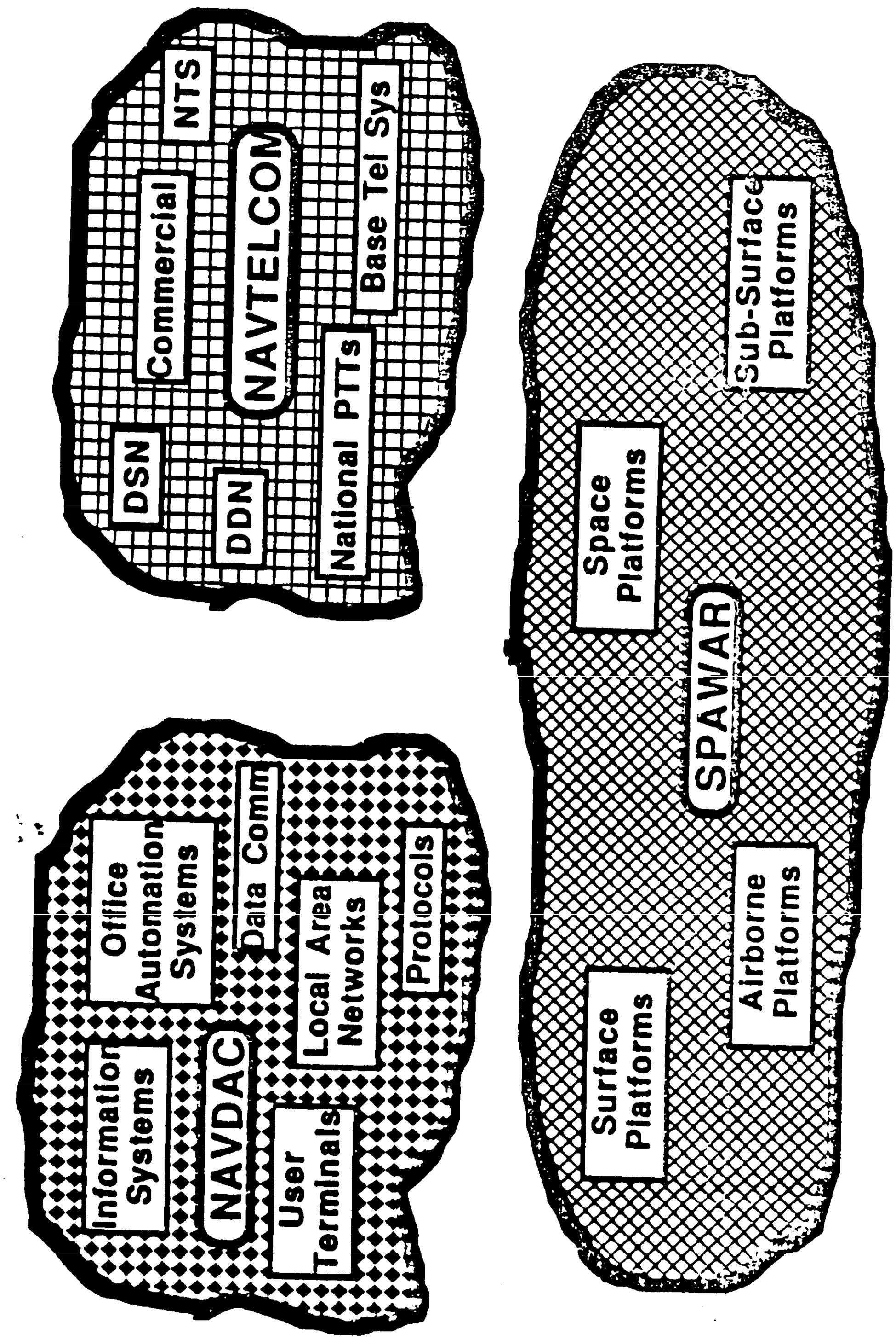


Figure 1-2
Architectural Efforts

As it evolves, the NDCCA will also summarize the overall architectural concept, provide Navy-wide goals and objectives, establish specific guidance, and reference other documents which provide additional details applicable to individual information and communication system elements.

1.3 Scope

An underlying theme of this architecture is that decision/mission support information systems, weapon systems, and C^2I information systems, support the Navy mission afloat. With this in mind, this architecture is intended to be used in conjunction with on-going efforts by SPAWAR and NAVTELCOM, as shown in Figure 1-3. The melding of these efforts should provide an in-depth understanding of the relationships and needs of the Navy and enhance the overall data communications posture.

1.4 Objectives

The NDCCA will include all decision/mission support information systems data communications needs as well as related areas such as DDN and base telephone service. The NDCCA will not include the Navy message system except for information systems interfaces to the NTS for support of the afloat segment of the architecture. Coordination with the ongoing SPAWAR and NAVTELCOM architectural efforts is also a key objective of the NDCCA.

The Navy Data Communications Control Architecture will:

a. Describe the overall Navy information and related communication systems framework and summarize the relationships between subordinate programs, systems, subsystems, and elements.

b. Identify the key policies, standards and guidelines which are needed to influence near term information and related communication system development decisions and to shape long term evolution.

c. Define the essential attributes and key features required of all Navy information and communication systems to ensure consistency with overall objectives.

d. Establish guidance which will facilitate evolution of more responsive, more modular, and more cost effective systems.

1.5 Background

In 1986, the Navy requested The MITRE Corporation to analyze the Navy process of planning data communications. The results of that analysis indicated that a top level architecture was needed to describe the overall

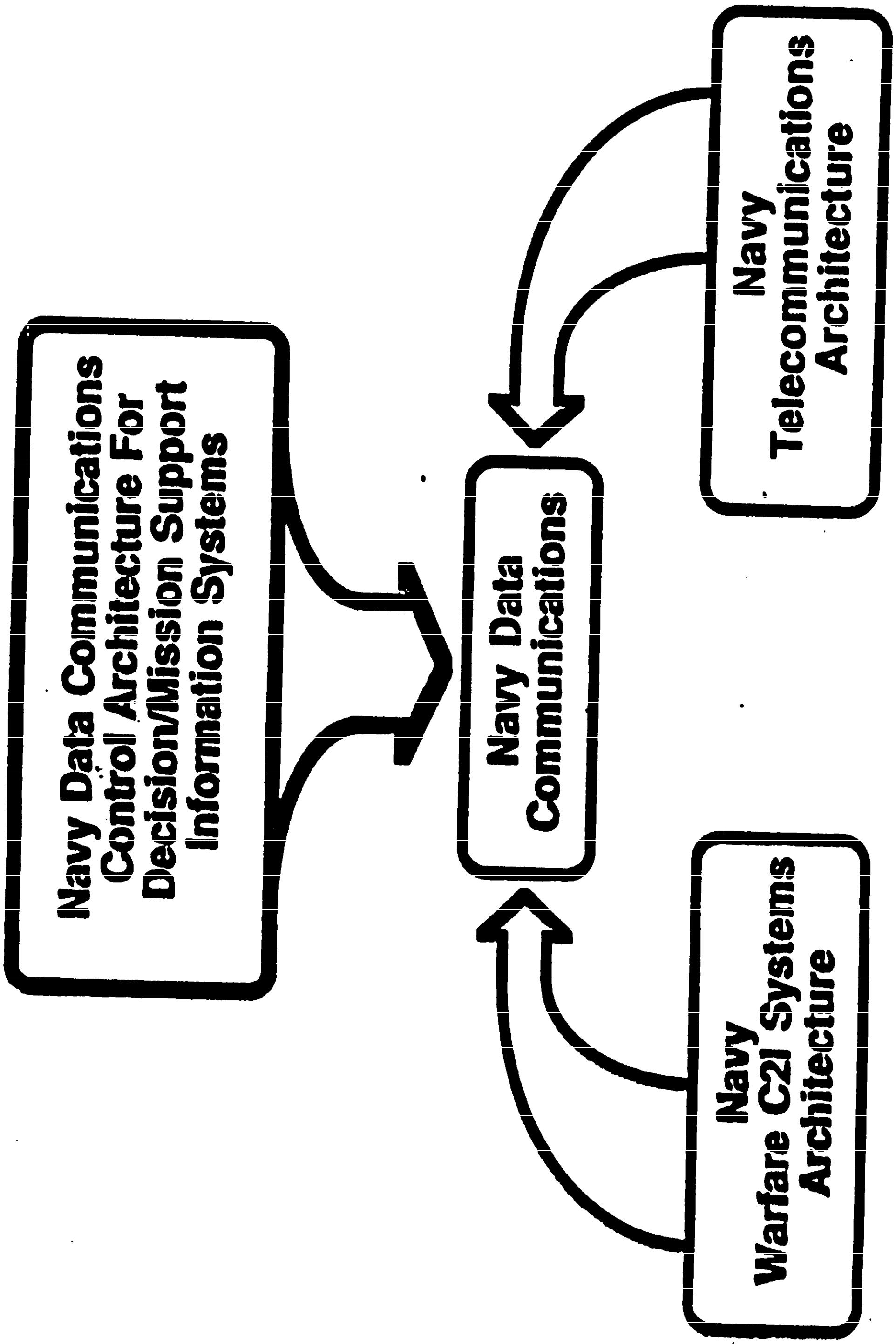


Figure 1-3
NDCCA Scope

systems framework for Navy data communications, to identify and promulgate standards and policy to influence system development decisions, to define the essential attributes and key features of the overall target system, and to establish guidance for future evolution. The architecture was to include Department of Defense (DOD) efforts such as the Integrated Services Digital Network (ISDN), Security, the Government Open Systems Interconnection Profile (GOSIP) and the DDN.

During the third meeting of the Navy Data Communications Users Group (NDCUG) on 10-12 February 1987, a top-level structure for the NDCCA was promulgated as the framework within which the more detailed architecture was to be developed, as shown in Figure 1-4. The original framework indicated four subordinate architectural segments; BITS, DCS, Shipboard, and Ship-to-Shore. Because of their close relationship, the shipboard and ship-to-shore segments of this control architecture were later combined into a single Afloat architecture segment. Later, during an Afloat Core Group meeting, a third category, ship-to-ship, was added to the Afloat segment of the NDCCA. As the control architecture evolved, two other segments (Security and Protocol) were added in order to properly address these key data communications issues.

The major issues confronting Navy data communications, as promulgated during the NDCUG meeting in February 1987, were of two types: technical and managerial. Some of the technical issues cited were:

a. The proliferation of non-interoperable systems.

b. The existence of very different communications environments.

c. The lack of resource management.

d. The limited media capacity/availability.

The principal management issue that developed from this meeting regarding Navy data communications was the fragmentation of data communications developments which can be traced to a lack of central direction.

1.6 Mission Responsibilities

DONIRM directed the development of the NDCCA, guided by a set of working groups each devoted to one of the major segments of the architecture as shown in Figure 1-4. The control architecture specifies the components, their interfaces, and the management structure for the implementation. The top-level components, interfaces and responsible agencies for the architecture are depicted in Figure 1-5. The following paragraphs delineate some of the specific responsibilities of the organizations/commands.

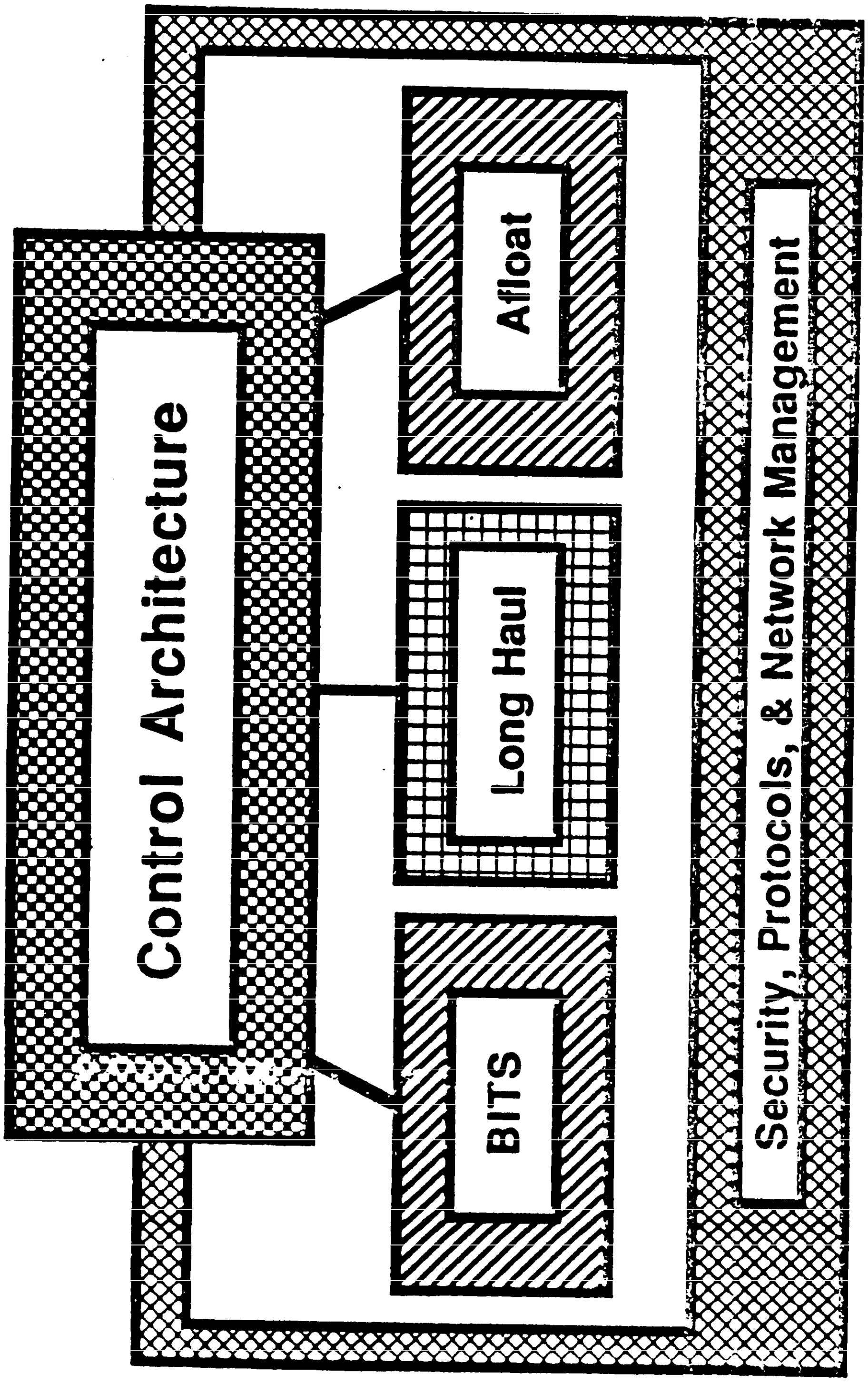


Figure 1-4
NDCCA Elements

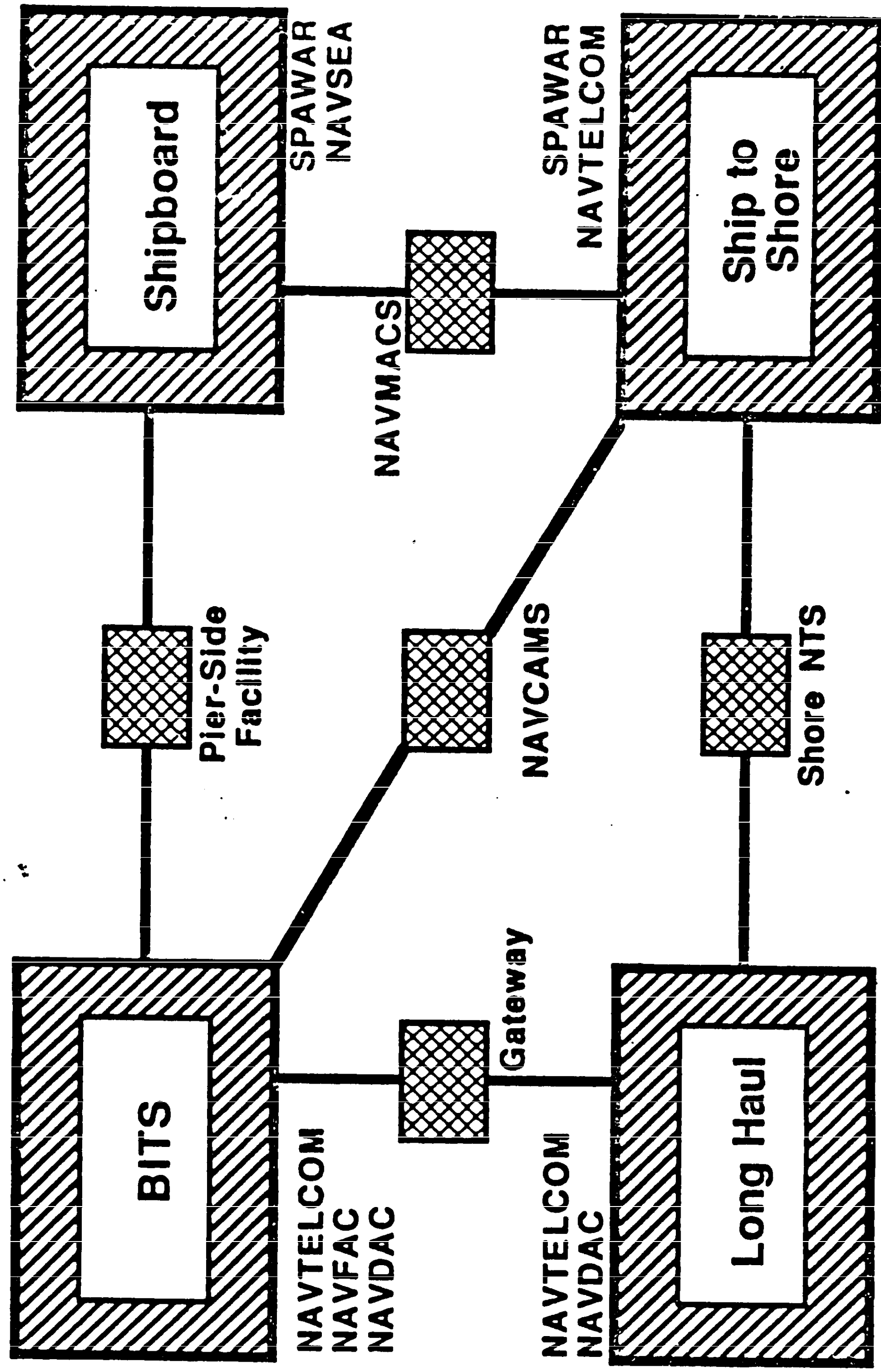


Figure 1-5
Organizational Responsibilities

Responsibility for development of the NDCCA and its sub-architectures was assigned to the NAVDAC. NAVDAC's overall responsibilities include information resources architectural and management support to the Chief of Naval Operations (CNO), as well as planning and budget oversight for information systems within its mission area. NAVDAC is the information systems support architect.

NAVTELCOM's responsibility includes planning, configuration control, budgeting, material resource support, readiness, operations, maintenance, and management support for the NTS as well as Defense Communications Agency (DCA) coordination for the Navy to include DDN and all long haul communications services, dedicated lines, and commercial packet switch services. The Navy Commercial Communications Office (NAVCOMCO), as a field activity of NAVTELCOM, provides oversight management, policy development, and standards for Navy base administrative telephone systems, a type of information system technology, for shore-based Department of Navy (DON) activities worldwide. NAVCOMCO is also responsible for long haul circuit ordering, commercial long distance and has the functions and responsibilities of the DON Telecommunications Certification Office (TCO).

Naval Facilities Command's (NAVFAC')s responsibility is to provide major Navy base construction, to include buildings and communications facilities. NAVFAC maintains central data bases with base-related information, including the Master Activity General Information and Control (MAGIC) file, and the Navy Facility Assets Data Base (NFADB). NAVFAC's Engineering Field Divisions maintain digital base maps for areas under their geographic cognizance on the Graphics Engineering and Mapping System (GEMS).

SPAWAR's responsibility is to provide material and technical support (acquisition and life cycle support) for space systems, Command, Control Communications and Intelligence (C^3I), Electronic Warfare (EW), and undersea surveillance; and to provide force warfighting architecture and requirements integration among total Naval battle forces. SPAWAR also provides program management for the SNAP program.

2.0 CONTROL ARCHITECTURE

This section of the report provides an overview of the control architecture. Provided herein is a brief description of some of the architectural perspectives which need to be considered in developing the architecture. This is followed by a description of the current situation with regard to Navy decision/mission support information system data communications, a description of the target architecture as developed, to date, and interim scenarios/actions which are of potential use in solving some of the near term problems.

2.1 Architecture Perspectives

User information systems are growing rapidly. Users expect Navy information and communications systems to provide responsive, accurate, effective, and affordable support to their needs. Ever increasing demands for information at all levels of management have created new problems for every Navy organization. Users must cope with a flood of information and must have effective tools to gather, store, maintain, and distribute or communicate it to others for their use.

Strategies are needed to guide the evolution of Navy information and communications systems and provide more effective support to mission needs. The relationship of the architectural perspectives to the NDCCA operational environments is depicted in Figure 2-1. The following paragraphs describe the services, environmental factors, and attributes of the information and communications systems, and provide evolutionary guidance for the establishment of the NDCCA.

2.1.1 System Services

System services are the general Navy data communications needs and key characteristics. The system services reflect a composite of the opinions of the organizational members of the Afloat and BITS Core Groups and do not, necessarily, identify fleet validated requirements in the development of the architecture.

2.1.1.1 File Transfer. This service, also referred to as bulk data transfer, is used to send large volumes of raw data or reports from one location to another. Normally, the process is initiated by a user or automated request and queued for transmission. The quality of service is typically measured by throughput speed and reliability. The files to be transferred are commonly in character, binary or facsimile data format, although, in the future, new data types are expected such as graphic or pictorial images.

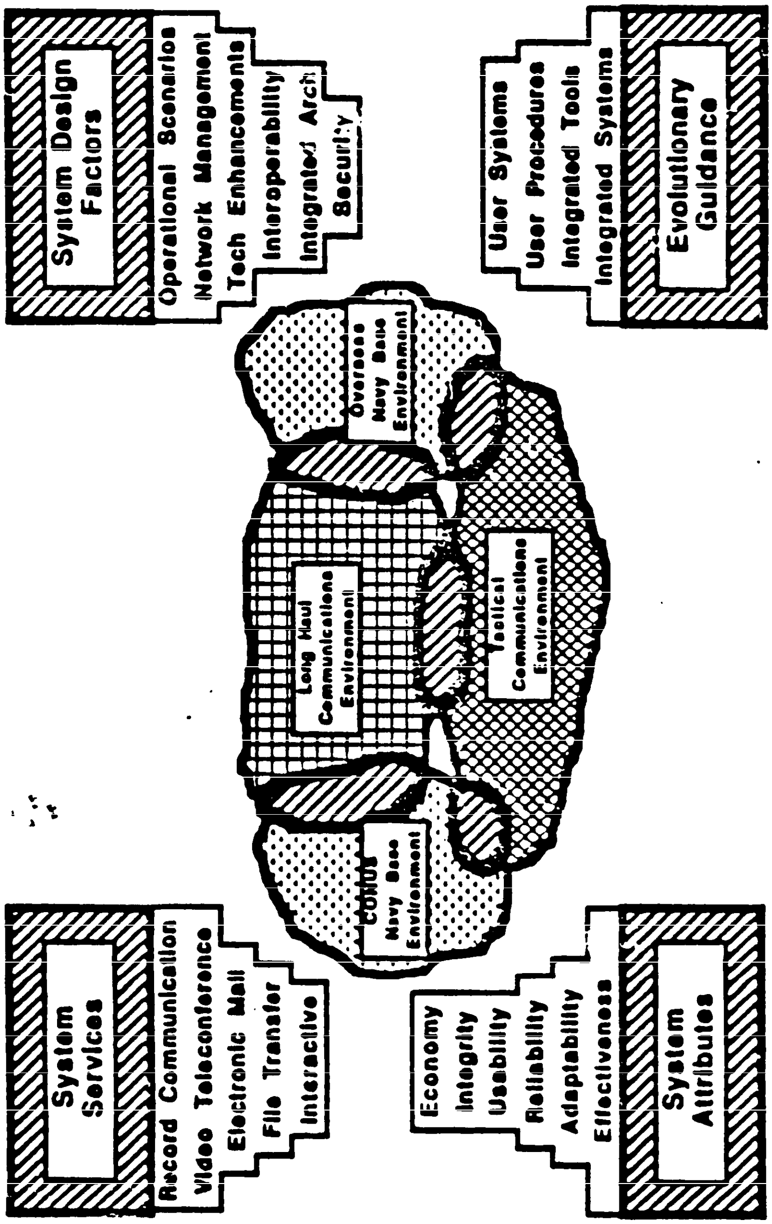


Figure 2-1
Architectural Perspectives

2.1.1.2 Interactive. This service, also referred to as transaction processing, is used when a terminal user or host computer process desires information from a host processor. The interaction is characterized by the user composing a "line" or "screen" query, sending it to the host for processing, and getting a response. This mode is used for most end user applications. The quality of service is typically measured by response time and reliability. The data format is commonly either character or graphics.

2.1.1.3 Electronic Mail. This service is used when informal messages are composed by a user and sent upon request to one or more locations for review or use by a recipient. The quality of service is typically measured by ease of composition and editing, ease of addressing, accountability, and transmission efficiency. Typical applications are informal office memoranda such as meeting arrangements or commenting on documents.

2.1.1.4 Video Teleconferencing. This service literally means a conference using telecommunications. In a data communication environment, teleconferencing means that information composed by any participant is broadcast to all participants or a designated subset. The quality of service is typically measured by the clarity of the visual image and/or the amount of distortion.

2.1.1.5 Record Communication. This service is used to send formal, highly structured and formatted messages which are composed by a user to one or more recipients or organizations. The quality of service is typically measured by the time of writer to reader service, accountability, security, message integrity, and retention for possible retransmission. Typical applications are the transmission of directives, orders, or formal requests for response or action.

2.1.2 System Design Factors

The following system design factors reflect a composite of the opinions of the organizational members of the Afloat and BITS Core Groups and are meant to identify areas of consideration in the development of the architecture.

2.1.2.1 Network Management. The system design must support both centralized and decentralized network management, control and standard operating procedures. These are necessary to sustain network operations under stress, to assist in fault identification, isolation and repair, and to minimize manpower and training requirements. Protocols should be available which use minimum host and data communications resources under selected circumstances.

2.1.2.2 Integrated Architecture. The system design should allow automatic invocation of pre-planned use of resources when confronted by situations of reduced resources. The precedence system provides such a mechanism; however, problems arise when this concept is used universally in automated systems. The problem is magnified when information systems are involved; the data cannot be easily "read" and decisions to send data are often determined indirectly or without human intervention.

2.1.2.3 Interoperability. The system design should allow interoperability of data communications systems. Interoperability addresses the issues of how well different systems work with each other. Two dimensions need to be addressed: media and applications. Interoperability should also address how well Navy systems work with joint service and allied systems.

2.1.2.4 Security. The system design must allow for incorporation of security aspects. Security involves many considerations including management of risk, unauthorized disclosure of sensitive information, vulnerability to disruption either through denial of service or information distortion, and proper as well as authorized use of resources. DOD security technology is far more extensive than equivalent commercial systems both in type and strategy. The extent of DOD security and security commitments to military Allies have no direct commercial equivalent. National Security Agency (NSA) guidance on network security should be a primary reference.

2.1.2.5 Technology Enhancements. The system design must allow for the migration to new technology. Examples of new technology include data compression methods, automatic communications system reconfiguration (robustness), integration of voice and data, and increased ability for High Frequency (HF) communications.

2.1.2.6 Operational Scenarios. The system design should include scenarios such as military operations of ships at sea with stressed or blacked out communications. The ability of data communications capabilities to survive enemy attack and continue service is critical. The availability of data communications systems for administrative purposes during such periods is also critical. The system design should include strategies to achieve an acceptable level of administrative data communications survivability for some hierarchy of information requirements yet undefined. Administrative data communications circuitry should have restoration priorities assigned in accordance with current National Command Authority (NCA)/DCS procedures.

2.1.3 System Attributes

The most important consideration in integrating information and communications systems is to ensure that the mission essential needs of the tactical operating and supporting forces are satisfied. These mission essential needs must be supported throughout the spectrum of operational environmental conditions. System integration must also be capable of providing responsive, accurate, effective, and affordable support to these forces. Mission needs, threats, current capabilities, performance requirements, emerging technologies, cost, and schedules must be considered during the integration process.

2.1.3.1 Effectiveness. Mission critical requirements for information must be satisfied throughout the spectrum of operational environments (peacetime, crisis, and conflict). The principal factors of the effectiveness attribute are: readiness, supportability, survivability, sustainability, surge capacity, planned redundancy, and sensitivity to priorities.

2.1.3.2 Reliability. Information and communication systems must be available for use when and where required and must provide consistently reliable services. The principal factors of the reliability attribute are: availability, robust design, fault tolerance, and maintainability.

2.1.3.3 Usability. The system must provide a basis for assessing the degree of user satisfaction with information and communication system services. The goal to achieving usability is providing a single system to users regardless of application or geographic location. The principal factors of the usability attribute are: appropriateness, quality, timeliness, ease of use, and responsiveness.

2.1.3.4 Integrity. Users must trust systems to ensure the integrity of the information supplied and to follow consistent procedures. The principal factors of the integrity attribute are: accuracy, security and privacy, and auditability.

2.1.3.5 Adaptability. It is essential that the system incorporate design features which help ensure the responsive support to changing user requirements. The principal factors of the adaptability attribute are: modularity and interoperability.

2.1.3.6 Economy. Mission needs must be satisfied at the lowest total overall life cycle cost to the government. The principal factors of the economy attribute are: productivity, and affordability.

2.1.4 Evolutionary Guidance

Information and communication systems and services must appear to a user as a cohesive set of tools which provide reliable and effective service as needed. To establish this set of tools, the following evolutionary guidance has been developed.

2.1.4.1 Integrate Systems into User Environments. Information and communication systems must be designed and installed as a cohesive part of the user work environment. Sometimes called office automation, this approach is equally applicable to command posts, tactical environments, and any work area where users require IS access.

2.1.4.2 Provide Integrated Tools to End Users. Most users now require access to several different information handling tools or services. As more flexible user-oriented resources become available, this trend will accelerate.

2.1.4.3 Integrate User Systems with Network Services. End users must have access to all the information needed to get their job done.

2.1.4.4 Establish User Procedures to Manage Data. Information which is distributed to end-user work areas may be inaccessible to other users who need it. Effective management of data becomes increasingly complex.

2.2 The Current Situation

For decision/mission support information systems support, Navy data communications is physically separated between information and message processing systems, as depicted in Figure 2-2. It is anticipated that in the future the functions of DDN and the Automatic Digital Network (AUTODIN) will evolve to a single system. Command and Control systems utilize the same communications media. A separate effort from this and the Command and Control Architecture will discuss coordination between the two architectures for optimizing utilization of communications assets. On the individual Navy bases, independent users and office automation networks are not, for the most part, interconnected. Data traffic is processed through the DCS-DDN where a DDN host processor is currently available, or in some cases through one of the public data networks for some independent users or groups of users. Dial up service to the DDN is available on some user terminals. Navy message data is processed through the AUTODIN system via the Local Digital Message Exchange (LDMX) in the local base Naval Telecommunications Center (NTCC) or through the Navy Communication Processing and Routing Systems (NAVCOMPARS) at one of the four Navy Communication Area Master Stations (NAVCAMS) and at Naval Communications Station (NCS) Stockton. A ship in port has the option of using the base Navy Communications Station (NAVCOMSTA) for its traffic or maintaining its communications guard and communicating as if it were still at sea as in the case of an Aircraft Carrier (CV).

The method of passing data between shore-based and shipboard decision/mission support information systems is either by mailing magnetic tapes or written reports, or by encapsulating the data in a Navy message format for transmission over the NTS. Neither of these methods provides a totally satisfactory solution. The mail is, for the most part, too slow, causing accuracy and timeliness problems in ashore/afloat data bases.

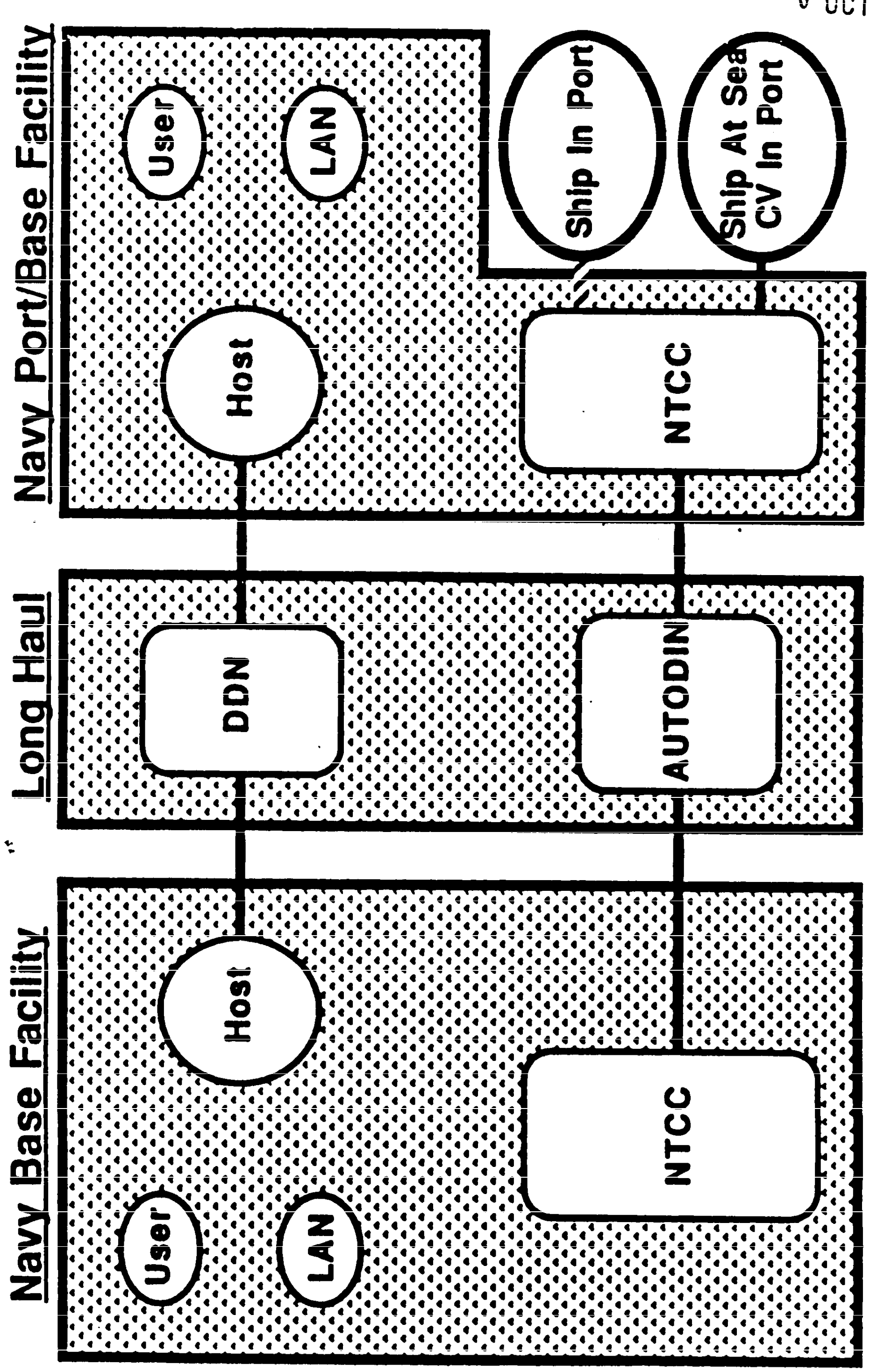


Figure 2-2
Current Situation

Within the NTS, High Frequency (HF) transmission has low capacity and propagation induced errors. Tactical satellite systems provide high data rate capability but system capacity is limited and fully utilized by command and control systems. Because of this, low precedence decision/mission support data can be delayed causing problems in information system data accuracy. Navy command and control systems are supported by dedicated data communications systems which provide real time, data base to data base exchange of information.

Data communications for a ship in port is also limited. Present methods are hand delivery of magnetic tapes or Optical Character Reader (OCR) formatted messages between the ship and local base facilities. In many cases the magnetic tapes as well as written reports are mailed at the port facility to their addressees due to the sheer volume of data or lack of interface capability.

2.3 The NDCCA Target Architecture

The target architecture is a totally integrated ISDN capability both for shore-based and afloat ISs and IS users, as depicted in Figure 2-3.

The migration of the DCS common-user data systems toward a system of Integrated Data Services (IDS), is a part of the target architecture evolution. At the most basic level, IDS can be viewed as a value-added data exchange server which builds upon raw transmission facilities and services to provide data exchange services to the system users, operators, and managers. The International Standards Organization (ISO) reference model for Open Systems Interconnect (OSI) provides a basis for the IDS architecture which includes: access services provided by the OSI network layer, transport services provided by the OSI transport layer, and high-level services composed of application processes and processes in the OSI session, presentation, and application layers. In addition to these data services, IDS includes security services which ensure that data will not be compromised during the use of the data exchange services, and support services which give additional support to system users to facilitate the use of the data exchange services. IDS also includes the operations and management functionality needed by the IDS system manager for successful operation of the IDS system.

The BITS program to improve the individual Navy base voice and data capabilities addresses the problems associated with local and long haul data transfer between shore-based information systems. Installation of digital base switches at the individual bases could provide the capability for shore-based information systems and individual users to communicate on an automated basis, on either an intra or inter base level through the DDN or in some cases other public switched networks. BITS development will include pier extensions that will allow a shipboard host computer facility

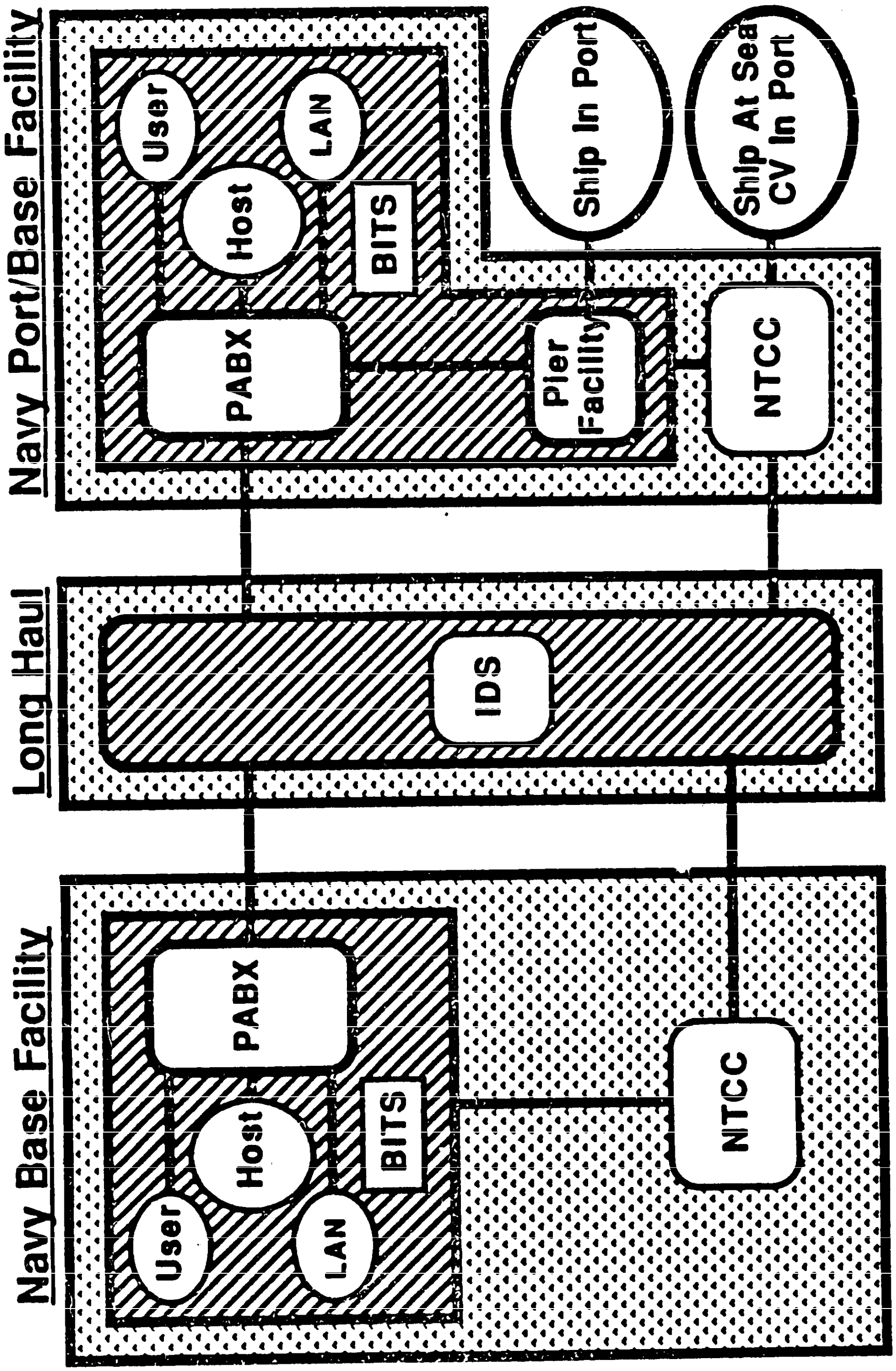


Figure 2-3
NDCCA Target Architecture

and/or terminal direct interconnection into a DDN host. This pier facility will act as another building on the base, providing a wiring closet for connection of multiple customers (ships in port) to the DDN or local transmission plant.

The target architecture period may also see the advent of multilevel secure transmission facilities in the long-haul network both for information systems and to support the Navy message handling requirements.

It is envisioned that some form of interface will be provided between the BITS and NTCC.

2.4 <u>NDCCA Interim Scenarios/Actions</u>

Interim scenarios/actions for the NDCCA target architecture will be addressed in detail in the specific segment architectures.

For the afloat information systems and information system users, upgrades are being developed and programmed to provide relief, on a short term basis, to some of the more significant deficiencies such as the current interfaces between systems and the elimination or reduction of the congestion problems.

For the shore-based information systems and information system users, planning will continue toward eventual implementation of the total BITS capability. The primary tasks for the interim period will be the identification of specific requirements and services, and the programming and budgeting of resources to accomplish the BITS implementation.

Improvements in the long haul portion of the architecture will be characterized by migration of the DDN to OSI data transmission protocols and consolidation of the separate networks of the DDN using a multilevel security architecture.

3.0 AFLOAT SEGMENT ARCHITECTURE

The results of the Fleet Workshops (CINCLANTFLT - 23-25 March 1987, CINCPACFLT - 20-24 April 1987) and the Afloat Core Group meetings (5-6 March 1987, 11-13 May 1987) provided an overall summary of current data communications system capabilities and established a number of issues to be addressed in the Afloat Data Communications Architecture (ADCA).

This section of the NDCCA will summarize the current situation and target architecture regarding the NDCCA Afloat segment. Next, some interim scenarios will be examined which will provide relief to current problems.

3.1 Afloat Current Situation

While at sea, the ship's transmission means for decision/mission support information system data communications to and from shore are satellite and high frequency via.NAVCAMS/NCS, as shown in Figure 3-1. The data must be in Navy message format for transmission and handling. For ship-to-ship data communications, satellite, high frequency, and line of sight transmission systems are available. Again, the data must be in Navy message format. For this architecture, ship to ship is considered a special case of ship-at-sea communications.

While in port, the ship's primary transmission media for decision/mission support information system data communications to and from shore are the local communications services provided by a NAVCOMSTA or NTCC. Large ships such as CV's are an exception as they maintain their communications guard as they would while at sea. General Service (GENSER) message traffic provided in OCR format is delivered by ships in-port to a local message center for retransmission via shore-based systems. Maintenance, logistics and supply information are delivered to either the local Navy Regional Data Automation Center (NARDAC) or Navy Supply Center (NSC) for processing and/or retransmission/mailing. Magnetic tapes or written reports can also be used if the data is to be mailed to the shore-based information system.

The shipboard data communications capability has been separated from the discussion of ship-at-sea, ship-to-ship, and ship-in-port, primarily because the ships have different capabilities depending upon type. The main concern of the architecture is that the shipboard capabilities interface and interoperate with shore-based systems whether the ship is at sea or in port. As shown in Figure 3-2, while at-sea the primary capability for decision/mission support information system data communications is through the Navy Modular Automated Communications System (NAVMACS) computer, which in turn is a part of the ship's communications facility. Currently, the data communications is handled in Navy message format and is processed by providing the message to the shipboard communications center in paper tape format.

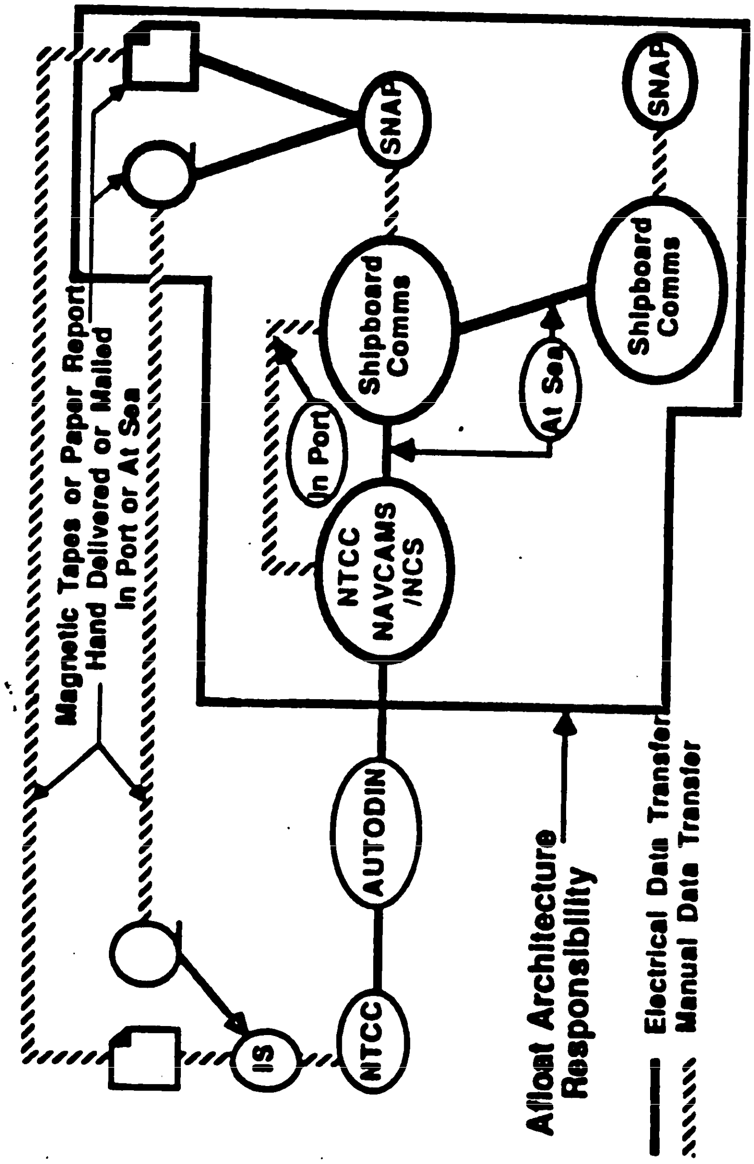


Figure 3-1
Afloat - Current Situation

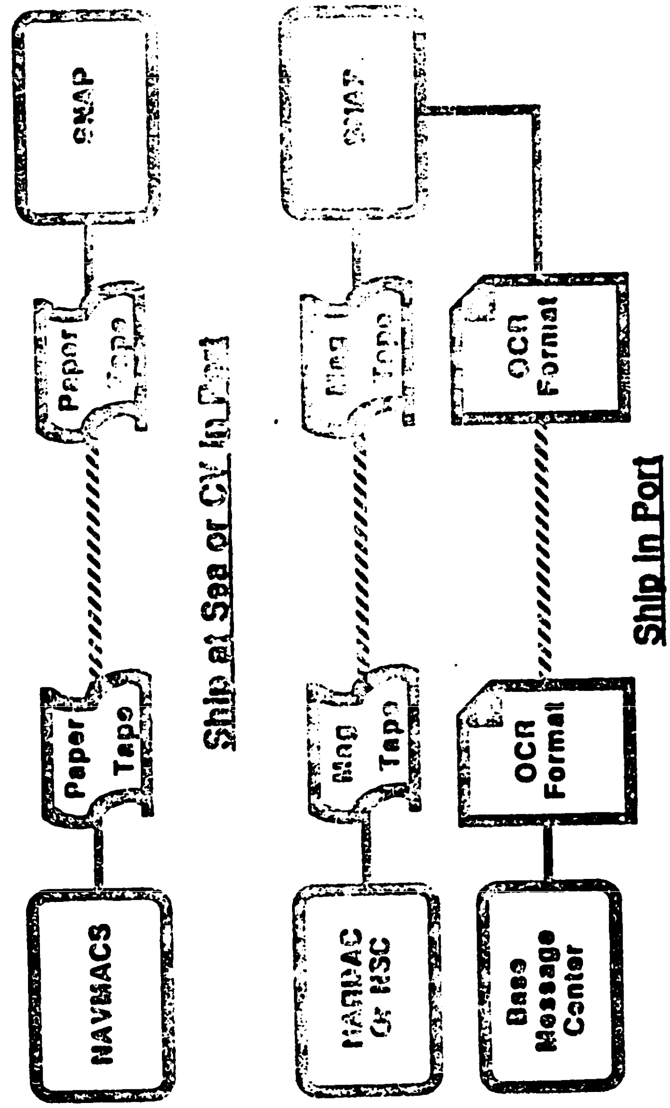


**Figure 3-2
Shipboard Current Situation**

3.2 Afloat Target Architecture

In communications and information systems the distinction between tactical and non-tactical, C^2I and decision/mission support, is disappearing. There is a need for an integrated ship/shore approach, under the control of the fleet and operational commanders, adaptable to operational situations such as EMCON, and including ship-to-ship communications alternatives.

The ship-at-sea data communications target architecture is primarily concerned with investigating the implementation opportunities for technology improvements within the communications and information systems themselves, and with determining the potential of developing better operational concepts for data transfer. Figure 3-3 depicts the target afloat architecture within the target control architecture framework. Some of these potential technology opportunities include implementing data compression techniques, using existing and planned commercial systems to augment the NTS, and providing automatic communication system reconfiguration. The target architecture could subsume all data communications, decision/mission support and C^2I, in a single, comprehensive structure. This will require a composite understanding of all information system requirements and needs throughout the spectrum of deployed operational scenarios (peacetime, crisis, and conflict), and coordination with the on-going architectural efforts being accomplished by SPAWAR and NAVTELCOM.

The target architecture for ships in port is to by-pass the existing NAVCAMS/NAVCOMSTA structure for file transfers and establish a direct connection from the ship's decision/mission support information systems to the DDN. This will be possible once the BITS capability has been added to the Pier/Base facilities. In order to develop such a capability a plan should be developed in the interim period for such a connection at the Pier. A capability to expand the system services to allow interactive data communications and electronic mail between shore-based information systems and the ship's automated information systems will be possible once the direct connection to DDN is available. The advent of DDN service directly to the ship will surely be available during the target architecture period and plans for its implementation should be formulated early.

SPAWAR has initiated long term actions to accomplish improvements to the shipboard data communications capability in the target architecture period. These include a direct connection between the Shipboard Non-tactical ADP Program (SNAP) and NAVMACS computers, and connection to a shipboard Local Area Network (LAN) for transfer of all data traffic on board/to/from the ship. The direct connection between SNAP and NAVMACS is undergoing analysis as not all NAVMACS configurations have a port available, and there are some potential security problems. The shipboard LAN concept would have the communications center act as the network

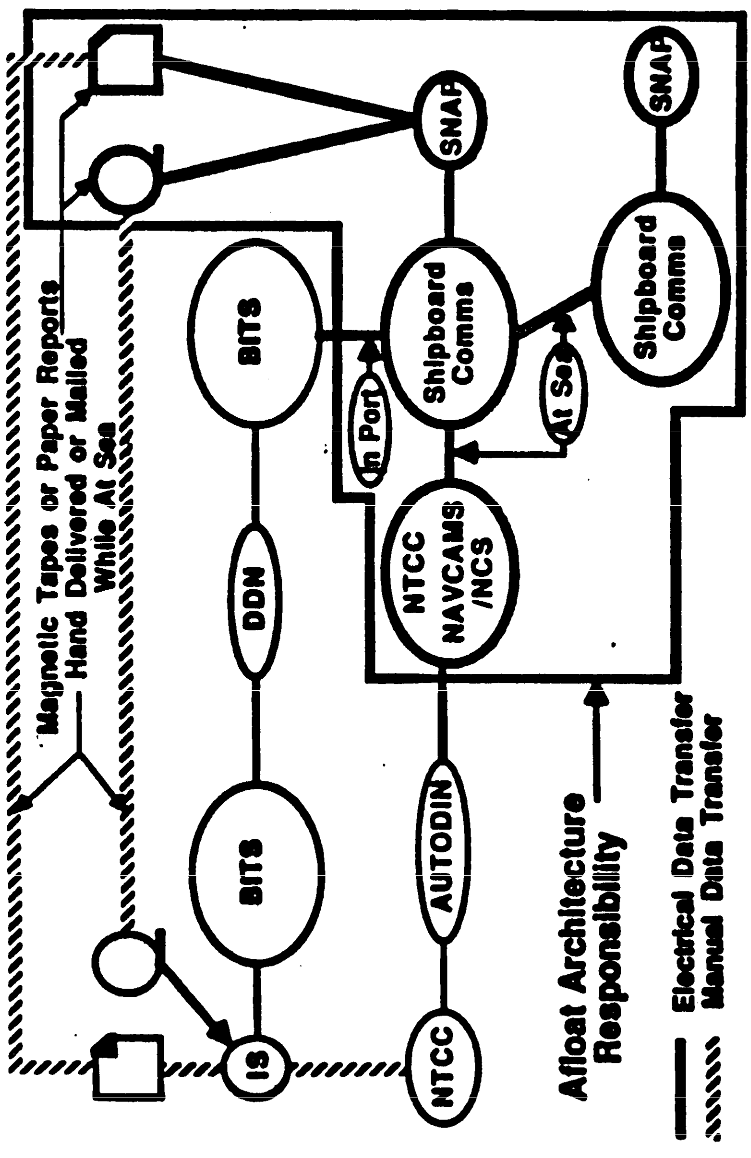


Figure 3-3
Afloat - Target Architecture

controller and manager. This is not a new concept but its implementation requires much additional study prior to any implementation being considered.

3.3 Interim Afloat Scenarios/Actions

This section provides some of the potential opportunities for improving the current situation on an interim basis. While not all of these interim scenarios or potential actions are recommended to be a part of the target architecture, they will provide improved operational capabilities.

The primary issues in the current situation are that the volume of data to be passed between ship and shore is too large to be handled within a short period of time by electronic means, and that there are saturation problems both ashore and afloat which create choke points for data traffic. Other issues are also in need of corrective action, such as the proliferation of non-interoperable systems and system interfaces. There is a need to address these problems not only for the target architecture but also for the interim period.

3.3.1 DAMA Capability

Demand Assigned Multiple Access (DAMA) capability is already programmed for implementation in the FLTSAT system. This capability should, if properly implemented, provide some relief in terms of data throughput by allocating the channels in use between ship and shore and allowing some form of priority to be implemented with regard to message and traffic types. Other methods to increase throughput capacity of the FLTSAT system, such as increasing the data rate of individual channels and actual channel assignment, could also be investigated for their impact and potential.

3.3.2 Shore-Based Automated Screening Process

An interim solution to relieve decision/mission support message traffic congestion ashore could be the development of an automated screening process for the NAVCOMPARS. This process would determine the preferred method of decision/mission support traffic transmission to ships via information systems thus providing congestion relief on NTS tactical data support circuits. It would also perform any necessary format conversion(s), assign message traffic priority and sequence, and monitor message transmission status. It filter would operate under the direct control of the NAVCOMPARS site and would be transparent to C^2I data transmission requirements.

3.3.3 Submarine To Tender Data Transfer

Potential opportunities for improvement to the ship-to-ship communications capability do not appear to be readily available except for transfer of data from a submarine to a tender while being serviced. The submarine/tender interim solution would be a floppy disc or magnetic tape interface between the SNAP computer to the tender data processing system. This would eliminate the need for manual transfer of work orders and requisitions, and allow the submarine to prepare the data in advance using the facilities available on the SNAP system. It would provide time savings, improve accuracy, and reduce current inefficiencies.

3.3.4 SNAP To DDN Connection

Currently under operational test on SDSA prototype ships, is a capability to dial-up a DDN connection when the ship is in port to allow it to receive its mail from a designated host off the DDN network. The ship can also send data into the network using this same connection. Although workable and useful, this does not provide a broad range of capability. It has demonstrated, however, that a direct connection to DDN is within the realm of capabilities to be further investigated and utilized. For the interim a more sophisticated capability is needed, and potentially available, either from a direct connection from the ships SNAP computer to an existing shore based information system with a DDN access capability, or through shore-based, designated SNAP hosts having direct access to DDN.

3.3.5 SPAWAR - SNAP Upgrades

SPAWAR has already initiated several actions to improve shipboard data communications. Paper tape processing within the NAVMACS will be automated requiring less if any operator intervention by development of a micro computer front end for both the SNAP and NAVMACS computers. This will allow for exchange of messages on magnetic media (floppy disc) and eliminate the punched paper tape interface. For in port capabilities the SNAP is to be modified to allow computer output of messages in DD-173 OCR format. A longer term action to provide a direct connection between the SNAP and NAVMACS computers on all ships has been identified for detailed analysis and implementation if approved.

3.3.6 COMNAVTELCOM Upgrade Efforts

COMNAVTELCOM has a number of communications support upgrade efforts underway. The Fleet Routing Indicator (FRI) concept provides a unique 3 character name for each ship and component to simplify addressing and message processing, and, initially, to manage the flow of fleet traffic within the DCS and ashore NTS. New procedures and equipment are being fielded to increase the reliability of HF equipment and correct transmission errors in messages from the fleet prior to distribution to shore activities. Manual interfaces and use of paper materials, including the pervasive use of paper tape are being phased out.

4.0 BITS SEGMENT ARCHITECTURE

The results of the BITS Core Group meetings (10-12 March 1987 and 9-10 June 1987) provided an overall summary of current data communications system capabilities and established a number of issues to be addressed in the BITS Data Communications Architecture. Through discussions at these meetings it became clear that the 4th generation PABX switches included in NAVCOMCO's plan could be configured to operate as a LAN. Correctly configured, these switches could provide an option for a modern, cost effective, high-bandwidth communications system that would satisfy some of the current and future office automation data transmission requirements.

This section of the NDCCA will summarize the current situation and target architecture regarding the NDCCA BITS segment, and highlight BITS architecture related activities.

4.1 Current Situation

The existing Navy base communications capability consists of separate networks having very little if any interoperability, as shown in Figure 4-1. The current Office Automation Networks (OANs) provide data communications capability for select users sharing a subset of common database information. Data communications between Navy base facilities are provided by a local DDN host(s). File transfer and electronic mail are the principal services provided via the DDN, although not all OAN users have access to the long haul network on an automated basis. Message traffic transmission is provided by a local NTCC using an LDMX or Standard Remote Terminal (SRT) with direct connection to the AUTODIN network, or via a Remote Information Exchange Terminal (RIXT) homed to an LDMX. Local telephone service is provided by the base telephone exchange or Private Branch Exchange (PBX), with connections to both the DOD Automatic Voice Network (AUTOVON) and commercial telephone networks. For shore-to-ship data communications, the common practice is to mail bulk data using a magnetic tape media.

4.2 BITS Target Architecture

The basic BITS topology integrates data transfer into the base cable plant using base switches provided for base support. A potential solution for base switch upgrades to satisfy this topology could be the use of fourth generation digital PABX's. BITS sites would be connected by gateways and bridges through a DCA long haul network, as shown in Figure 4-2. This backbone system would allow terminals connected to outlying discrete LANs to be connected to other nodes in the system using standard software protocols.

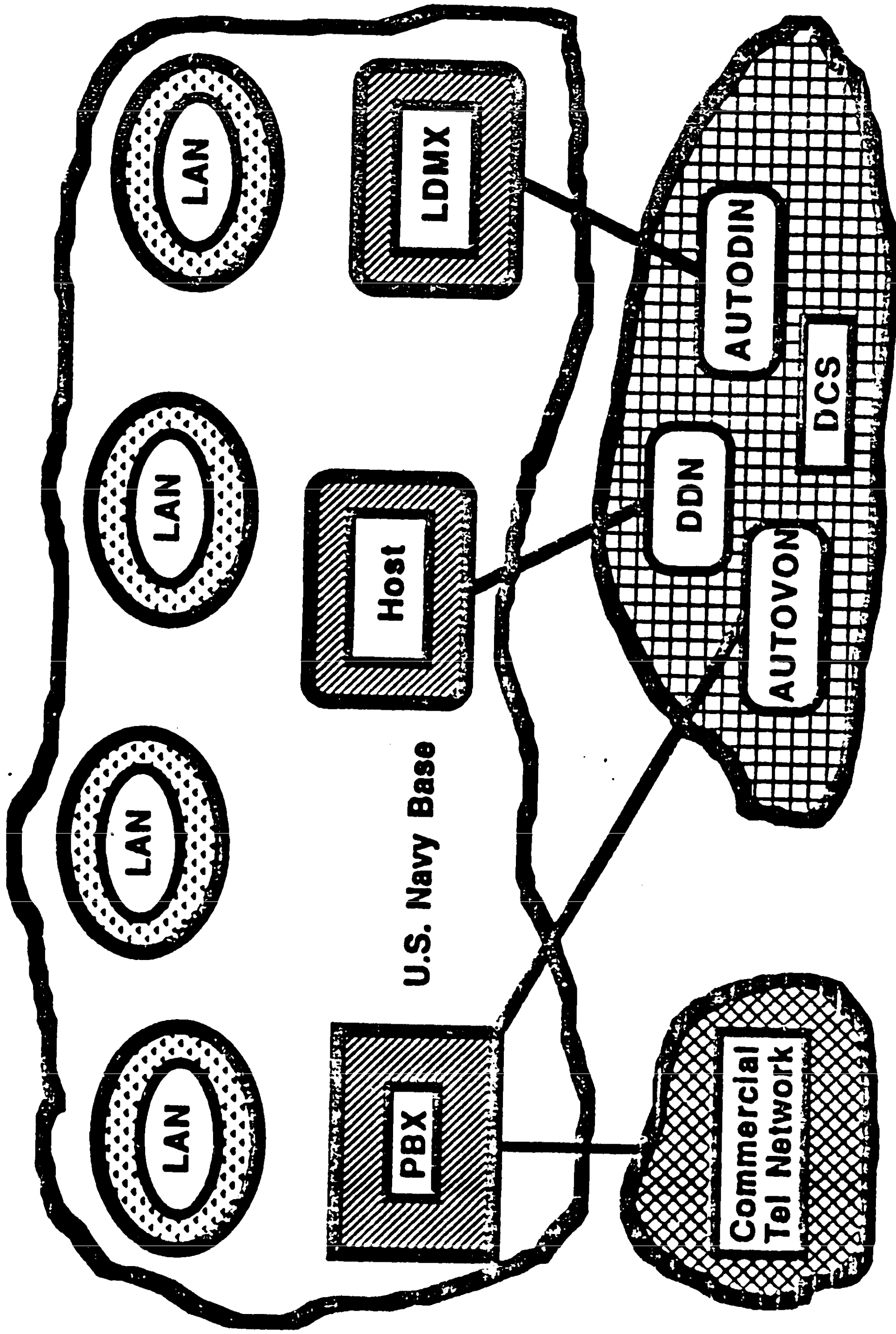


Figure 4-1
BITS Current Situation

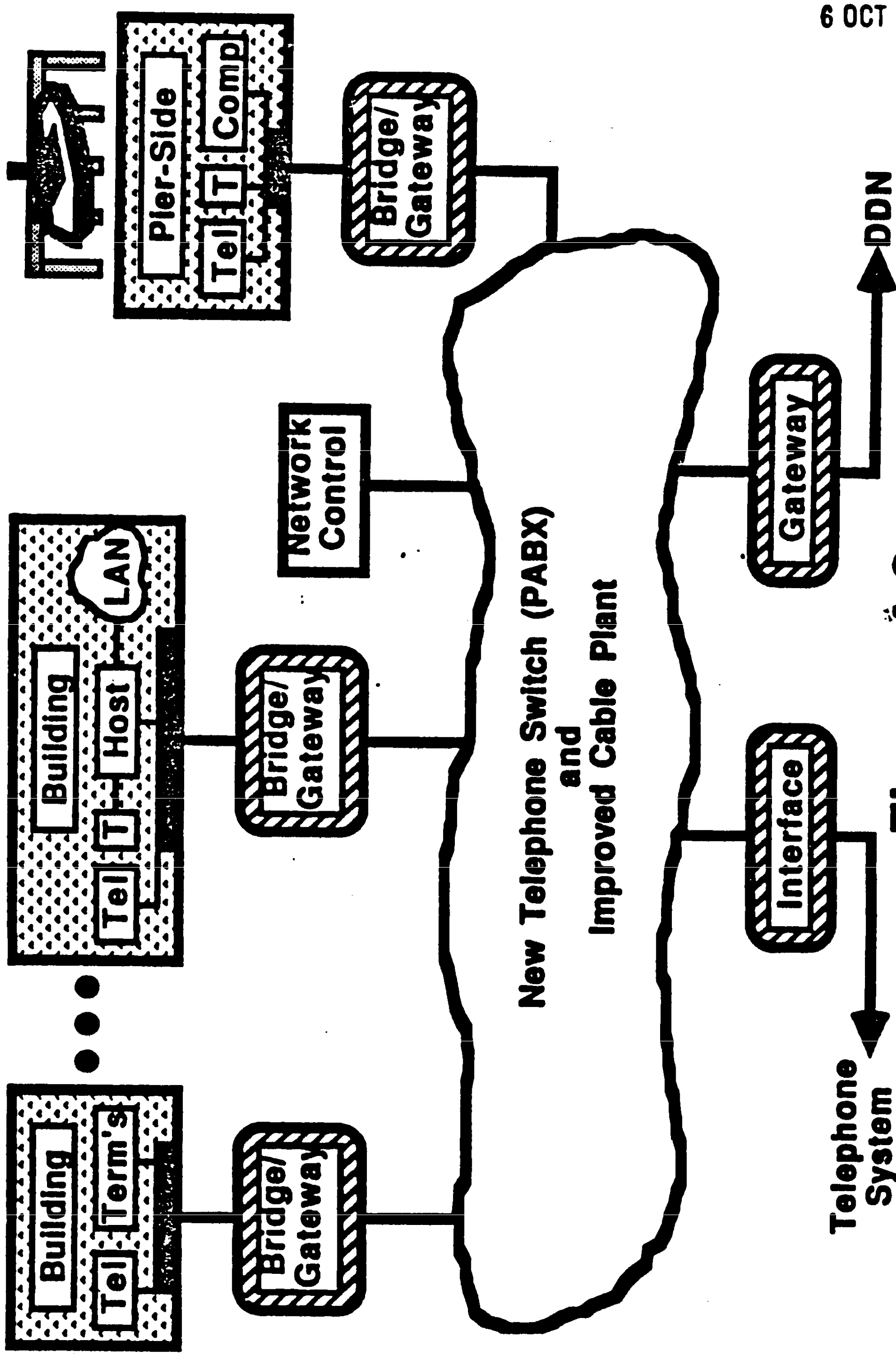


Figure 4-2
BITS Target Architecture

Intrabase communications can be supplied over a base or geographical planning area by connecting all users to a base switch. This connection can, in many cases subject to the requirements for competition, use the existing copper twisted pair cable plant that has been previously installed for telephone communications. If an upgrade is deemed necessary, a fiber cable from the switch to the wiring closet of the building can be considered. The physical and link layer protocols being offered by switch manufacturers today allow 64 KB full duplex digital data transmission over the copper twisted pair. This will provide more than sufficient bandwidth to user terminals. Most of the protocols are similar to the 2B + D ISDN protocols and will comply fully with the standard when it is approved. The various user equipments connected to the network must use approved standard protocol suites for interoperability. The ISDN backbone may be augmented by various LAN strategies to satisfy unique requirements. Networks having dissimilar characteristics will require gateways or bridge elements for connections to the base switch. The number and kinds of connections required would depend on each installation and on what existing services must be included in the network..

Interbase communications between geographical planning areas, that meet the minimum distance requirement for connection to DDN, would be connected to DDN through a gateway. This gateway will perform several functions; flow control, routing table and algorithm maintenance, and protocol translation providing connections for all on-base hosts and terminals for off-base access.

Pier-side communications between a shore-based system and a ship in port presents unique requirements that are unlike the base-to-base communications requirements, in some respects. Delivery procedures for data and narrative correspondence to ships (at-sea or in-port) will continue to be accomplished using current NTS procedures upon full activation of DDN ashore. The NAVCAMS will continue to be responsible for delivery of message traffic to the ship underway or in-port. A modification to the ships' guard shift message will be required to identify the ships' pierside connection into the DDN when a ship shifts it's communications guard ashore. The NAVCAMS will then use this information to update the data base to ensure proper delivery of correspondence transmitted electrically to the ship. The pierside communications will consist of possible connections to a base switch with sufficient bandwidth to accommodate the voice and data requirements of the ship in-port.

The ultimate target architecture for the Navy BITS program is ISDN. The BITS architecture being developed must be upgradable to or compatible with ISDN. For years, network architects have been touting the completion of ISDN, proclaiming it as the way of the future. The future is here and there exist some implementations of some of the ISDN standards although they are still not complete. Many vendors are trying to guess what the full set of standards will be and move in front of the rest of the market place by going ahead now and offering products that are close to the ISDN standard. These products will be upgraded to the standard when it is approved.

4.3 BITS Architecture Related Activities

4.3.1 BITS Model

This architecture uses a hierarchical arrangement of switches at the local or base level with a second level of switches at each building. Long haul communications is supplied by the DDN or other public data networks. A small sample section of the network used for modeling purposes is shown in Figure 4-3. The model shows interoperability between an existing source routing IEEE 802.5 Token Ring LAN and an IEEE 802.3 broadcast Carrier Sense Multiple Access with Collision Detection (CSMA/CD) network at another location. The topology demonstrated here is from one base to another base. The topology required to transport data from a base to a pier-side connection is similar to the base to base scenario.

4.3.2 Integration of Voice and Data - ISDN

All communications vendors are building equipment consistent with the ISDN. The result will be more capacity, local and long haul. In addition to voice and data, many services such as teleconferencing, more direct dialing options, knowing who is calling, and vibrant voice messaging systems will be available. The proper design of the BITS base switch will allow the migration to and inclusion of ISDN standards, which is the goal of the DoD communications plans. The adoption of a digital base switch architecture would obviate the need for procurement and installation of discreet copper or fiber based LANs. Two efforts are underway now, a Telephone Modernization Program to upgrade telephone switching facilities, and the BITS to develop base information system data communications plans. These efforts are now being integrated at the planning level to fully exploit the technology.

4.3.3 Network Management

All successful networks eventually evolve to strong, central management who oversees and assigns resources to maintain the highest level of readiness possible supplemented by local contacts/technicians. When problems arise, the manager has the authority to direct personnel to solve the problems in any area of the country and to assign traffic flow to any circuits available, including alternate routing through other parts of the country including full redundancy/backup of all services. With appropriate management such as is being included in the BITS, the network will become a collection of inter-operating communications systems. Network management

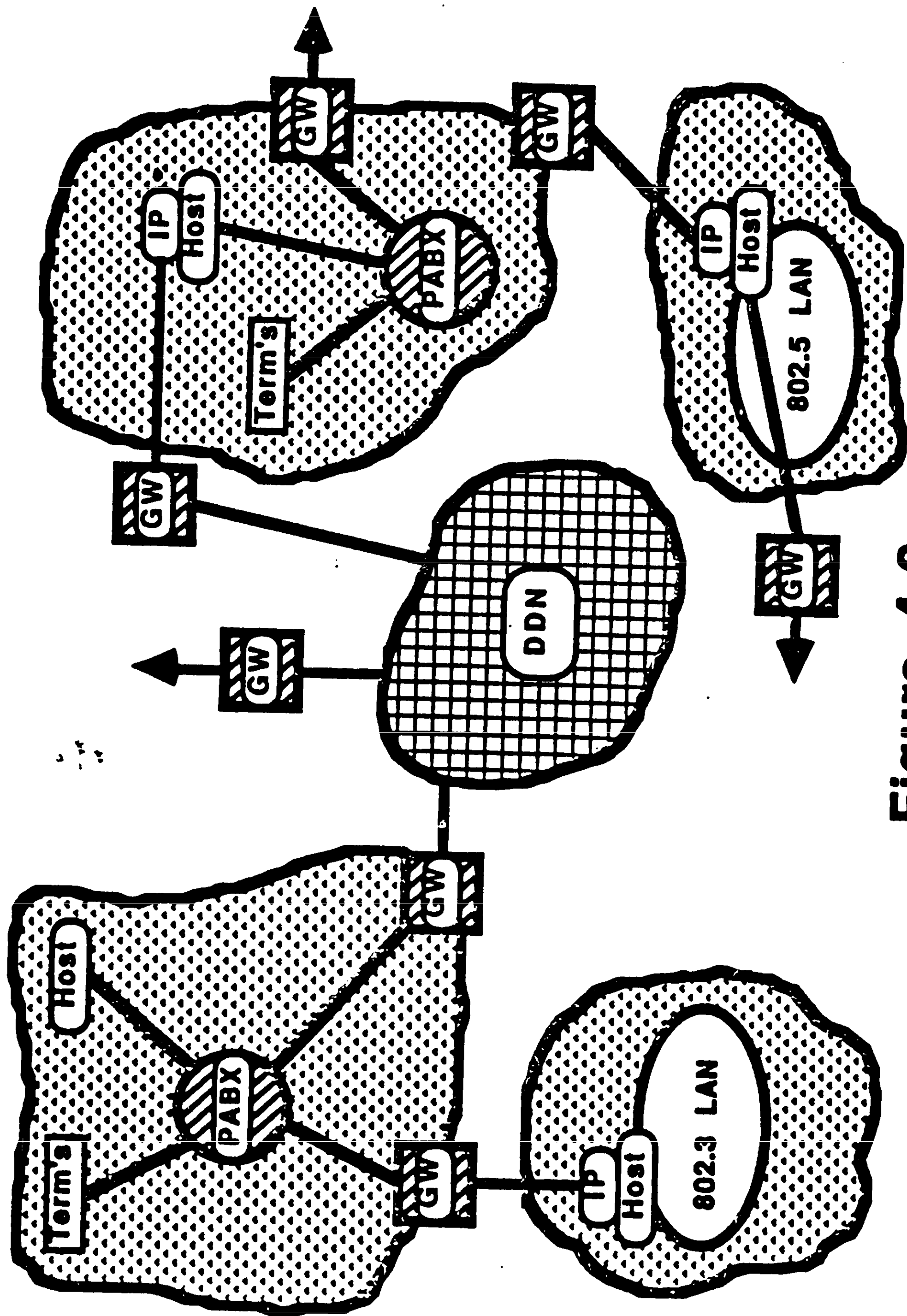


Figure 4-3
BITS Model

will provide services like fault isolation and repair, address assignment, billing information, alternate routing, and collection of statistical data on network performance. Development of a rule-based semi-automatic communications asset management/decision aid to ensure that essential communications (both Command and Control and Mission/Decision Support) are completed in time of high demand is essential for a successful network management structure.

4.3.4 Integrated Base Support Structure

To date, communications information has been maintained by the telephone company and has not been available. With divestiture, the development, operation, and maintenance of user systems became the responsibility of the user. Base communications information is not centrally available or maintained within the Navy. However, other centrally available base related information is maintained by NAVFAC including base geographic maps, building diagrams, and pier support capabilities. As the BITS effort grows, such information will, of necessity, be developed in some form of integrated data base structure.

4.3.5 Pier Support Capabilities

Current pier-side telephone links do not provide sufficient bandwidth or quality to support transmission of shipboard computer data into the DDN. Existing pier-side telephone links must be upgraded, or fiber optic cable in the 100 megabit range must be installed pier-side, to provide proper connectivity into the DDN node ashore. Extensive pier support capabilities are required by the fleet at each port for data interchange. These are being defined and validated to provide the basis for information system and port facilities upgrade.

4.3.6 Overseas Base Support Structure

The implications of overseas support have not been fully explored. Host nation standards, operating and political agreements, as well as physical differences make normal base/station solutions inadequate. Adding to the complexity is the availability of the U.S. DCS and the types of service available to the overseas base facility versus a base in the CONUS. It is expected that the majority of sites can be accommodated in a standard architecture with a minimum number of modifications, however; the architecture needs to address unique issues involved with overseas locations in order to ensure that accommodations are made.

5.0 LONG HAUL SEGMENT ARCHITECTURE

The results of the DCS Comms Core Group meetings (3-4 June 1987, 17 June 1987) provided an overall summary of current data communications system capabilities to be addressed in the Long Haul Data Communications Architecture of the NDCCA.

This section of the NDCCA will summarize the current situation, interim and target architectures regarding the NDCCA long haul segment.

5.1 Long Haul System Description

The current common-user long haul data communications systems are among others the DSN, the DDN and the AUTODIN.

The DDN is a collection of several DOD data networks implemented using Advanced Research Projects Agency Network (ARPANET) technology, as shown in Figure 5-1. ARPANET was originally established by the Defense Advanced Research Projects Agency (DARPA). This network included both DOD operational users and users who were associated with computer networking research prior to its assumption by the DDN program management office. The DDN program split the ARPANET into a community of DOD unclassified users called the Military Network (MILNET) and an experimental network. These two networks are interconnected via gateways and they support only unclassified subscribers. The U.S. European Command (EUCOM) Movements Information Network (MINET) has become a part of MILNET in Europe.

The classified segment of the DDN is a combination of several new and existing ARPANET-like networks. These include the Defense Integrated Secure Network (DISNET) for SECRET system-high general service, and three TOP SECRET (TS) system-high special networks. The TS networks include the World Wide Military Command and Control System (WWMCCS) Intercomputer Network Communications Subsystem (WINCS); the Strategic Air Command Digital Network (SACDIN), and the DOD Intelligence Information System (DODIIS).

Host systems are connected to DDN packet switches using either X.25 or ARPANET (1822) interfaces. Transmission speeds of the host access circuits range from 9.6 to 56 Kbps. The average end-to-end transmission time of a high priority packet across the DDN backbone has been stated in DDN program documentation (Defense Data Network, Defense Communications Agency, p.5.) as about 90 milli seconds with 99 percent of all packets being transmitted within approximately one-half second. This level of performance would support query/response and interactive applications as well as batch or record transmissions. The data transmission protocol standard used in the DDN is the Transmission Control Protocol/Internet Protocol (TCP/IP). These DOD protocols are incompatible with the ISO data transmission protocols.

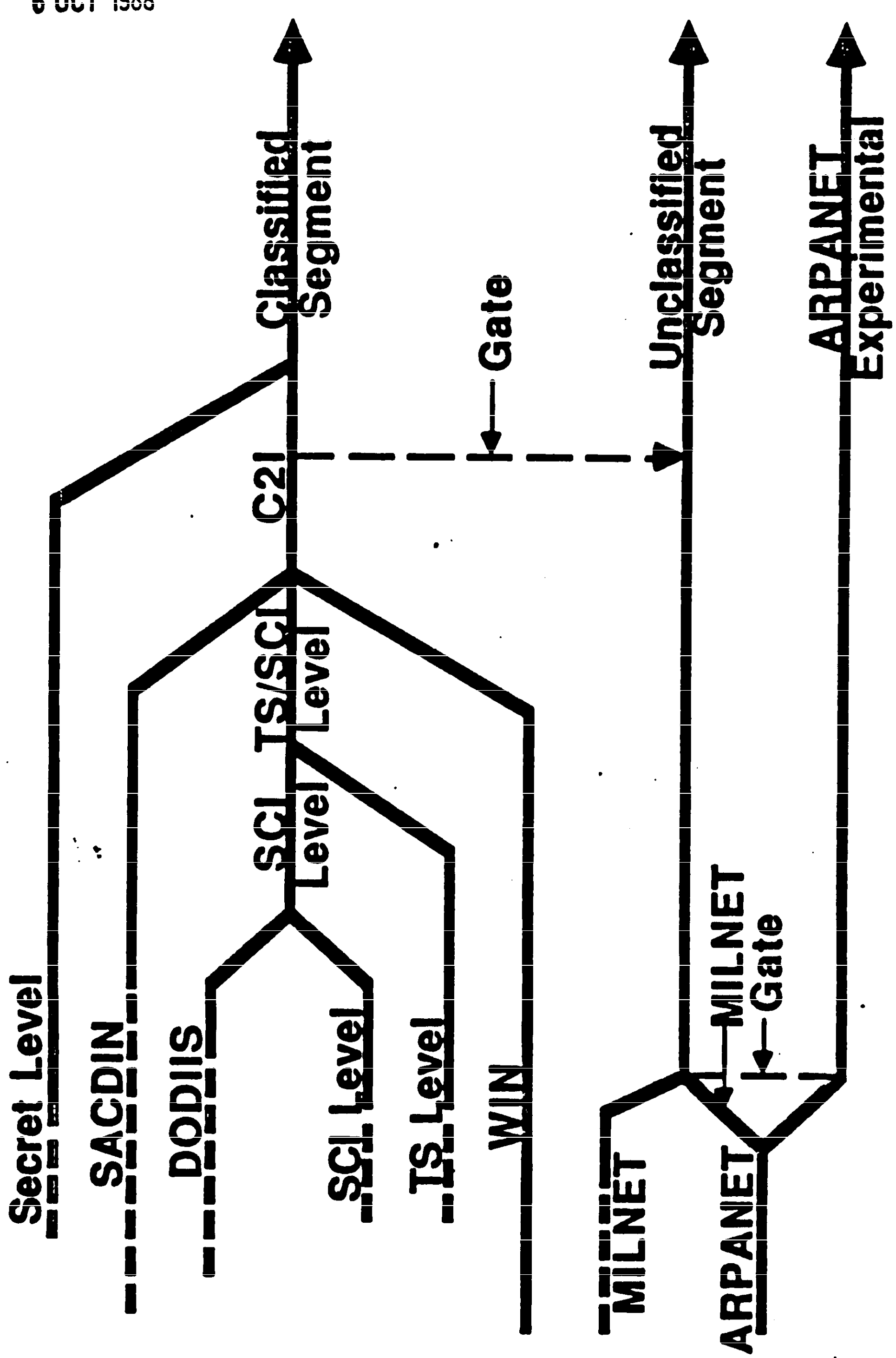


Figure 5-1
DDN Current Situation

A goal of the DDN program is for all networks and security levels to be interoperable. However, at present, technical and security issues prevent this goal from being realized. The current or baseline configuration of the DDN architecture is therefore the organization of isolated networks described above.

One of the primary functions of the DCS is to support the Services and Agencies record data communications requirements. These functions have been supported since the early 1960s, by the AUTODIN system under the management of the DCA.

The AUTODIN Switching Centers (ASCs) and their Inter-Switch Trunks (ISTs) constitute the backbone of AUTODIN and as such, provide an efficient, reliable, secure and automated store and forward DOD message switching network, a sub-system of the DCS. The ASCs were state-of-the-art when designed and via several modifications and expansions which have been incorporated, they have met new requirements, provided enhanced services, and have extended their operating life. However, the ASCs have become increasingly inadequate to support ever expanding requirements for message switching.

5.2 DDN Policy/Guidance

5.2.1 DOD Policy on Utilization of DDN

In April 1982, DOD directed that the DDN be implemented as the DOD common user data communications network. The Office of the Secretary of Defense (OSD) policy issued 10 March 1983, states:

> "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 User Requirements Data Base (URDB). Once registered in the URDB, requests by a Service/Agency for an exception to this policy shall be made to the Deputy Under Secretary of Defense (DUSD) Command, Control and Communications and Intelligence (C^3I). Requests for exceptions for joint interest systems shall be routed to DUSD (C^3I) through the Joint Chiefs of Staff (JCS)."

5.2.2 Navy Policy on Utilization of DDN

A modification of Navy policy for utilization of the DDN is outlined below. From that policy modification there follows a Navy strategy for utilization of the DDN near-term and the utilization of the more general common user data communications services that will be provided by the DCS in the interim and target time frames. The Department of the Navy Information Resources Management (DONIRM) policy regarding DDN utilization states:

> "Navy claimants (DDN "users") are responsible for the planning and completion of connections to DDN for IS's under their purview. All Navy IS's will connect to DDN in compliance with CNO Washington DC message DTG 080107Z Oct 83. Based upon operational requirements a user may request DDN be supplemented (but not replaced) by non-DDN alternatives. IS's requiring interoperability will use the international or DOD standard file transfer protocol to support initial inter-IS data communication requirements.".

5.3 Long Haul Current Situation

Navy policy has supported the OSD mandate to utilize the DDN for all long haul data communications. In October 1983, the Chief of Naval Operations (CNO) promulgated the OSD mandate (CNO, Washington D.C., Message DTG 080107Z, October 1983). Since that time, Navy activities have begun to evolve data communications support from dedicated long lines to the DDN. All Navy informations systems are required to plan for DDN connection. The Navy Laboratories have used ARPANET for many years and are now members of the DDN community. Some ISs, such as the NAVDAC sponsored DCP-40 network, use DDN as trunks for the operational network. Others are ready to connect.

Recent management attention has turned to implementing planned and ordered connections. Navy user connection requirements are contained in the User Requirements Data Base (URDB). The Navy undertook a comprehensive review and revalidation of the URDB submissions of Navy users. This has been completed with the complete Navy data base managed by COMNAVTELCOM with operation delegated to NAVTASC.

Timely connections are now being accomplished. DCA manages all connections to DDN. They have allocated approximately one-third of the scheduled monthly connections to the Navy with the Navy (OP-941) specifying the priority. OP-941 uses validated URDB entries to identify connections to DCA. The connections identified to DCA comply with the system priority list approved by CNO. The process is working well with Navy able to influence DCA management and accomplish Navy objectives.

DDN provides two major but distinct roles; protocol standardization for interoperability and communications capacity, especially for long haul. DOD (DDN) protocol implementations are now available to support most manufacturer host suites and many local area network configurations. Concern is being expressed related to the ability of DDN to satisfy Navy capacity requirements and the resulting cost to users. The Navy position, connecting to DDN with potential augmentation where needed, is generally accepted as the DOD policy position. This strategy provides interoperability with additional alternatives available to reduce cost.

5.4 Long Haul Interim Architecture

The near to intermediate term evolution of the DCS data communications system will be characterized by three principal developments:

a. Migration of the DDN to OSI data transmission protocols.

b. Consolidation of the separate networks of the DDN using a multilevel security architecture.

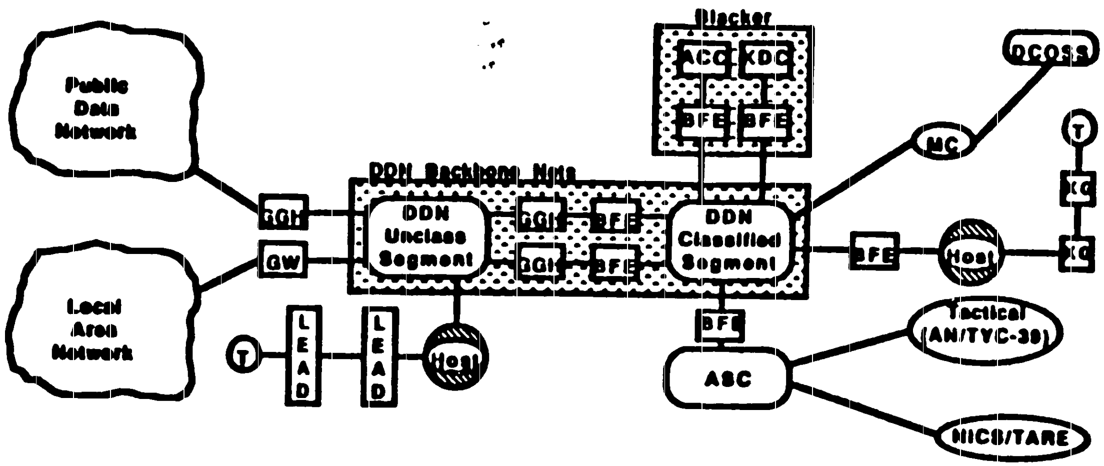
During this interim period the DCS data communications architecture will be as shown in Figure 5-2. The unclassified and classified segments of the DDN have been integrated. The system will use BLACKER devices to implement an end-to-end capability for concurrently supporting multiple, logically distinct communities of interest within a common backbone network.

5.5 Long Haul Target Architecture

In the target (ISDN) architecture, DOD/ISDN will include integrated voice, secure voice, and data services. The user will have a common access point for multiple services. The backbone networks will include the DSN, DDN, and Digital Patch and Access System (DPAS) networks. The linkage among control systems will improve significantly. The ISDN will use different telecommunications modes (e.g., circuit or packet switched connections) to provide a network transport capability for a variety of services. In addition to the transport capability, the ISDN could also incorporate information storage and processing facilities such as teletex, videotex, telefax, and data base services.

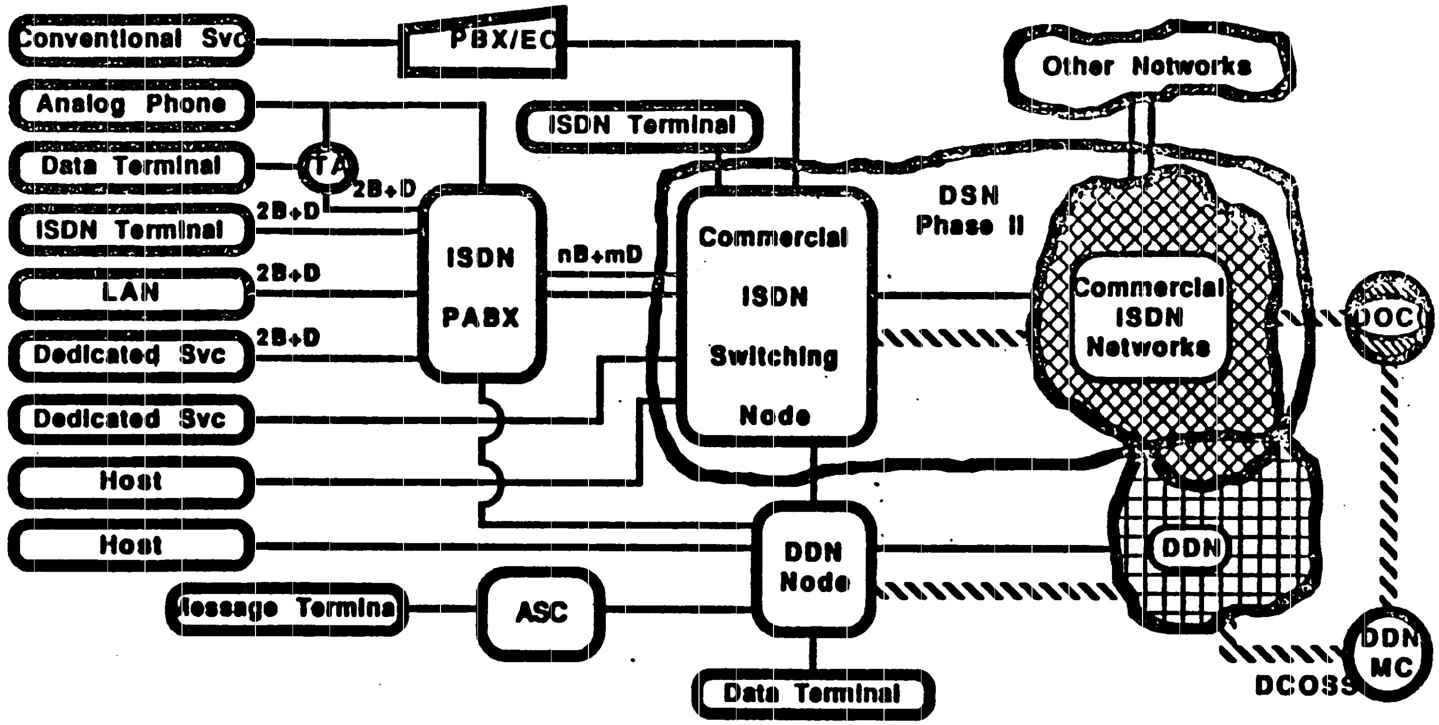
5.5.1 Target Architecture for CONUS

The target architecture for the CONUS comprises mainly leased services, as shown in Figure 5-3. The maintenance and management are handled by the network provider. Virtual private line networks (software defined networks) could be a major part of the DCS network in CONUS. The virtual private line network allows the customer to define its unique network attributes such as numbering plan, routing, call screening,



ACC - Access Control Center
KDC - Key Distribution Center
ASC - AUTODIN Switching Center
MC - Monitoring Center
BFE - Blacker Front End
NICS/TARE - NATO Integrated Comm Sys/Telegraph Automatic Relay Equip.
GW - Gateway
DCOSS - Defense Communications Operational Support System
GGH - Guard Gateway Host

Figure 5-2
DCS Interim Architecture



TA - Terminal Adapter for non ISDN Terminals

DOCC - DCA Operation Control Center

DCOSS - Defense Communications Operations Support System

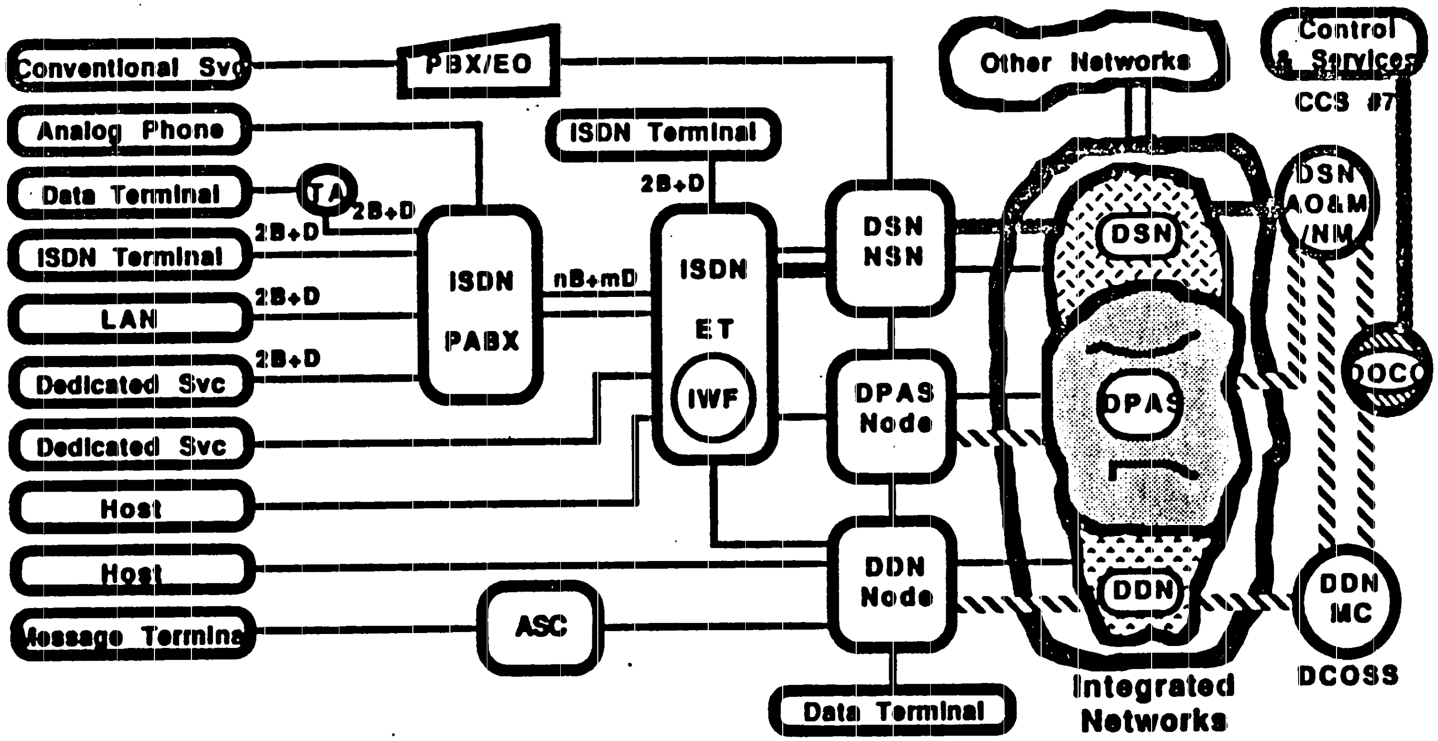
\\\\\\\\\\ Network Control Line

Figure 5-3
DCS Target Architecture for CONUS

Multilevel Precedence Preemption (MLPP), etc., while sharing network resources and access facilities with the public networks. Although the implementations of CONUS and Outside CONUS (OCONUS) segments are different, the Consultative Committee on International Telephony and Telegraphy (CCITT) ISDN based architecture is applicable for both segments of the DCS network.

5.5.2 Target Architecture for OCONUS

The target architecture for OCONUS shown in Figure 5-4, will permit the provision of all services as described in paragraph 5.3 above. Cost-effective provision of these services requires that existing loop plants be fully utilized with minimum modification. These considerations lead to all non-video being provided on enhanced existing loops, and video or wide band (greater than 64 Kb/s) services being provided on overlay T-carrier or fiber-optical facilities through DPAS control or dedicated lines. The non-video services can be satisfied by providing two 64Kb/s B-channels of the standard ISDN subscriber access loop which can independently carry a wide variety of information including digital voice, packet, circuit-switched, or channel-switched data. The 16 Kb/s D-channel transports out-of-band signalling information and telemetry and packet-switched data. The total user bandwidth requirement for delivering all non-video services to the majority of subscribers adds up to 2B+D, or 144 Kb/s.



TA - Terminal Adapter for non ISDN Terminals
ET - Exchange Termination (Access Node, DPAS)
NSN - DSN Network Switching Node
DOCC - DCA Operation Control Center
IWF - Interworking Functions
DCOSS - Defense Communications Operations Support System

Figure 5-4
DCS Target Architecture for OCONUS

6.0 SECURITY SEGMENT ARCHITECTURE

This section of the NDCCA will summarize the security considerations, current situation and target architecture regarding the NDCCA Security segment. The target architectures will be discussed separately for the Afloat and BITS segments.

6.1 Security Considerations

Protection of data must be commensurate with the sensitivity and vulnerability associated with the type, class, or level of data. For Navy data communications non-tactical mission support computer systems and or networks, the main issues are:

a. The protection of the Level II -- unclassified but sensitive data.

b. Data aggregation and inference control, and protection of ship movement information.

c. Changes in operational environment/scenario.

d. Direct connection of SNAP to NAVMACS (while at sea) and DDN (while in port).

e. Sufficient network controls to allow accreditation.

According to Navy directives, there are four main categories of Level II data; data under the Privacy Act protection (e.g., personal), For Official Use Only (FOUO) data, Finance data, and Technical document. Access to Level II data shall be limited to specific application programs, records, and files to which the individual seeking access has a specific need to know in performing their official duties. All physical, administrative, procedural, and technical safeguards should be implemented to protect Level II data in accordance with those specified in the OPNAVINST 5239.1A and SECNAVINST 5211.5C commensurate with Level II data protection.

Data aggregation and inference impose additional threats to Navy data communications. The aggregation problem is that Level II and III data even if unclassified in isolation, can reveal highly classified information (up to TS) when taken in the aggregate. The inference problem is that sensitive ship movement information (some data may be up to TS) can be derived as a conclusion from facts or premises of Level II and/or III data. For example, ship movement information may be derived from supply parts requisition, repair parts/spare parts inventory, or platform maintenance data. Therefore, the NDCCA must properly and effectively deal with the data aggregation and inference threat.

Changes in operational environment/scenario may also change data classifications drastically. For example, the same ship location data may be classified differently from Level III (unclassified) to Level I (Top Secret) depending on whether the ship is at her home port, or a foreign port, and the situation is peacetime-deployed; crisis, or conflict.

There are also generic security issues, for example, in connecting SNAP directly to the NAVMACS or to DDN. Currently, SNAP is an unclassified computer processing Level II and III data, and NAVMACS is a classified computer system processing GENSER traffic from unclassified to TS. Additional security protection is required when the SNAP and NAVMACS systems are connected in order to prevent classified data from being delivered to an unclassified system or host processor. It has been DDN's policy that all subscriber hosts must meet, at a minimum, Trusted Computer System Evaluation Criteria (TCSEC) Class C2 requirements by 30 September 1988, or else have formal waiver from DDN. Therefore, the plan for the NDCCA evolution shall comply to this security requirement.

6.2 Security Current Situation

6.2.1 Afloat Systems

Currently there are two segregated, physically separate systems for NAVMACS and SNAP on ship, with no direct connection. SNAP and NAVMACS are now manually interfaced through paper tapes which is in the process of being upgraded to magnetic media (e.g., floppy discs). The architecture is one of absolute separation, i.e., two different systems that are completely separate, both physically and logically, running at different security levels. The advantages include off-the-shelf availability, low development cost, and relative ease of certification/accreditation. However, the disadvantages include high cost and rigidity.

6.2.2 Shore-Based Systems

Currently there are two physically separate shore-based systems for processing classified and unclassified traffic. Typically, the classified system employs networks with a Protected Wire Distribution System (PWDS) while the unclassified system uses the Commercial-Off-the-Shelf (COTS) equipments. There are on-going efforts to increase current security by providing encryption protection enhancement for communications lines carrying Level I and II data. There is also widespread use of add-on packages or plug-in personal computer (PC) boards to enhance system access control and data security.

6.3 Security Target Architecture

6.3.1 Afloat Security Target Architecture

At this time, the Afloat security target architecture will consider the shipboard requirements only. The security provisions for data transmission between the shore-based facilities and the ship are provided by the NTS. Afloat network security will be addressed by the SAFENET architecture.

As shown in Figure 6-1, the afloat security target architecture is a Multilevel Secure (MLS) LAN interconnecting SNAP, NAVMACS, and other computing devices. The MLS LAN will support devices of different system high security levels. There should be an absolute barrier built into the MLS LAN to prevent data from flowing between two devices running at different security levels. Each device is connected to the MLS LAN through an Interface Unit (IU). The MLS LAN security can be divided into two major areas; the interface unit security and the transmission medium security.

6.3.2 BITS Security Target Architecture

As shown in Figure 6-2, the target BITS security architecture is a multilevel secure LAN which processes data within the same network structure. The architecture concept is very similar to the Secure Data Network System (SDNS) program under NSA's directorship. SDNS is a multilevel secure LAN built upon cryptologic protection and separation through end-to-end encryption and link encryption, and automatic, remote key distribution. The basic security requirements are: end-to-end protection for message text, link encryption for traffic analysis protection and NSA provided crypto algorithms.

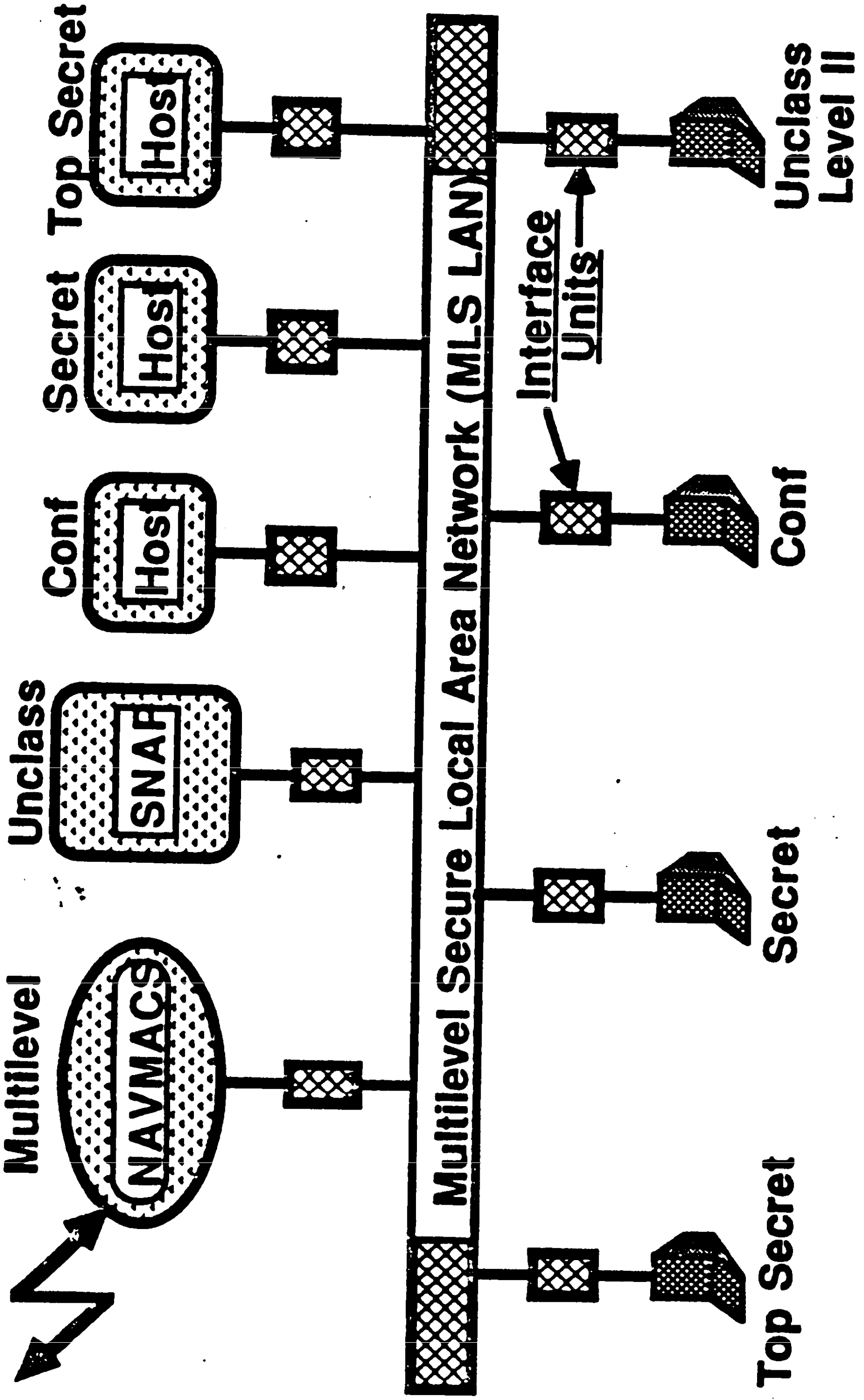


Figure 6-1
Afloat Security Architecture

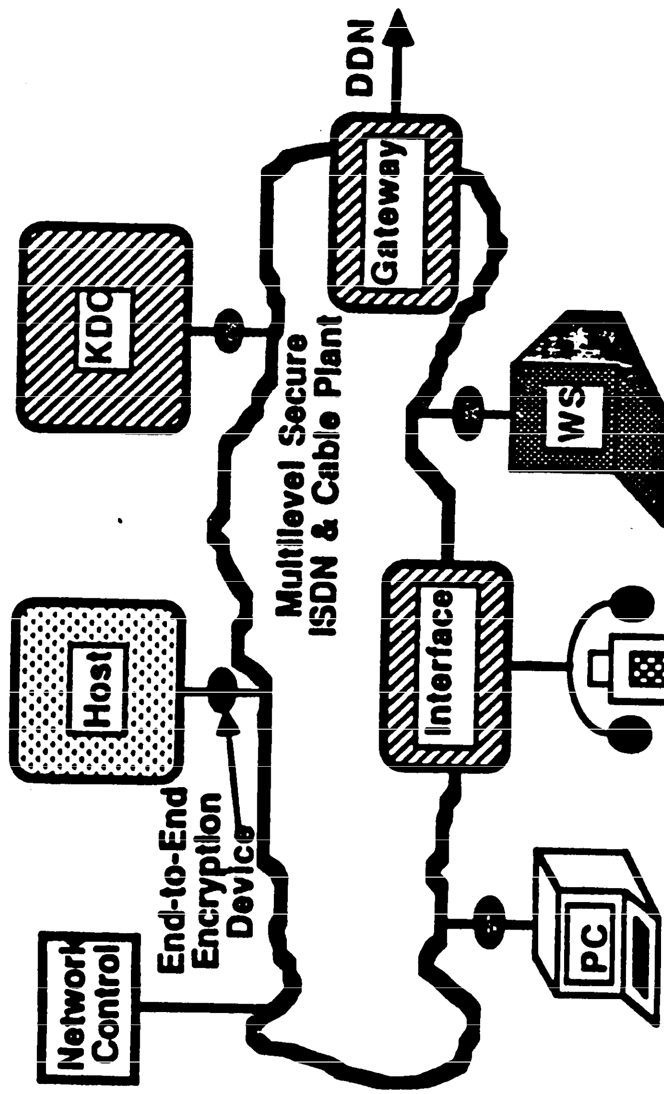


Figure 6-2
BITS Security Target Architecture

7.0 PROTOCOL SEGMENT ARCHITECTURE

The principal purpose of the protocol segment of the NDCCA is to develop a data communications protocol architecture based on the International Organization of Standardization (ISO) Open System Interconnection (OSI) reference model for Navy use in the target architecture time frame.

This section of the NDCCA will summarize the protocol considerations, current situation and target architecture regarding the NDCCA protocol segment.

7.1 Protocol Considerations

In the Navy data communications environment, the end-to-end communication path may transverse several different systems and or networks such as; shore-based IS devices, base LANs, DCS networks, satellite and or HF radio networks, shipboard communications systems and LANs, and shipboard IS devices. Since each of these systems and/or networks has its own operating procedure and performance measurement, a protocol for communicating the management information among those involved is required. In addition, a concept of end-to-end IS network management needs to be defined including performance measurement, operating procedures, and integration with the management concepts of the systems and or networks involved. Efforts to develop the relevant standards, policy, and management protocols are also required.

To this end, when a physical movement of paper tape, magnetic media, etc., is involved in the end-to-end transmission path, something must be done to compensate for the unreliability of this transmission segment to ensure that the entire process (end-to-end) is made reliable. For this, yet another higher level protocol to govern the overall movement of data is required in order to ultimately ensure that transmission of data between physically as well as electronically disconnected source and destination IS hosts is given end-to-end reliability and management.

The Navy data communications system requires an IS end-to-end management capability which provides for effectively integrating the Navy's human management structure, and the OSI network management and operational structure. This involves integrating the current Navy operating procedures and management structure (e.g., base security officers), with the requirements and capabilities of an OSI seven-layered network. The objective is to ensure that the whole environment is able to be managed including determining how well the system is operating and assisting in diagnosing and solving problems.

7.2 Current Protocol Situation

The NDCCA advocates the use of protocols that are International Standards (IS) or Draft International Standards (DIS) which are augmented; if necessary, by proposed protocol efforts and existing Navy standards. Six categories of application/service were identified for Navy data communications: file transfer, electronic mail, terminal support, process control, office automation and workstation support, and others such as digital voice/video teleconferencing, as shown in Figure 7-1.

The protocols associated with these applications are the ISO standard protocols and are in concert with the Government Open Systems Interconnection Profile (GOSIP) and the Computer-aided Acquisition and Logistics Support (CALS). In particular: File Transfer, Access and Management (FTAM) and Common Application Service Elements (CASE) are used for file transfer; Consultative Committee on International Telephony and Telegraphy (CCITT) X.400 recommendations are used for electronic mail; Virtual Terminal Protocol (VTP) and CASE are used for terminal support; Manufacturing Automation Protocols (MAP) - FTAM, CASE, and Manufacturing Message Format Standard (MMFS) are used for process control; and Technical and Office Protocols (TOP) - FTAM and CASE are used for automation and workstation support. The known/developed protocols for the remainder of the application layers are as shown in Figure 7-2.

7.3 Target Protocol Architecture

The target architecture for the NDCCA will include those shown in Figure 7-2, for the current situation plus some others as shown highlighted in Figure 7-3. The protocol suites have been delineated to ensure interoperability. Protocols for digital voice/video teleconferencing are still in the development stage. Presentation Layer Protocol (PLP) must be developed for the terminal support service type. Host-to-Gateway Protocol (HGP) and Exterior Gateway Protocol (EGP) must be developed for all current service types for the network layer.

In addition, the Initial Graphics Exchange Specification (IGES) should be used in defining formats of the graphics data files used in the Computer Aided Design and Computer Aided Manufacturing (CAD/CAM) environments.

Service Type / Appl Layer	File Transfer	Electronic Mail	Terminal Support	Process Control (MAP)	Office Automation Workstation Support (TOP)	Others (e.g. Digital Voice, Video Tele-Conferencing)
Layer 7	FTAM CASE	X.400	VTP CASE	FTAM CASE MMFS	FTAM CASE	

Figure 7-1
Protocols Current Situation

Service Type / Appl Layer	File Transfer	Electronic Mail	Terminal Support	Process Control (MAP)	Office Automation Workstation Support (TOP)	Others (e.g. Digital Voice, Video Tele-Conferencing)
Layer 7	FTAM CASE	X.400	VTP CASE	FTAM CASE MMFS	FTAM CASE	
Layer 6	ASN.1	Null		ASN.1		
Layer 5	BSS	BAS	BCS			
Layer 4	TP4	TP0		TP4		
Layer 3	Connectionless IP	CONS		Connectionless IP		
Layer 3	Internetwork Control Message Protocol (ICMP					
Layer 2	802.2					
Layer 1	802.3,4,OR 5			802.4	802.3,4,OR 5	

Figure 7-2
Protocols Current Situation (Cont)

Appl Layer \ Service Type	File Transfer	Electronic Mail	Terminal Support	Process Control (MAP)	Office Automation Workstation Support (TOP)	Others (e.g. Digital Voice, Video Tele-Conferencing)
Layer 7	FTAM CASE	X.400	VTP CASE	FTAM CASE MMFS	FTAM CASE	
Layer 6	ASN.1	Null	PLP	ASN.1		
Layer 5	BSS	BAS	BCS			TBD
Layer 4	TP4		TP0	TP4		
Layer 3	Connectionless IP		CONS	Connectionless IP		
	Internetwork Control Message Protocol (ICMP)					
	Host-to-Gateway & Exterior Gateway Protocols (HGP & EGP)					
Layer 2	802.2					
Layer 1	802.3,4,OR 5			802.4	802.3,4,OR 5	e.g. ISDN, etc

Figure 7-3
Protocols Target Architecture

REFERENCES

Cornwell, Joseph D. et al. (1987), Navy Data Communications Architecture: WP 87W00283 McLean, VA: The MITRE Corporation.

Hoh, Yan-Shek (1987) An Analysis of 1992 Time Frame Data Communications Protocol Suite Implementation, MTR 87W00195, McLean, VA: The MITRE Corporation.

Jeng, Albert B. (1987) Navy Data Communications Control Architecture Security, MTR-87W00211 ,Draft, McLean, VA: The MITRE Corporation.

Naval Data Automation Command (1987), Navy Data Communications Architecture, Draft.

National Bureau of Standards (1985), A Proposed Navy Communications Architecture, ICST/SNA-85-19.

National Research Council (1983), Navy Nontactical Automatic Data Processing Policy, Organization and Management, Interim Report to the United States Navy.

The MITRE Corporation (April 1988), Navy Base Information Transfer System (BITS) Architecture, Draft.

The MITRE Corporation (1987), Navy Data Communications Afloat Architecture, Draft.

The MITRE Corporation (February 1988), Navy Long Haul Communications Architecture, Draft.

GLOSSARY

Acronyms

AACG	Afloat Architecture Core Group
ACC	Access Control Center
ADCA	Afloat Data Communications Architecture
ADP	Automated Data Processing
ARPANET	Advanced Research Projects Agency Network
ASC	AUTODIN Switching Center
ASN.1	Abstract Syntax Notation 1
AUTODIN	Automatic Digital Network
AUTOVON	Automatic Voice Network
BACG	BITS Architecture Core Group
BAS	Basic Activity Subset
BCS	Basic Combined Subset
BFE	BLACKER Front End
BITS	Base Information Transfer System
BPS	Bits Per Second
BSS	Basic Synchronized Subset
C^2	Command and Control
C^2I	Command, Control and Intelligence
C^3I	Command, Control, Communications and Intelligence
CACG	Control Architecture Core Group
CAD/CAM	Computer Aided Design/Computer Aided Manufacturing
CALS	Computer-aided Acquisition and Logistics Support
CAMS	Communications Area Master Station
CASE	Common Application Service Elements
CCITT	Consultative Committee on International Telephony and Telegraphy
CCS	Common Channel Signaling
CINCLANTFLT	Commander in Chief Atlantic Fleet
CINCPACFLT	Commander in Chief Pacific Fleet
CMC	Commandant Marine Corps
CNO	Chief of Naval Operations
COMNAVDAC	Commander NAVDAC
CONS	Connection-Mode Network Service
CONUS	Continental United States
COTS	Commercial-Off-the-Shelf
CSMA/CD	Carrier Sense Multiple Access with Collision Detection
CV	Aircraft Carrier
DACG	DCA Architecture Core Group
DAMA	Demand Assigned Multiple Access

DARPA	Defense Advanced Research Projects Agency
DCA	Defense Communications Agency
DCS	Defense Communications System
DCOSS	Defense Communications Operations Support System
DDN	Defense Digital Network
DIRDONIRM	Director DONIRM
DIS	Draft International Standards
DISNET	Defense Integrated Secure Network
DOCC	Defense Operation Control Center
DOD	Department of Defense
DODIIS	DOD Intelligence Information System
DON	Department of Navy
DONIRM	Department of Navy Information Resource Management
DPAS	Digital Patch and Access System
DSCS	Defense Satellite Communications System
DSN	Defense Switched Network
DUSD	Deputy Under Secretary of Defense
EGP	Exterior Gateway Protocol
EMCON	Emission Control
EO	Exchange Operator
ET	Exchange Terminal
EUCOM	European Command
EW	Electronic Warfare
FLTSAT	Fleet Satellite
FOUO	For Official Use Only
FRI	Fleet Routing Indicator
FTAM	File Transfer, Access and Management
GEMS	Graphic Engineering and Mapping System
GENSER	General Service
GGH	Guard Gateway Host
GOSIP	Government Open Systems Interconnection Profile
GW	Gateway
HF	High Frequency
HGP	Host-to-Gateway Protocol
ICMP	Internetwork Control Message Protocol
IDS	Integrated Data Services
IEEE	Institute of Electrical and Electronic Engineers
IGES	Initial Graphics Exchange Specification
IP	Interface Processor or Internet Protocol
IS	Information System
ISDN	Integrated Services Digital Network
ISO	International Standards Organization

IST	Inter-switch Trunk
ITACS	Integrated Tactical Automated Communications System
IU	Interface Unit
JCS	Joint Chiefs of Staff
KBPS	Kilo (1,000) Bits Per Second
KDC	Key Distribution Center
KG	Cryptographic Device
LAN	Local Area Network
LDMX	Local Digital Message Exchange
MAGIC	Master Activity General Information & Control
MAP	Manufacturing Automation Protocols
MBPS	Mega (1,000,000) Bits Per Second
MC	Monitoring Center
MILNET	Military Network
MINET	Movements Information Network
MLPP	Multilevel Precedence Preemption
MLS	Multilevel Secure
MMFS	Manufacturing Message Format Standard
NARDAC	Navy Regional Data Automation Center
NATO	North Atlantic Treaty Organization
NAVDAC	Navy Data Automation Command
NAVCAMS	Navy Communication Area Master Station
NAVCOMCO	Navy Commercial Communications Office
NAVCOMPARS	Navy Communication Processing and Routing System
NAVCOMSTA	Navy Communications Station
NAVFAC	Navy Facilities Command
NAVMACS	Navy Modular Automated Communications System
NAVSEA	Naval Sea Systems Command
NAVTELCOM	Naval Telecommunications Command
NCA	National Command Authority
NCS	Naval Communications Station
NDCCA	Navy Data Communications Control Architecture
NDCUG	Navy Data Communications Users Group
NFADB	Navy Facility Assets Data Base
NICS	NATO Integrated Communications System
NSA	National Security Agency
NSC	Navy Supply Center
NTCC	Naval Telecommunications Center
NTS	Navy Telecommunications System
OAN	Office Automation Network
OCONUS	Outside CONUS
OCR	Optical Character Reader

OPNAV	Operational Navy Instruction
OPNAVINST	Operational Navy Instruction
OSD	Office of the Secretary of Defense
OSI	Open Systems Interconnect
PABX	Private Automatic Branch Exchange
PACG	Protocol Architecture Core Group
PBX	Private Branch Exchange
PC	Personal Computer
PLP	Presentation Layer Protocol
POM	Program Objective Memorandum
PPBS	Planning, Programming and Budgeting System
PSG	Policy Steering Group
PTT	Postal Telephone and Telegraph
PWDS	Protected Wire Distribution System
R&D	Research and Development
RIXT	Remote Information Exchange Terminal
S/A	Service and/or Agency
SACDIN	Strategic Air Command Digital Network
SACG	Security Architecture Core Group
SAFENET	Token ring LAN with survivability enhancements
SATCOM	Satellite Communications
SCI	Special Compartmented Information
SDNS	Secure Data Network System
SECNAVINST	Secretary of the Navy Instruction
SHE	Super High Frequency
SNAP	Shipboard Non-Tactical ADP Program
SPAWAR	Space and Naval Warfare Systems Command
SPLICE	Stock Point Logistics Integrated Communications Environment
SRT	Standard Remote Terminal
TA	Terminal Adapter
TARE	Telegraph Automatic Relay Equipment
TCP/IP	Transmission Control Protocol/Internet Protocol
TCSEC	Trusted Computer System Evaluation Criteria
TID	Trusted Interface Device
TOP	Technical and Office Protocol
TP0	Transport Layer Protocol Class 0
TP4	Transport Layer Protocol Class 4
TS	Top Secret
UHF	Ultra High Frequency
URDB	User Requirements Data Base
VTP	Virtual Terminal Protocol

WINCS	WWMCCS Intercomputer Network Communications Subsystem
WS	Work Station
WWMCCS	World Wide Military Command and Control System

DATA COMMUNICATION STEERING COMMITTEE CHARTER

1. AUTHORITY. The Navy Data Communications Steering Committee is chartered under the authority of the Assistant Secretary of the Navy (Financial Management) as DON Senior Official for Information Resources Managment and the Chief of Naval Operations (OP-094) as executive agent for data communications within the DON.

2. SCOPE. The objective of the charter is to put an Architecture in place to guide the development of data communications support for Navy information systems using common user resources and capabilities wherever possible. The initial step was to develop a control architecture for approval by the Steering Committee to identify and establish boundaries between major architectural support efforts (subarchitectures), define necessary procedures for maintenance, and assign responsibilities for architecture development and implementation. A standing core group will periodically review subarchitectures, determine specific goals, and identify development tasks needed to meet architecture objectives. Working group will initiate efforts to accomplish approved tasks and recommend specific architecture modifications.

3. DEFINITIONS.

A. Steering Committee. Selected Flag level representatives of major commands with data communications related missions to provide guidance and tasking for architecture development.

B. Control Architecture. A document which accomplishes the following:

(1) Defines related architecture efforts:
Warfare Systems Architecture (SPAWAR)
Navy Telecommunications Architectures (TELCOM)
Base Information Transfer Architecture (NAVDAC/NAVCOMO)
Defense Data Network (TELCOM)
Shipboard Data Communications Architectures (NAVSEA/SPAWAR)
Facilities Planning Criteria for Navy and Marine Corps Shore Installations (NAVFAC)

(2) Defines data communications responsibilities for architecture development and maintenance as well as Navy-wide implementation of the target architecture.

(3) Establishes criteria and procedures for approving and validating strategies, capabilities, standards, and services to guide the architecture development.

(4) Defines implementation policies to ensure mission effectiveness, efficiency, security, commonality, performance, and interoperability.

C. Architecture Control Board. Representatives from major staffs (CAPT/CDR or equivalent level) with broad functional experience and actively involved in DON data communications and architecture efforts.

The control board will perform the following:

(1) Develop and maintain the control architecture and interaction between subarchitectures.

(2) Document and maintain a record of approved requirements, strategies, and capabilities. COMNAVDAC will assist in this maintenance effort.

(3) Identify tasks to be performed and provide recommendations to the Steering Committee.

(4) For approved recommendations, representatives will oversee implementation within subarchitectures and provide resources for working group assigned tasks.

(5) Provide status reports to the Steering Committee.

D. Subarchitectures. Architectures as identified by the control architecture. These architectures will be maintained by commands within mission areas or covered by a Memorandum of Understanding (MOU) between multiple commands.

E. Working Groups. Representatives of fleet or major staffs identified by the Control Board to accomplish specific maintenance and working group efforts.

4. MANAGEMENT ORGANIZATION.

4.1 STEERING COMMITTEE

CNO (OP-094), Chair
CNO (OP-945), Executive Secretary
CNO (OP-44,941,942,943)
COMNAVTELCOM
COMSPAWARSYSCOM (SPAWAR-32)
COMNAVDAC

4.2 ARCHITECTURE CONTROL BOARD

CNO (OP-945), Chair
CNO (OP-941, 942, 943)
CINCPACFLT
CINCLANTFLT
COMNAVDAC
COMNAVTELCOM
COMSPAWARSYSCOM
COMNAVFACENGCOM

5. REPORTS. The architectures effort will begin as of the effective date of this charter. The Architecture Control Board will provide the following:

A. Quarterly reports to the Chair of the Steering Committee.

B. Formal brief semi-annually in October or November and May or June as directed by the Steering Committee Chair.

C. Control and Subarchitecture review by Navy commands. Formal fleet architecture review will be a standing agenda item of the Fleet Non-Tactical ADP Council. Navy information systems review will be scheduled to coincide with the Information Systems Conference and Navy Communications Work Group meeting.

D. Other as requested.