SRI- DDN NIC

2745-88

SRI International

AGENDA

Mr. Ray Martone

Defense Communications Agency

28 January 1988

SRI INTERNATIONAL
Engineering Research Group

1300	SRI Overview	EL 149	D.A. Johnson
1320	SRI Technical Base and Project Sampler	EL149	D.L. Nielson
1340	First and Second Floor (Bldg. E)		D.L. Nielson
1350	C^2 Networking and Third Floor (Bldg. E)	EJ330	M.S. Frankel
1445	Tour Bldgs. A and I		N.A. Walker
	Communications Systems	110	N.A. Walker
	Tour ERG Facilities		N.A. Walker
1600	Network Information Services and NIC Area	EJ228	E.J. Feinler
1630	SRI Support Systems and WDC	EL149	B.E. Camph J.J. Gruender R.M. Tidwell
1645	Wrap-up	EL149	D.L. Nielson J.P. McHenry
1700	Adjourn		

REPORTS

SRI International®
333 Ravenswood Ave. • Menlo Park, CA 94025
(415) 326-6200 • TWX: 910-373-2046 • Telex: 334-486

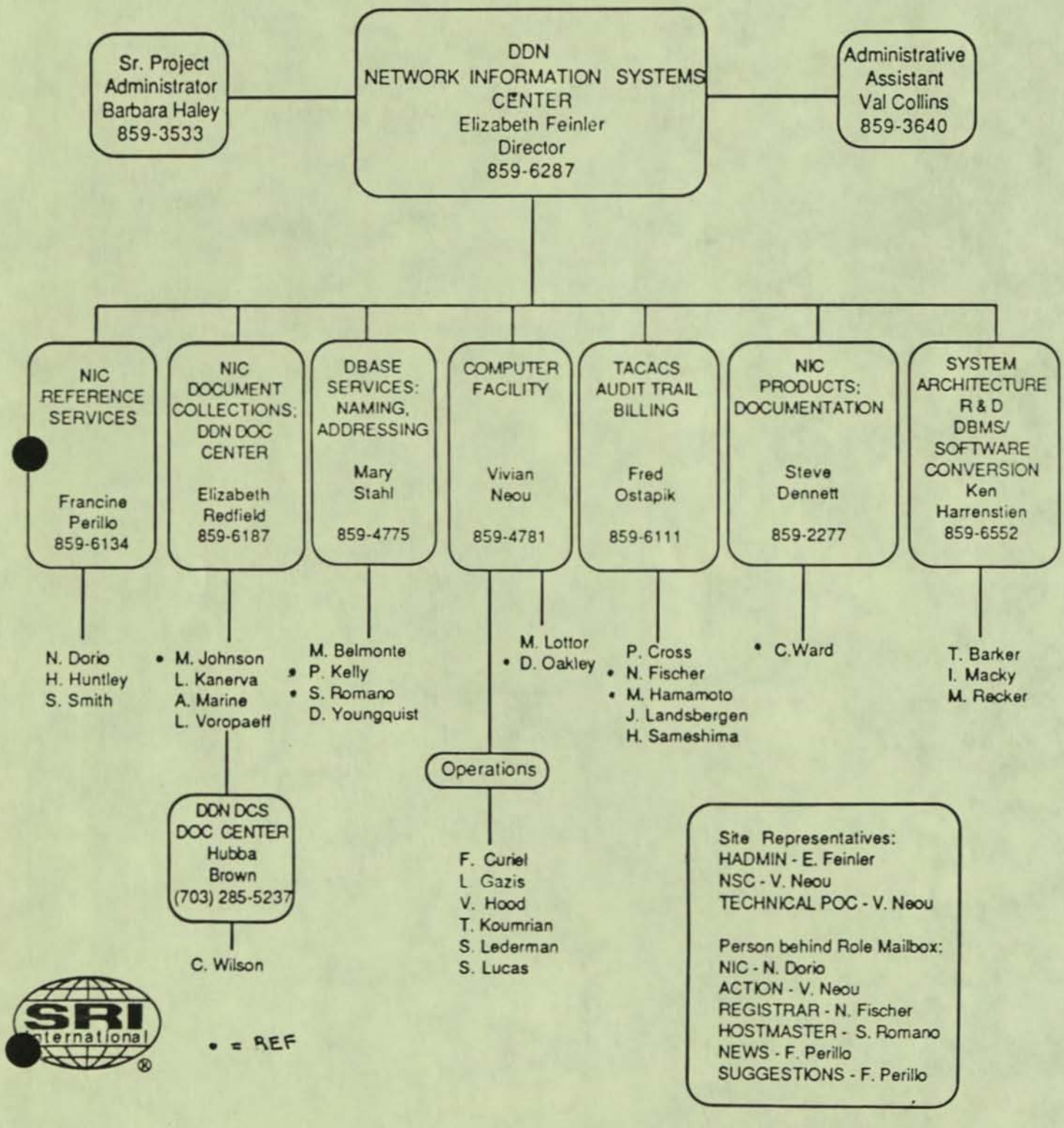
NETWORK INFORMATION
SYSTEMS CENTER

Computer and Information
Sciences Division

ENGINEERING RESEARCH GROUP

NIC HOTLINE (800) 235-3155
AREA CODE 415

DDN Network Information Systems Center
SRI International
Menlo Park, CA



Major Project Effort

DDN Network Information Center

NIC CONTRACT HISTORY

1970-1972	DARPA/RADC	CPFF, Unsolicited Research
1972-1983	DCA	CPFF, Unsolicited Research
1983-1988	DDN DCS	CPFF, Sole Source
1988-	???	Plan to compete

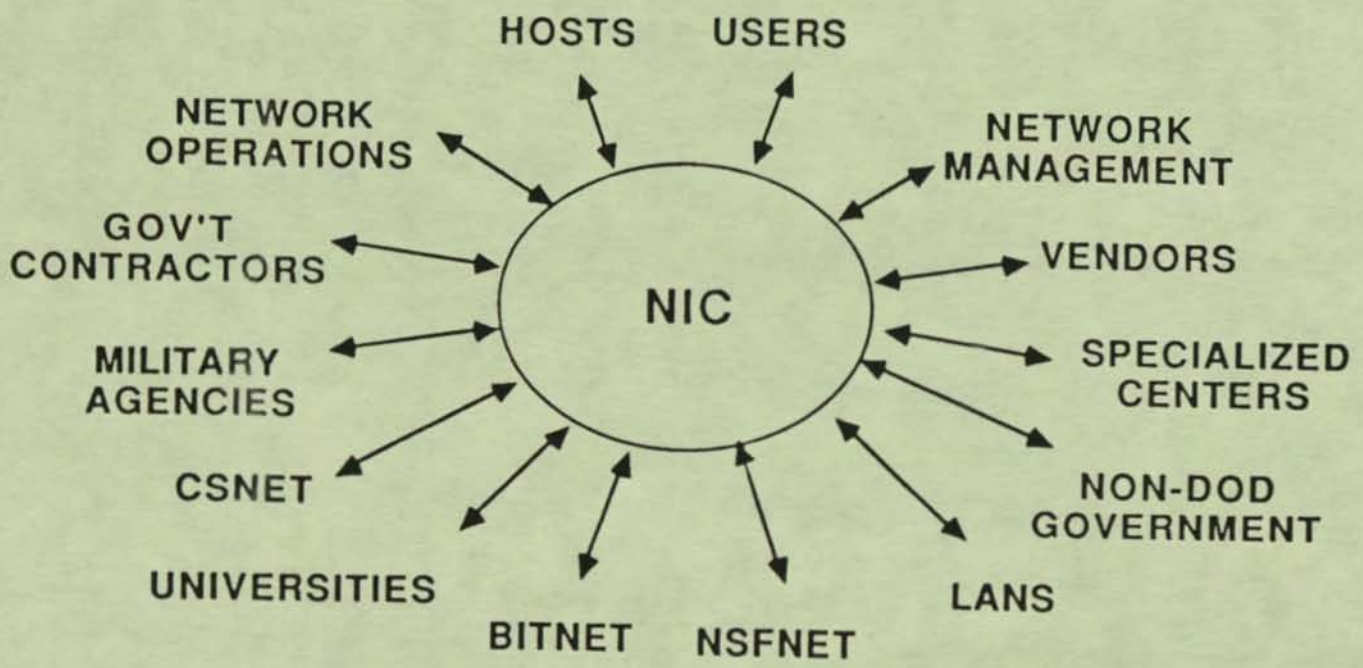
IMPACT OF COMPETITION

- Loss of Continuity
- Expensive to Move
- Confuses Users; Require Retraining
- NIC Loses "Neutral" Status
- Loss of SRI Co-Investment
- Contractor Forced Into Competitive Stance
- Interruption of Technology Transfer
- Loss of Valuable Information

ALTERNATE SUGGESTION

- Continue NIC as sole source contractor
- Set up military policy board
  - Policy
  - Services
  - Guidelines
- Sanction NIC as DCA online protocol and technology transfer POC
  - DDN software repository
  - Online services to DDN users
  - Assist DCA with info liaison to DTIC, NTIS, etc.
- Fund Internics activity to define
  - Infrastructure
  - Protocols
  - Administration

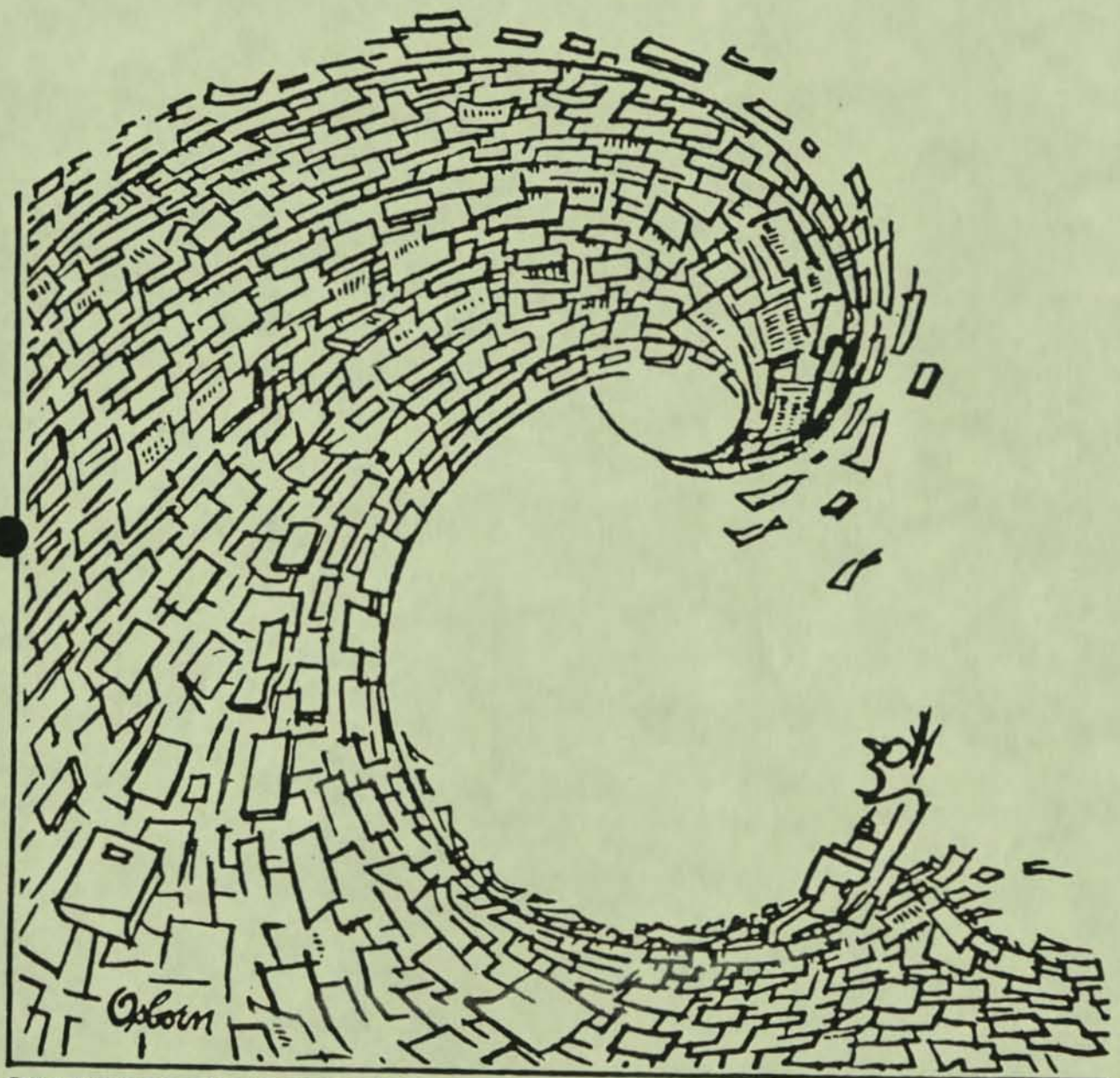
INTERCONNECTIVITY
AND INTEROPERABILITY



VALUE ADDED SERVICES

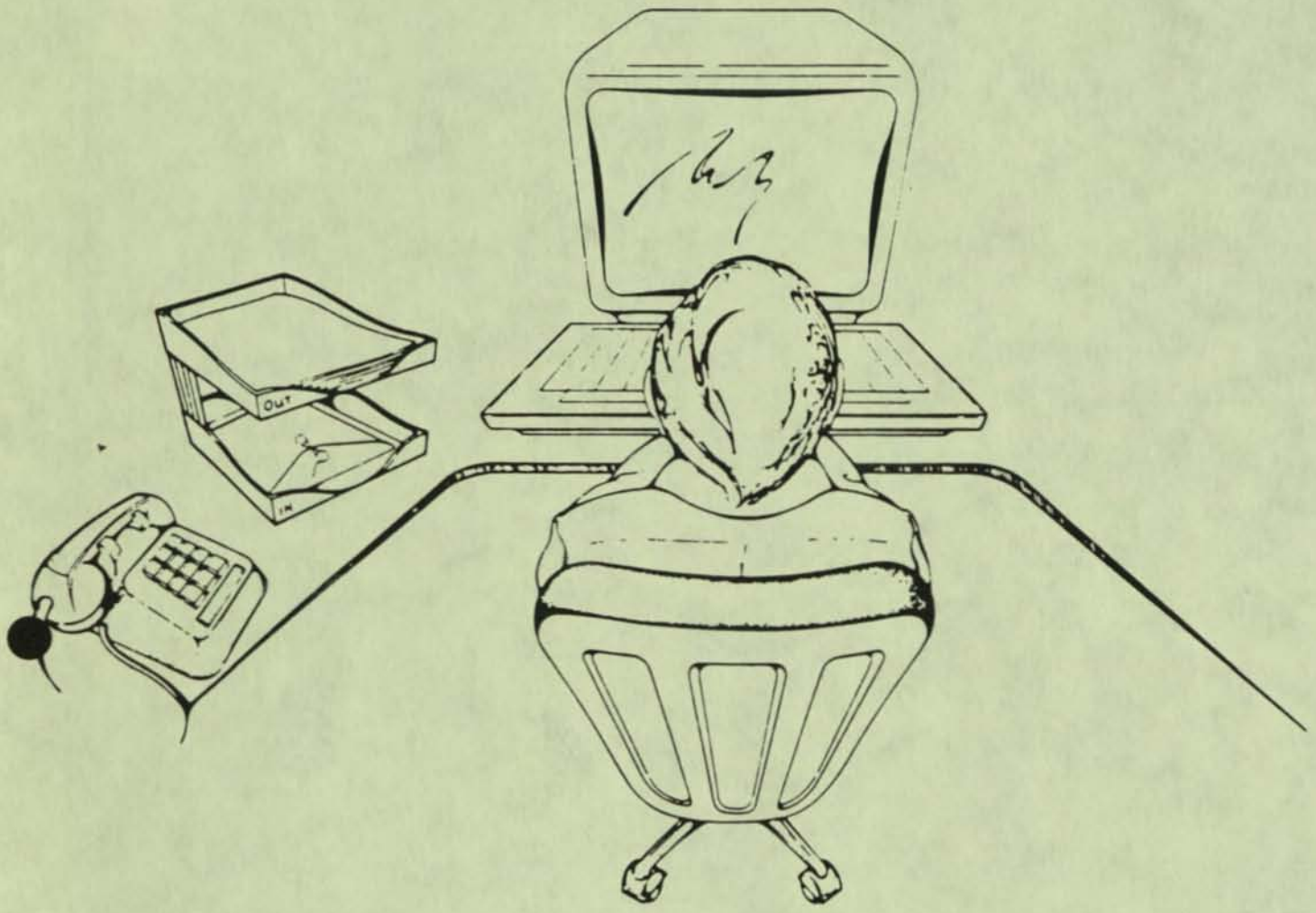
- Replication
- Generic Implementations
- Interoperability/Interconnection
- Internic Cooperation
- Neutrality and Objectivity
- Save Time for DDN DCS Personnel

THE PROBLEM

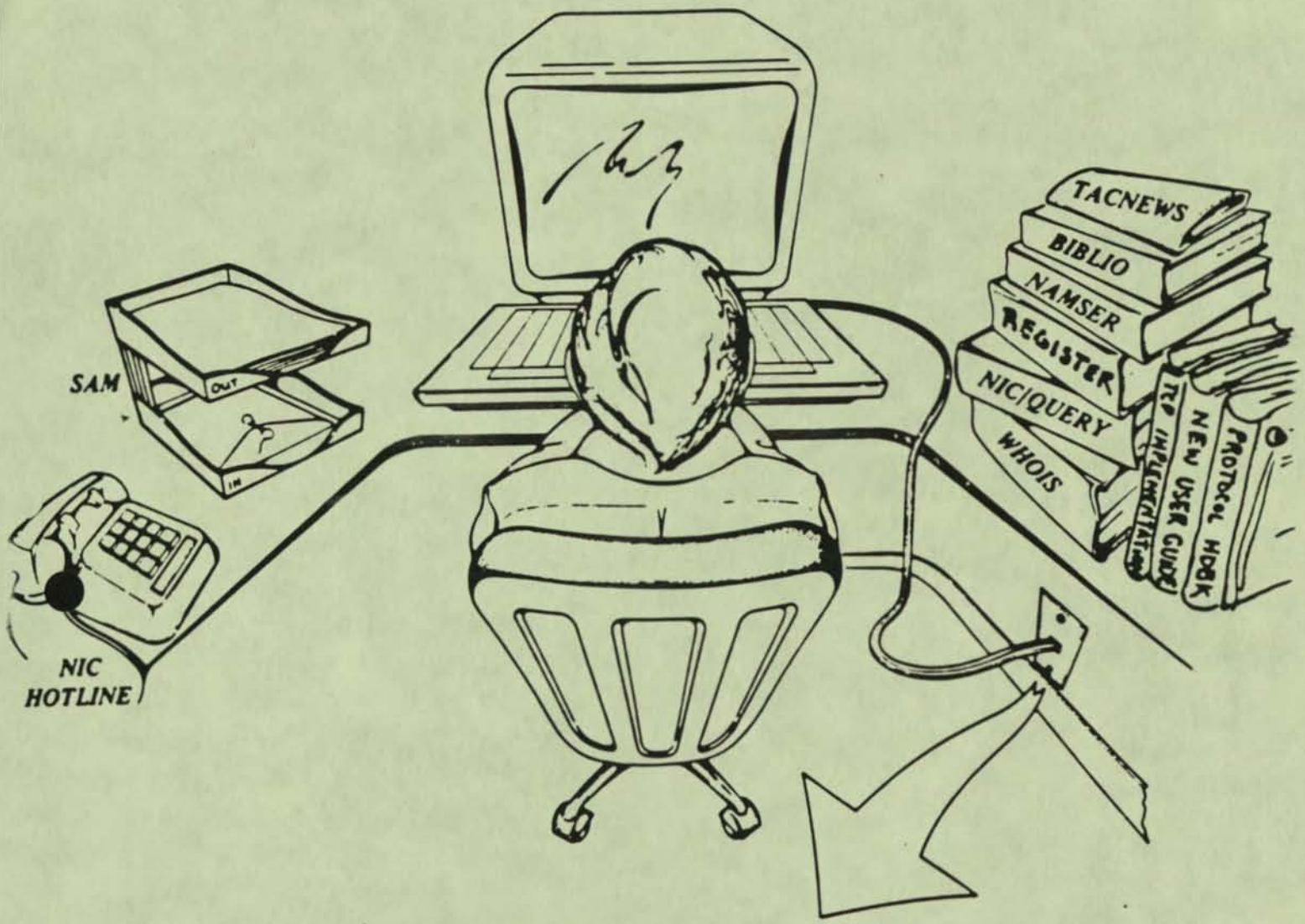


DRAWING BY ROBERT OSBORN

HOW WE HAVE APPROACHED THE PROBLEM



- GIVEN A TELEPHONE, A TERMINAL, AND THE NETWORK
- WE BRING INFORMATION TOOLS TO THE KNOWLEDGE WORKER ELECTRONICALLY



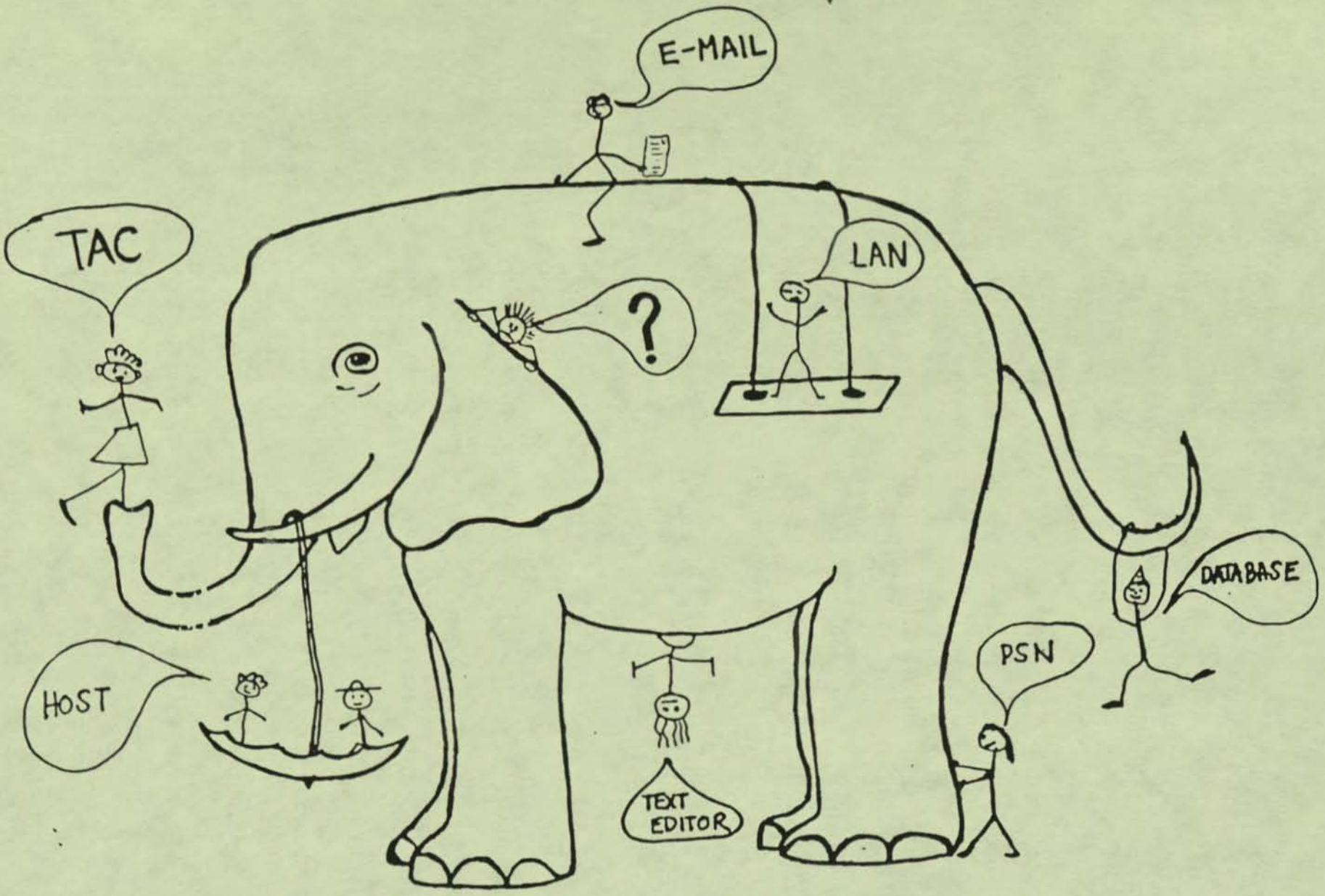
- BILLING
- ACCESS PERMISSION
- NAME SERVICE
- PROTOCOL INTERCONNECTION
- PRIVACY/AUDIT TRAIL

CURRENT NIC EFFORT

- Core NIC
- DDN Audit Trail/Billing System
- Internet Naming/Addressing
- User Registration
- TAC Access
- Maintain 2 Document Centers
- Maintain DCA Computer Facility
- Software Design/Implementation
- Publications/Products

CORE NIC

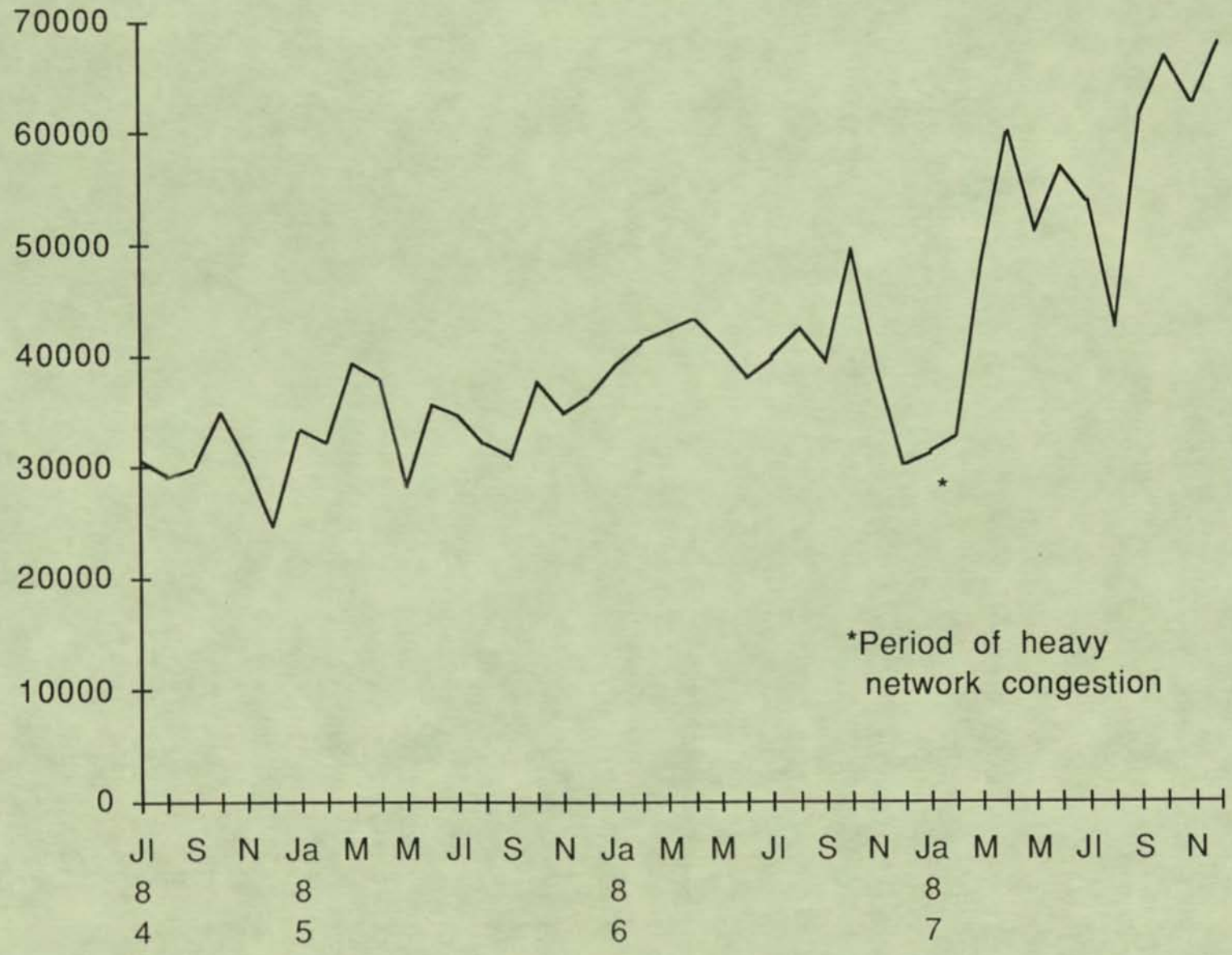
- User Assistance, Hotline, Online
- Repository, Document Centers
- Reference Software
- Network/DDN DCS Liaison
- Information Servers



"ACCESS TO THE DDN"

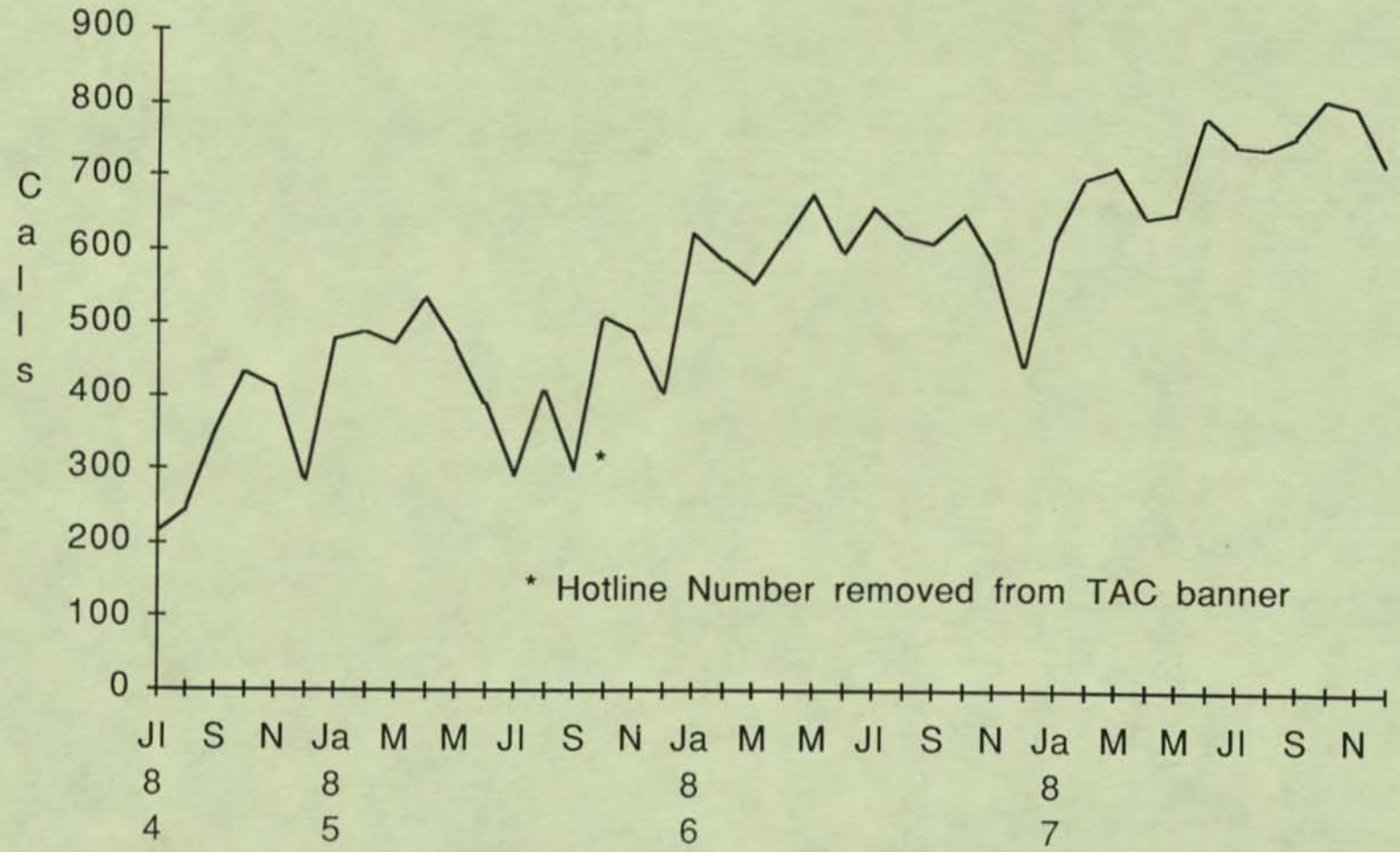
DDN Whois Usage

July 1984 - Dec. 1987



DDN Hotline Usage

July 1984 - Dec. 1987



DDN AUDIT TRAIL/BILLING

- Who, How Long, and Kind of Usage
- Capacity and Use Planning
- Billing to Individual Level

Network Audit and Control

- Tasked by Defense Data Network (DDN)

- Joint effort by DDN, SRI, BBN, AYDIN

- Three interlinked tasks:
  - TACACS
  - Network Audit Trail System (NAURS)
  - Network Billing and Usage System (NURS)

Network Audit Trail System

- TAC user activity
- Network utilization
- Capacity planning
- Network usage trends

Reports Generated

- Summary Reports
  - Number of logins
  - Average length of logins
  - Percent prime time use
- Incident Reports
  - Simultaneous TAC logins
  - Excessive duration of logins
- Ad hoc Reports
  - Emergency, one-of-kind reports

Billing Reports

- Based on usage
- Accumulated by PDCs
- Customized for:
  - DCA (Total net activity)
  - Service Branches
  - Organizations
  - Sites
  - Individuals

Future

- Profile User Activities
- Expert system
- Audit Trail Protocol enhancements
- Portable NAURS/NURS
- Applicability to other (classified) networks

Information Available

- Identity of TAC user
- Location of TAC used
- Time of use
- Locations of remote hosts
- Durations of sessions
- Data traffic

INTERNET NAMING/ADDRESSING

- Design
- Implementation
- Administration
- Replication

DDN Naming and Addressing

- Transition: Flat Naming -> Hierarchical Naming
- Transition: TCP/IP -> OSI

NIC's Role

- Registry for Hosts and Domains
- Administer Top-Level Domains
- Provide Data Files to Key Sites
- Provide Uninterrupted Network Operation
- Provide Official DoD Internet Host Table
- Assist Network Interoperability
- Teamwork - OSD, DCA, DARPA, NSF, NIC, MITRE

USER REGISTRATION/TAC ACCESS

- TAC Cards, Passwords
- Hotline
- WHOIS Directory Service

TACACS

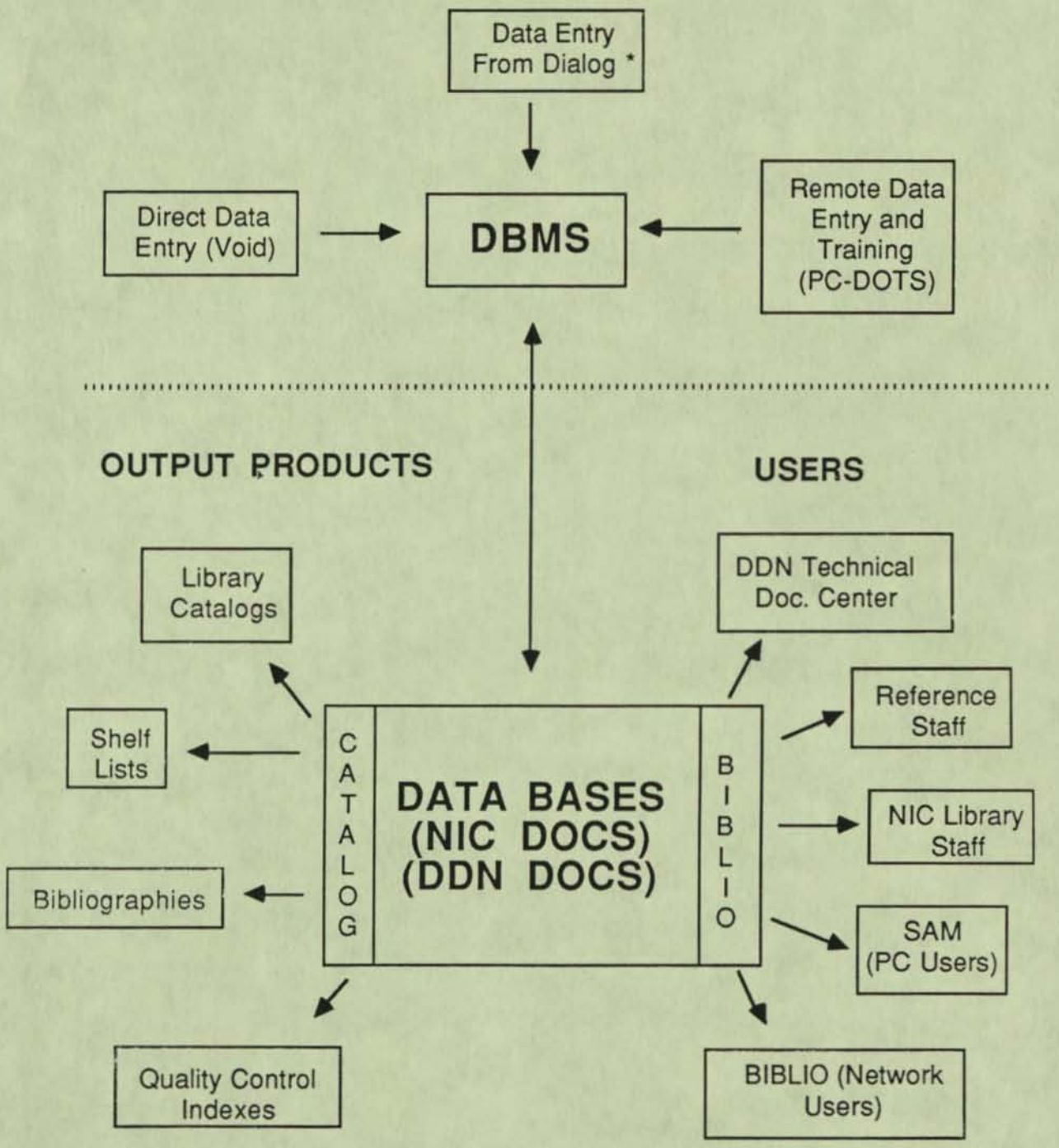
Terminal Access Control System

- Register users
- Issue TAC Cards
- Rolling update
- Remove unauthorized users

DOC CENTER SERVICES

- DDN NIC (Menlo Park)
- DDN Technical Document Center (McLean)
- Catalogs
- Online Search Service
- Collection Maintenance

DATA ENTRY

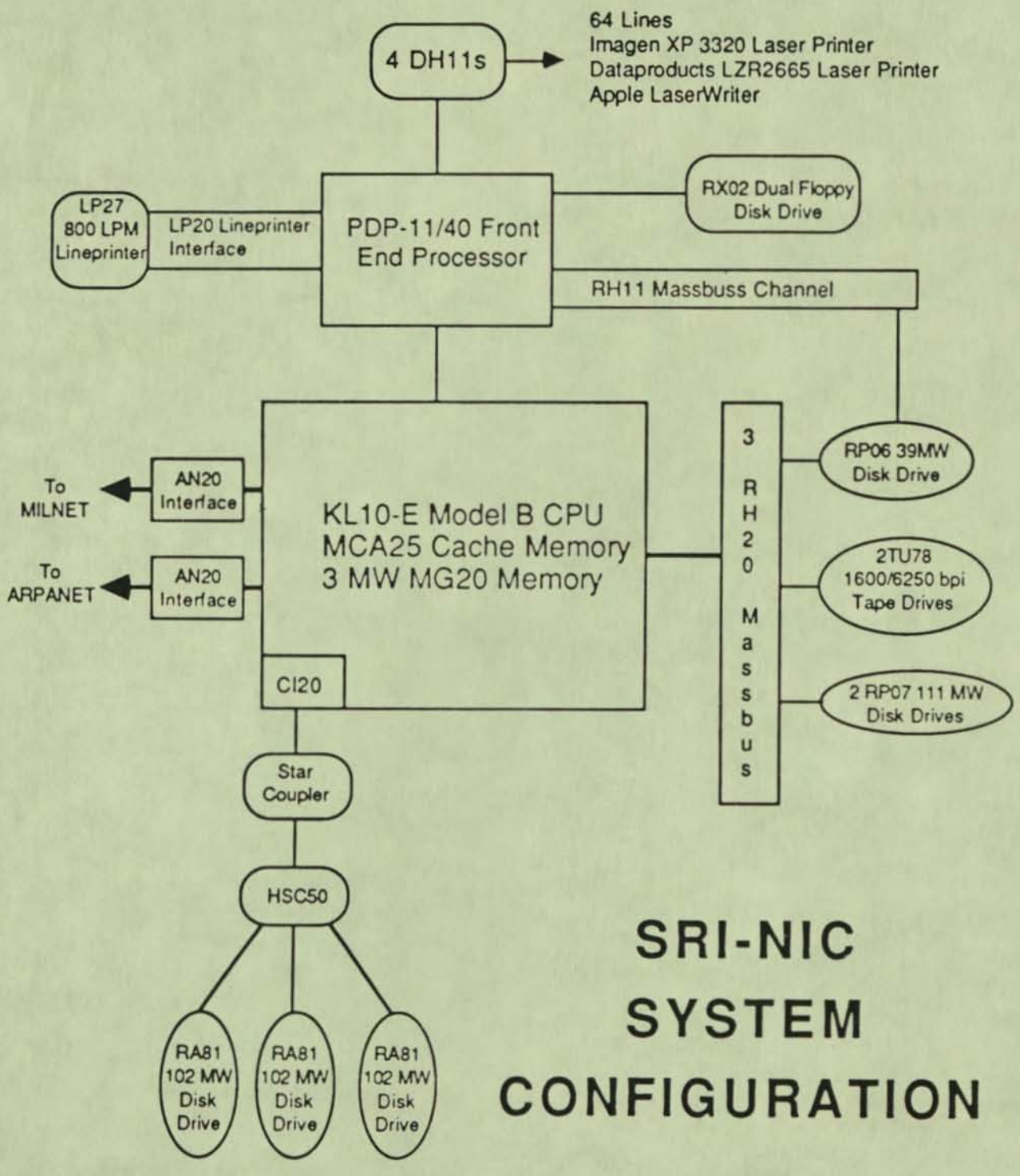


NIC Information Tools

* Available but not currently used

DDN COMPUTER FACILITY

- PSNs
- TAC
- Mainframes
- Peripherals
- Workstations
- LANs



SRI-NIC SYSTEM CONFIGURATION

SOFTWARE DESIGN/DEVELOPMENT

- User Programs
- Information Servers
- Distributed Data Bases
- Mail Systems
- Protocols
- RFCs

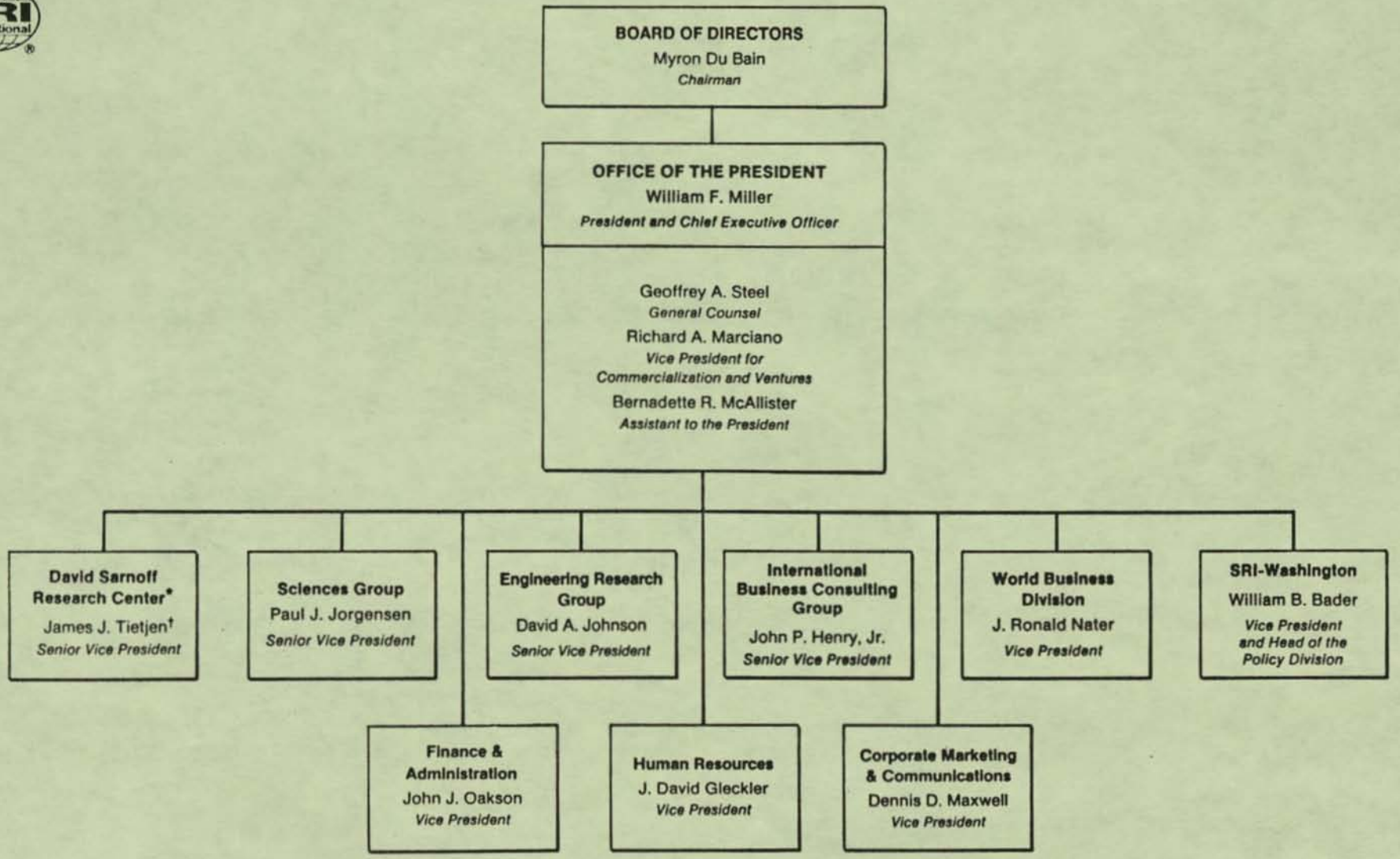
PUBLICATIONS/PRODUCTS

- PC Software Tools
- Handbooks
- User Manuals
- Protocol Guidelines
- Reference Documents

DDN NETWORK INFORMATION CENTER

IN PROGRESS REPORT

6/14/88

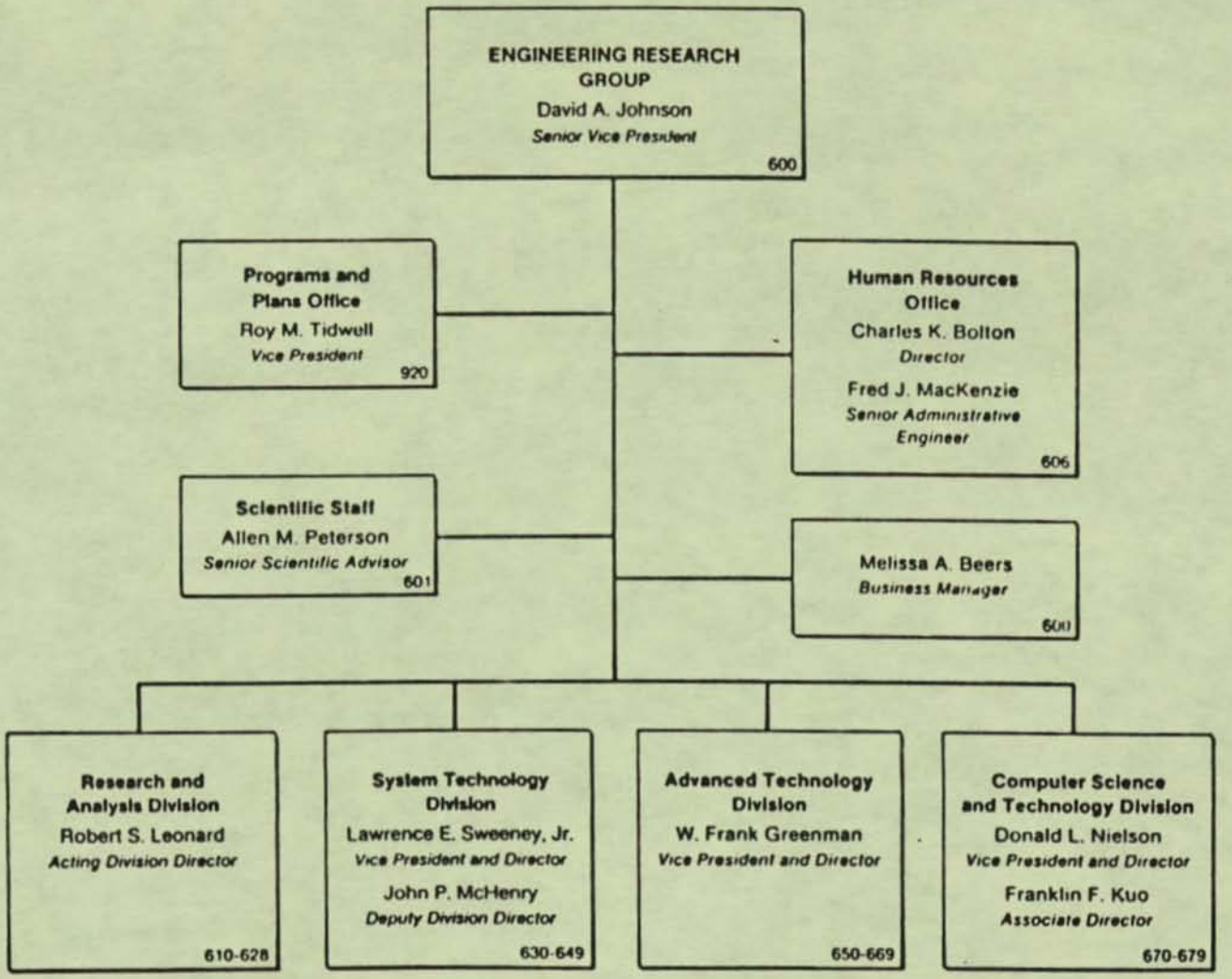


*A wholly owned subsidiary of SRI.

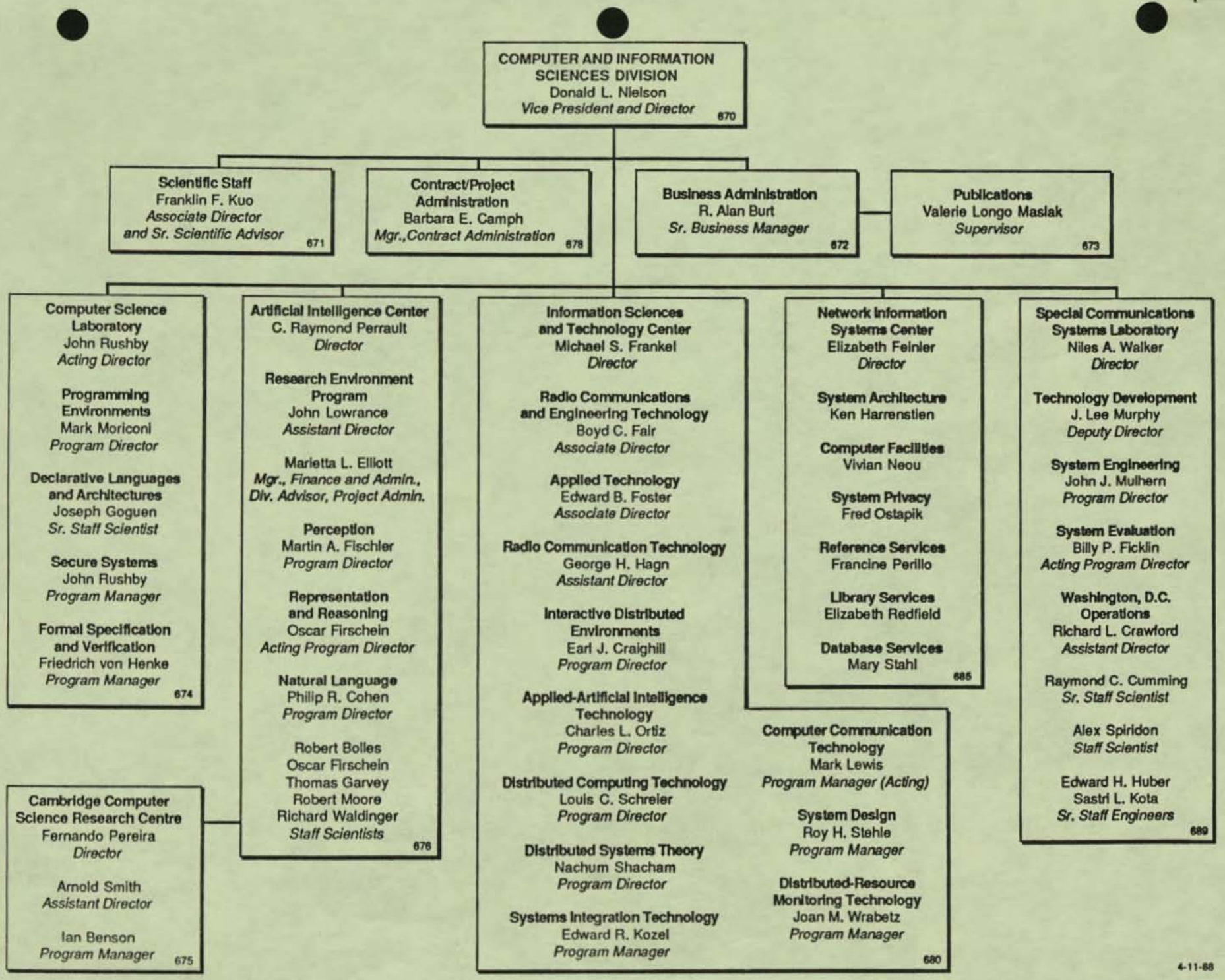
†President and Chief Operating Officer, DSRC.

ORGANIZATION CHARTS — 1000
OFFICE OF THE PRESIDENT — 1001

APPROVED
W. J. Miller

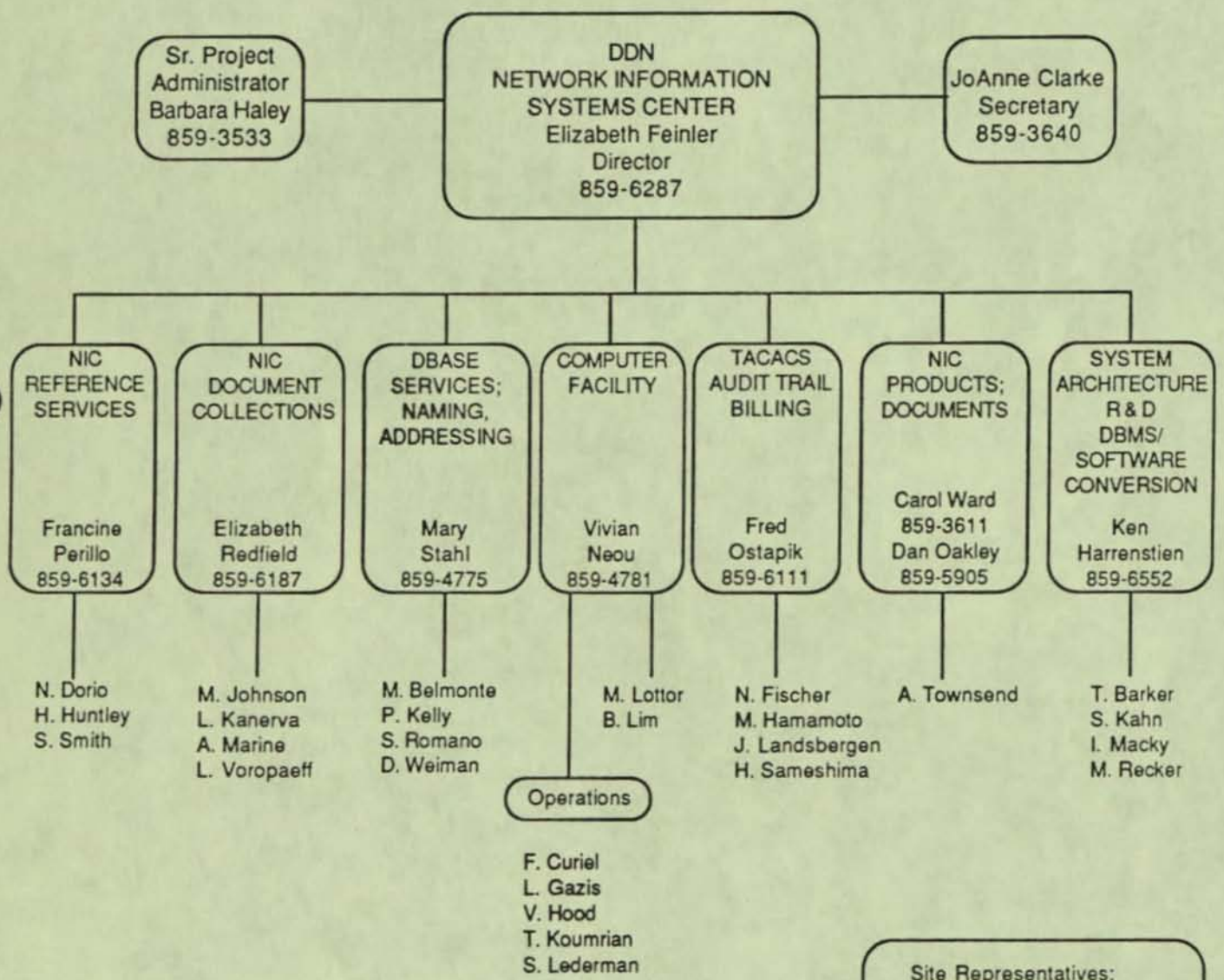


February 1986


COMPUTER AND INFORMATION SCIENCES DIVISION
Donald L. Nielson
Vice President and Director
670
Scientific Staff
Franklin F. Kuo
Associate Director and Sr. Scientific Advisor
671
Contract/Project Administration
Barbara E. Camph
Mgr., Contract Administration
678
Business Administration
R. Alan Burt
Sr. Business Manager
672
Publications
Valerie Longo Maslak
Supervisor
673
Computer Science Laboratory
John Rushby
Acting Director
Programming Environments
Mark Moriconi
Program Director
Declarative Languages and Architectures
Joseph Goguen
Sr. Staff Scientist
Secure Systems
John Rushby
Program Manager
Formal Specification and Verification
Friedrich von Henke
Program Manager
674
Artificial Intelligence Center
C. Raymond Perrault
Director
Research Environment Program
John Lowrance
Assistant Director
Marietta L. Elliott
Mgr., Finance and Admin., Div. Advisor, Project Admin.
Perception
Martin A. Fischler
Program Director
Representation and Reasoning
Oscar Firschein
Acting Program Director
Natural Language
Philip R. Cohen
Program Director
Robert Bolles
Oscar Firschein
Thomas Garvey
Robert Moore
Richard Waldinger
Staff Scientists
676
Information Sciences and Technology Center
Michael S. Frankel
Director
Radio Communications and Engineering Technology
Boyd C. Fair
Associate Director
Applied Technology
Edward B. Foster
Associate Director
Radio Communication Technology
George H. Hagn
Assistant Director
Interactive Distributed Environments
Earl J. Craighill
Program Director
Applied-Artificial Intelligence Technology
Charles L. Ortiz
Program Director
Distributed Computing Technology
Louis C. Schreier
Program Director
Distributed Systems Theory
Nachum Shacham
Program Director
Systems Integration Technology
Edward R. Kozel
Program Manager
Computer Communication Technology
Mark Lewis
Program Manager (Acting)
System Design
Roy H. Stehle
Program Manager
Distributed-Resource Monitoring Technology
Joan M. Wrabetz
Program Manager
680
Network Information Systems Center
Elizabeth Feinler
Director
System Architecture
Ken Harrenstien
Computer Facilities
Vivian Neou
System Privacy
Fred Ostapik
Reference Services
Francine Perillo
Library Services
Elizabeth Redfield
Database Services
Mary Stahl
685
Special Communications Systems Laboratory
Niles A. Walker
Director
Technology Development
J. Lee Murphy
Deputy Director
System Engineering
John J. Mulhern
Program Director
System Evaluation
Billy P. Ficklin
Acting Program Director
Washington, D.C. Operations
Richard L. Crawford
Assistant Director
Raymond C. Cumming
Sr. Staff Scientist
Alex Spiridon
Staff Scientist
Edward H. Huber
Sastri L. Kota
Sr. Staff Engineers
689
Cambridge Computer Science Research Centre
Fernando Pereira
Director
Arnold Smith
Assistant Director
Ian Benson
Program Manager
675
4-11-88

NIC HOTLINE (800) 235-3155
AREA CODE 415

DDN Network Information Systems Center
SRI International
Menlo Park, CA



Site Representatives:
HADMIN - E. Feinler
NSC - V. Neou
TECHNICAL POC - V. Neou

Person Behind Role Mailbox:
NIC - N. Dorio
ACTION - V. Neou
REGISTRAR - N. Fischer
HOSTMASTER - M. Belmonte
NEWS - F. Perillo
SUGGESTIONS - F. Perillo

6/14/88

OBJECTIVES

- Review NIC progress to date
- Clarify NIC processes and procedures
- Explore problem or bottleneck areas
- Propose solutions
- Agree on future effort

6/14/88

SOME REALITIES

- Funding is tight
- Deadlines are approaching
- A coordinated plan of action is needed

6/14/88

KEY ISSUES

- Billing system needed by Oct. 89
- Transition to domain naming system in progress
- OSI protocols replacing TCP/IP
- DCA revising data management procedures
- New network architectures being considered

6/14/88

HOW CAN SRI HELP?

- Provide objective technical expertise
- Provide liaison and coordination
- Interpret requirements in terms of future technology
- Assist with preparation of a technical "roadmap" that will leverage DCA effort
- Provide rapid prototyping and bootstrapping within military community
- Draw on years of experience in DDN environment

6/14/88

Milestone Schedule

February 1988 through January 1989
Task 1

CORE NETWORK INFO CENTER SERVICES

- 1a - USER ASSISTANCE SERVICES
- 1b - USER/RESOURCE DIRECTORY MAINTENANCE
  - WHOIS DB
  - NETWORK RESOURCES DB
  - PROTOCOLS DB
  - BIBLIOGRAPHIC DB
- 1c - TABLE/DATA ADMIN

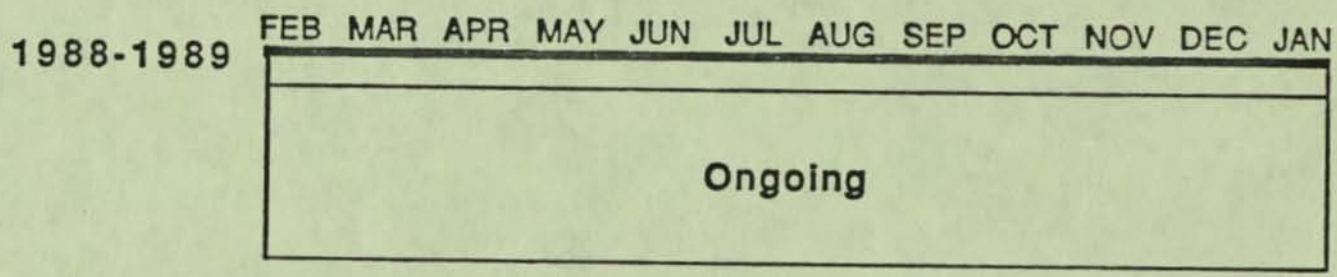
,CORE INFO CENTER SERVICES, Cont.

- 1d - TACNEWS, NOTIFICATION SERVICES, MGT BULLETINS
- 1e - NETWORK INFO SERVERS
- 1f - NCDS
- 1g - NAME/ADDRESS REGISTRATION
- 1h - LOCAL AREA CALLING LIST

Milestone Schedule

6/14/88

February 1988 through January 1989
Task 1a: User Assistance Services



Activities:

- Hotline Service (daily)
- Answering NIC@SRI-NIC.ARPA mail (daily)

6/14/88

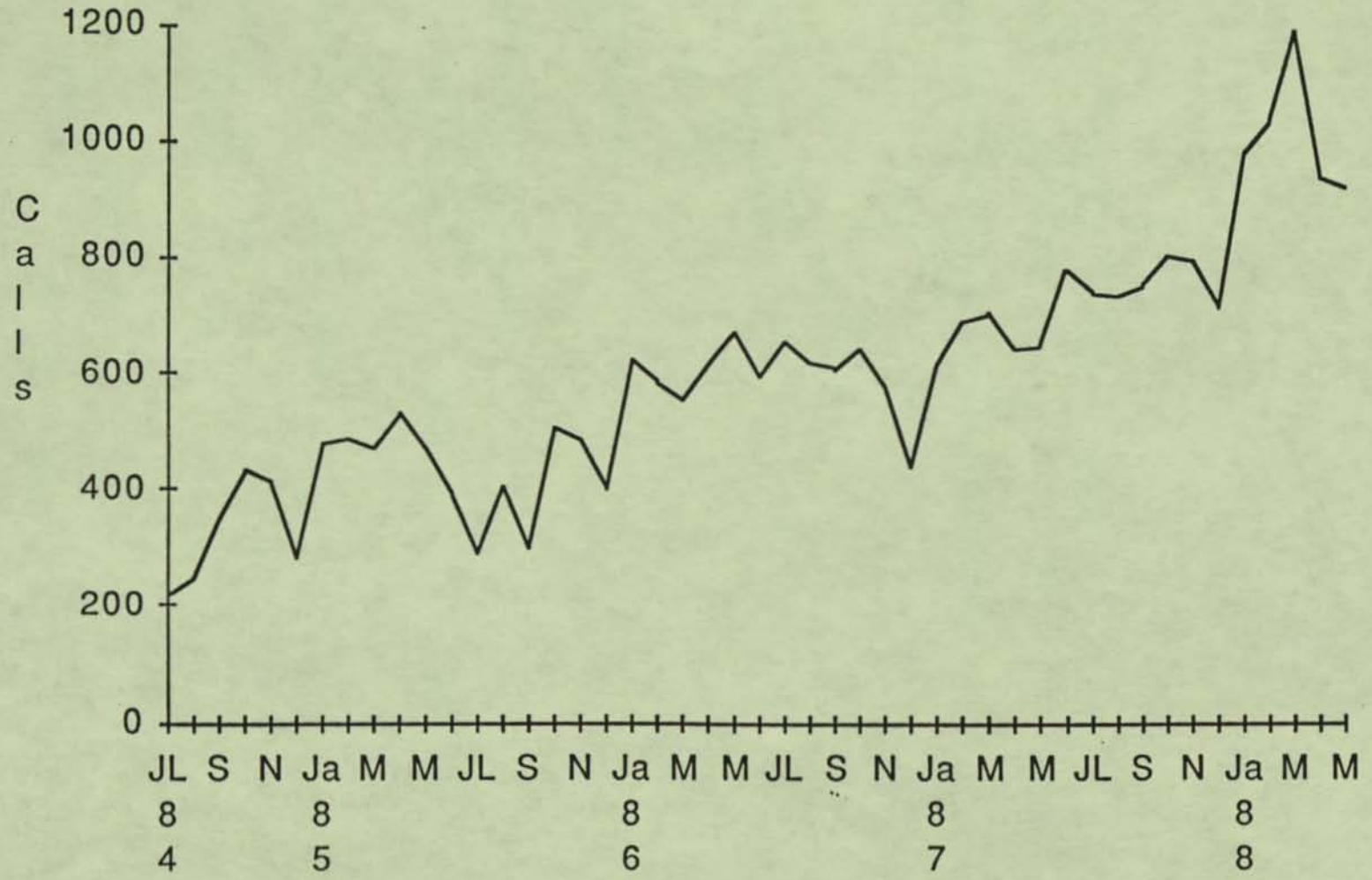
HOTLINE CALLS

Month	Totals
May 1987	652
May 1988	924

42% increase

DDN Hotline Usage

July 1984 - May 1988



6/14/88

NIC ROLE MAILBOX USAGE

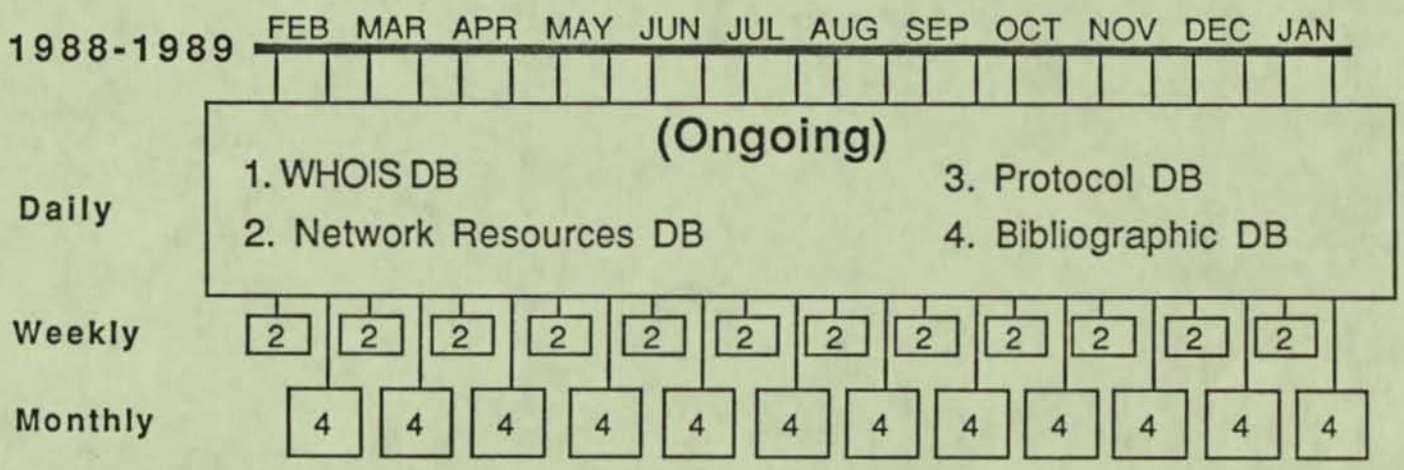
Mailbox	Usage	
	May 1987	May 1988
NIC	414	221
SERVICE	N/A	1568
REGISTRAR	1321	1486
HOSTMASTER	1231	1526
ACTION	407	217
TOTALS	3373	5018

49% increase

6/14/88

Milestone Schedule

February 1988 through January 1989
Task 1b



Activities:

1. WHOIS Database (updated daily)
2. Network Resource Database
   - TAC telephone list (daily)
   - NIC/QUERY files (weekly)
   - Online reference files (daily)
3. Protocol Database - DDN Protocol Implementations (daily)
4. Bibliographic Database (NICDOCS)
   - Data entry (daily)
   - Produce catalog & index (monthly)

6/14/88

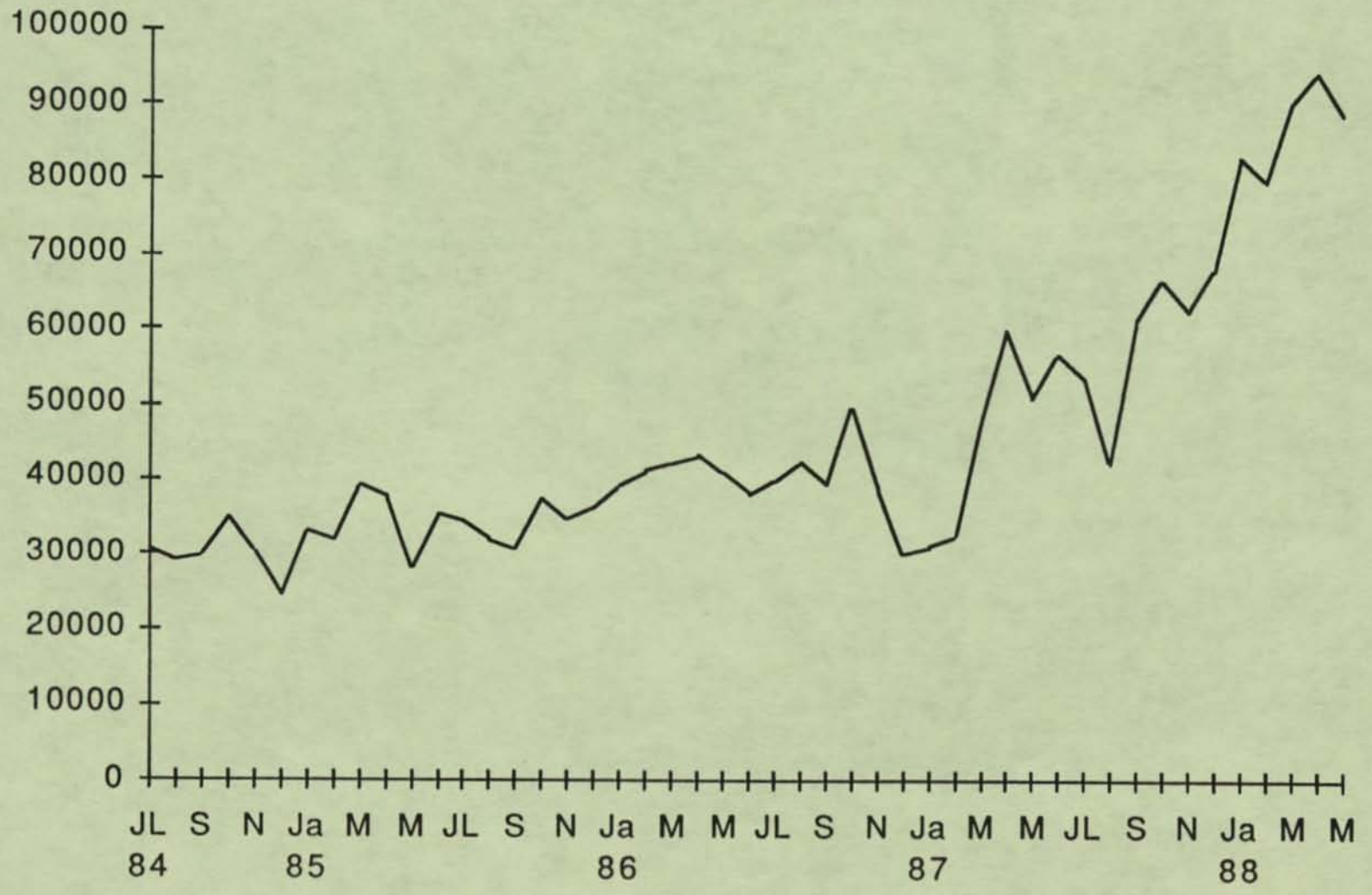
NETWORK INFO SERVERS

Service Name	Usage	
	May 1987	May 1988
WHOIS	51423	89265
TACNEWS	1817	1199
NIC/QUERY	2228	1342
TOTALS	55468	91806

66% increase

DDN Whois Usage

July 1984 - May 1988



6/14/88

NIC-MAINTAINED DIST. LISTS

List Name	List Count	
	July 1986	May 1988
POCs (HA, NSCs)	495	825
RFC List	679	603
TCP-IP List	423	419
NAMEDROPPERS	N/A	202

6/14/88

DDN PROTOCOL IMPLEMENTATIONS

Month	Totals
Products as of Feb 1987	194
Products as of Feb 1988	245

26% increase in one year

6/14/88

NIC DOCS DB

Month	Totals
May 1987	1923
May 1988	2527

31% increase in one year

6/14/88

Milestone Schedule

February 1988 through January 1989

Task 1d: TACNEWS, Notification Services, MGT Bulletins

Activities:

- TACNEWS Files (Update as needed)

- Newsletters, Mgt. Bulletins, Dist. Lists (Update as needed)

6/14/88

MGT BULLETIN ACCESS STATS

Filename	Totals
DDN-NEWS-23	1370
DDN-NEWS-36	1663
DDN-NEWS-37	1218
DDN-NEWS-38	1665
DDN-NEWS-39	1890
DDN-NEWS-40	1990
DDN-NEWS-41	1172
DDN-NEWS-43	747
DDN-NEWS-44	1036
DDN-NEWS-45	926
DDN-NEWS-46	885
DDN-NEWS-47	802
DDN-NEWS-48	504
DDN-NEWS-50	864
DDN-NEWS-51	1937
DDN-NEWS-52	1310
DDN-NEWS-55	178
DDN-NEWS.INDEX	12999

6/14/88

NEWSLETTER ACCESS STATS

Filename	Totals
DDN-MGT-BULLETIN-12	951
DDN-MGT-BULLETIN-17	1166
DDN-MGT-BULLETIN-18	1033
DDN-MGT-BULLETIN-20	1033
DDN-MGT-BULLETIN-22	1554
DDN-MGT-BULLETIN-26	779
DDN-MGT-BULLETIN-27	1063
DDN-MGT-BULLETIN-28	1304
DDN-MGT-BULLETIN-30	1519
DDN-MGT-BULLETIN-31	1025
DDN-MGT-BULLETIN-32	883
DDN-MGT-BULLETIN-33	821
DDN-MGT-BULLETIN-34	360
DDN-MGT-BULLETIN-35	420
DDN-MGT-BULLETIN-36	465
DDN-MGT-BULLETIN-37	416
DDN-MGT-BULLETIN-38	457
DDN-MGT-BULLETIN-39	485
DDN-MGT-BULLETIN-40	164
DDN-MGT-BULLETIN.INDEX	8874

6/14/88

NEW TACNEWS LOCATOR

Features

- Quick Look-up
- Provides three different TAC numbers
- Locates TACs on either MILNET or ARPANET
- Removes guesswork of finding nearest TAC

6/14/88

SUMMARY OF TAC NO. SERVICES

- TAC phone numbers printed on TAC cards
- CONUS TAC phone list
- EUR/PAC TAC phone list
- TAC Locator

6/14/88

DOCUMENTS SHIPPED, 1988
as of 06/10/88

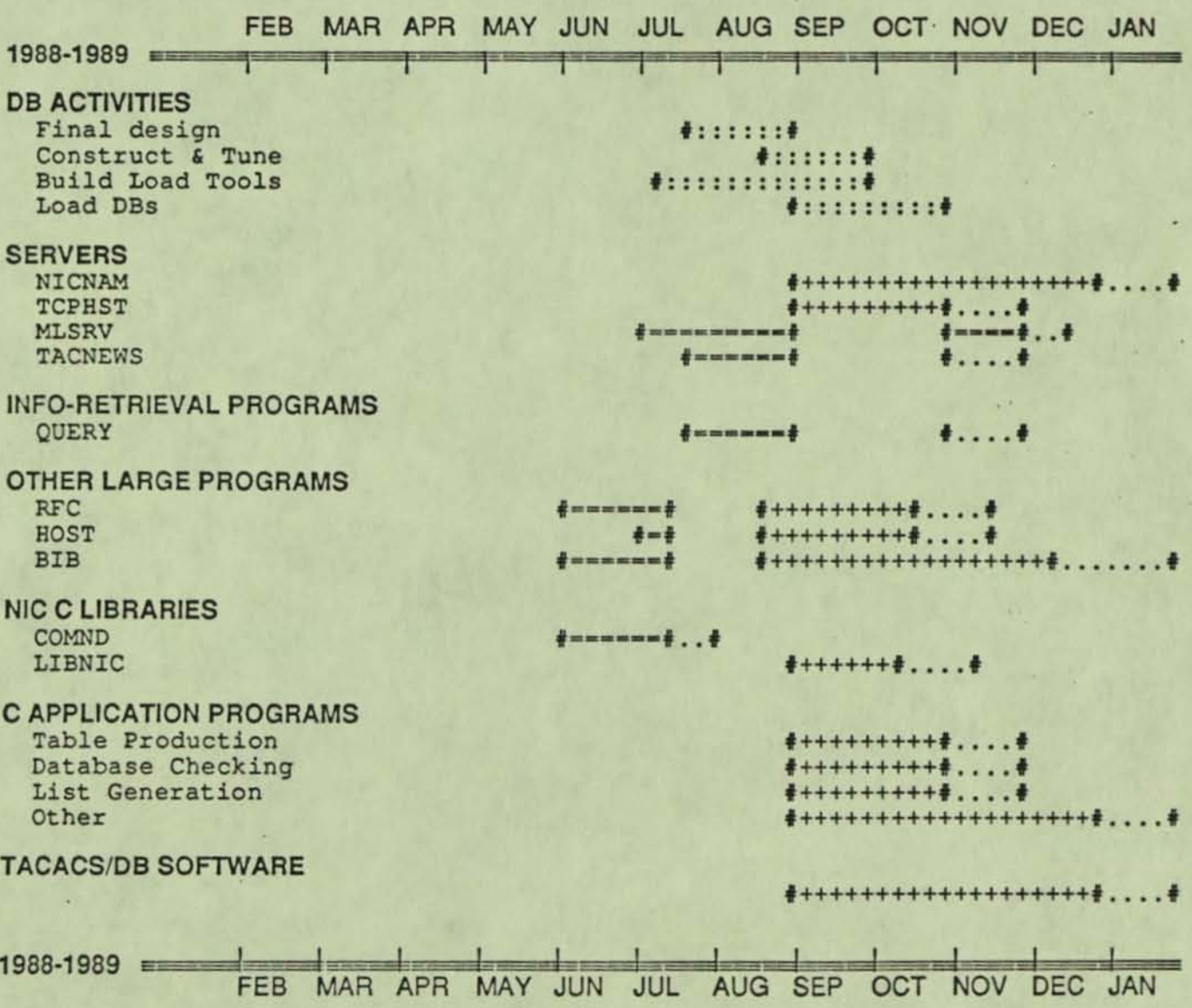
ARPANET Information Brochure	71
DDN New Users Guide	177
DDN Protocol Handbook	451
DDN Protocol Impl. and Vend. Guide	179
DDN Subscriber Interface Guide	104
DDN Subscriber Security Guide	65
DDN X.25 Specifications	73
RFCs	2,375
RFC Subscriptions	67

Milestone Schedule

February 1988 through January 1989
Task 2 - Software Conversion

Legend:

* Current location	+ DB Conversion
# Start or Complete Work	. Documentation & Testing
= UNIX Conversion	: Other



6/14/88

SOFTWARE CONVERSION STEPS

- Convert software to C-Language
- Convert software to UNIX operating system
- Convert software to use Ingres data base
- Test

6/14/88

INGRES INSTALLATION PROBLEMS

- All SUN equipment has been delivered
- Delivery slipped from Oct 87 to May 88
- The SUN 4/280 data-gathering machines only run under SUN OS 4.0
- Falcon did not deliver SUN OS 4.0
  (We are resolving this now)
- Ingres 5 (current) only runs on SUN OS 3.4
- Ingres 6 will run on SUN OS 4.0
- Ingres 6 will not be available until Aug-Nov 88

DBMS STRATEGIES

SOLUTIONS / IMPACT	1 Run both OSs	2 Use VAX-780	3 Wait
	Two Networks: Use SUN OS 4.0 on SUN-4s and on SUN-3s Use SUN OS 3.4 on SUN-3s	Use SUN OS 4.0 on all	Use SUN OS 4.0 on all
IMPACT	Install Ingres 5 on SUN OS 3.4 Switch when Ingres 6 available Aug-Nov?	Install Ingres on SRI VAX 780 Move when Ingres 6 available	Convert DB software when Ingres 6 available
COST	No additional cost for Ingres 5 to 6 upgrade	$40,000 +	
LABOR	Double Ingres installation Double SUN OS maintenance Conversion from 5 to 6	Double Ingres installation Conversion from 5 to 6	
SCHEDULE	Tight	Tight	May not finish by Jan 89
OTHER		May impact other SRI work	

ONGOING PROGRAMMING ACTIVITIES

All TASKS

- Maintenance of Current TOPS-20 Based Programs
- Programming Support of Naming and Addressing Work
- Modifying TACACS Registration Programs to Meet New Requirements
- Creating New Table Generation Programs As Needed
- Software Conversion Efforts

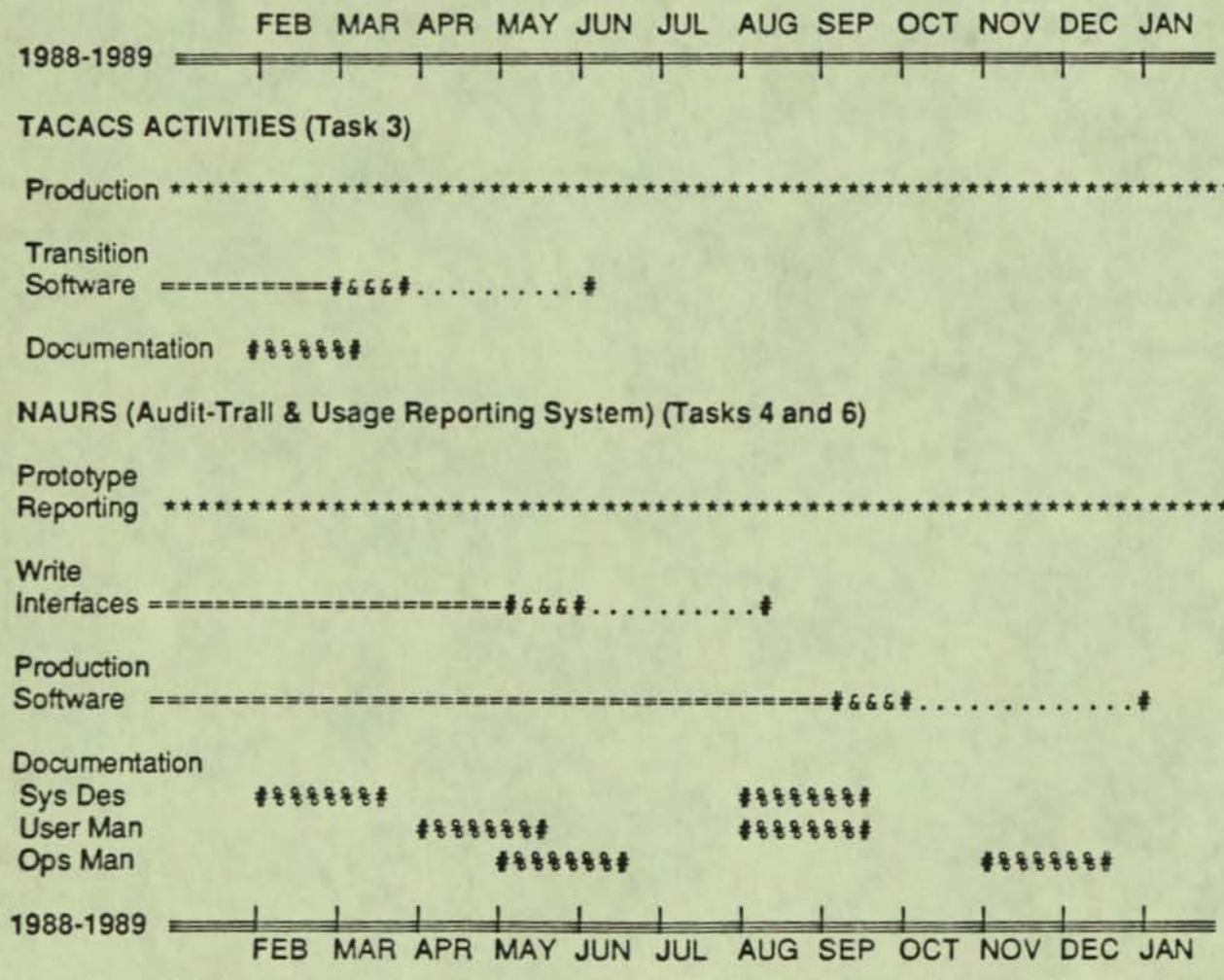
3/11/88

Milestone Schedule

February 1988 through January 1989
Tasks 3, 4 and 6

Legend:

# Start or Complete Work	& Software installation
* Ongoing production	. Testing & Implementation
= C/UNIX Conversion	% Documentation



6/14/88

MILNET REGISTRATION STATUS

- Operational and stable
- Reregistration proceeding smoothly
- Currently keeping on top of operational needs
  - Processing registration mail
  - Answering phone queries
  - Providing HAdmin training
  - Generating and mailing TAC Cards

6/14/88

ARPANET REGISTRATION STATUS

- System in transition
- Moving to same registration procedures as MILNET
- Will use same Userid scheme
- Will have HAdmin approval for both systems
- Data base clean-up taking place

6/14/88

POTENTIAL PROBLEM AREAS

- Current system barely meets today's needs
- Hotlist limits soon will be exceeded
- Incompatibility with ARPANET
- Incompatibility with NACs
- Rapid increase in hosts/HAdmins/NACs
- Too many untrained, unreachable HAdmins

6/14/88

SOLUTIONS

- Move to TAC Release 114
- Proceed with MILNET login hosts
- Eliminate hotlist system
- Standardize MILNET/ARPANET registration
- Provide HAdmins with registration training kit

6/14/88

AUDIT TRAIL - CURRENT STATUS

- Prototype running; meets specs and requirements
- New equipment delivery has slipped (May 88 vs Oct 87)

6/14/88

AUDIT TRAIL - NEXT STEPS

- Implementation of new equipment now targeted for 31 Jul 88
- Installation of prototype software on new equip now targeted for 31 Sep 88
- Installation of Ingres now targeted for Sept-Oct 88
- Implementation of production features by Dec 31
    - Real-time analysis
    - Integration with Ingres
    - Integration with usage/billing reporting system

6/14/88

AUDIT TRAIL - PROBLEM AREAS

- No resolution of Audit-trail V2 protocol issues
- V2 protocols dependent on TAC Release 114
- Lack of coordination NIC/NMCs/BBN/DCA
- Impact on Usage/billing
  - V2 protocols have precedence info
  - V2 has receive/send breakdown

6/14/88

SRI BILLING SYSTEM - STATUS

- Prototype system is running; meets specs
- Reporting system is modifiable
  - to meet Oct. 1989 deadline requirements
  - to be ported into DISNET environment

6/14/88

SRI BILLING SYSTEM - PROBLEMS

- File delivery problems from BBN
- Incomplete NCD data being delivered
- Lack of coordination NIC/NMCs/BBN/DCA

6/14/88

SUGGESTIONS
OPERATIONS/DATA FLOW

- Locate usage-data MC at SRI
- NIC operators could then monitor the MC
- Transfer data directly from MC to NAURS and eliminate slow FTP through busy PSN 73

6/14/88

SUGGESTIONS - DISNET PORTING

- Place PSN and UDH in SCIF environment at SRI
- Maintain WHOIS as unclassified db as it is being done for MILNET
- Blank DISNET TAC user info from general access in WHOIS
- Port billing data from WHOIS to secure UDH
- UDH -> PSN -> DDN -> DISNET all KG encrypted except physically secure connection from UDH to PSN
- Porting would only involve NAURS
- No need to classify WHOIS db to support DISNET
- DISNET host info already processed by NCDs

6/14/88

Milestone Schedule

February 1988 through January 1989
Task 1c

1988-1989	FEB MAR APR MAY JUN JUL AUG SEP OCT NOV DEC JAN
	Ongoing **Twice Weekly** 1, 2
	Ongoing **Once Weekly** 3, 4
	Ongoing **Daily** 5, 6

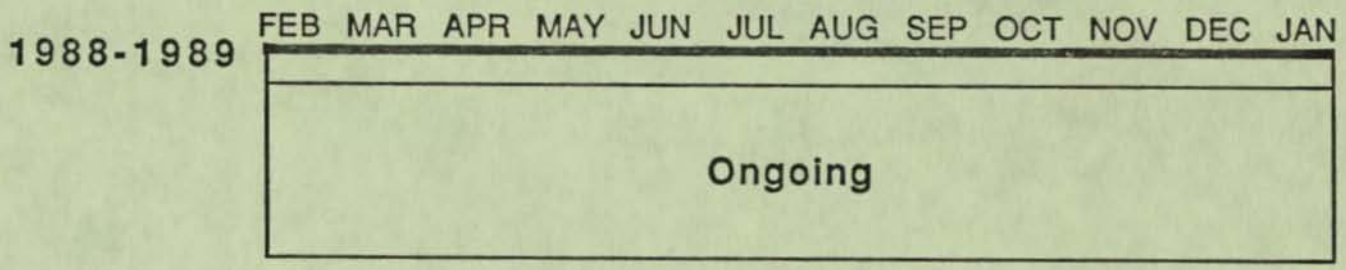
Activities:

1. Official DoD Internet Host Table (twice weekly)
2. Domain system root files (twice weekly)
3. NSC and HA distribution lists (weekly)
4. Supplementary host files (weekly)
5. NCDs/NCANs - monitor and maintain (daily)
6. WTRs/HLs/DSRs - monitor and maintain (daily)

6/14/88

Milestone Schedule

February 1988 through January 1989
Task 1f



Activities (now under task 1c):

- NCDs/NCANs - monitor and maintain (daily)
- WTRs/HLs/DSRs - monitor and maintain (daily)

6/14/88

DATA COLLECTION STATUS

NCD Problems

- Unclear purpose statement
- Missing or incorrect data
- Nonstandard and confusing data
- Numerous untrained NCD preparers
- No notification of template changes

6/14/88

DATA COLLECTION STATUS

Impact of Bad NCD Data

- Corrupts operational host tables and billing reports
- Wastes time and money
- No way to verify data with HAdmins and NSCs
  - Incomplete name or address info
  - No E-mail
  - No commercial phone number

6/14/88

DATA COLLECTION STATUS

NCDs - What is Needed

- Standardization
- Data Conformity
- Machine-readable format
- Simplification
  - Have POCs create SAFs
  - Give POCs access to data
- More coordination between NIC and net mgrs
- Procedure manual (with cooperation)

6/14/88

DATA COLLECTION STATUS

NCDs - How SRI Can Help

- Develop NCD data input program with built-in training
- Lead working group to standardize data
- Coordinate and train POCs
- Prepare procedure manual

6/14/88

DATA COLLECTION STATUS

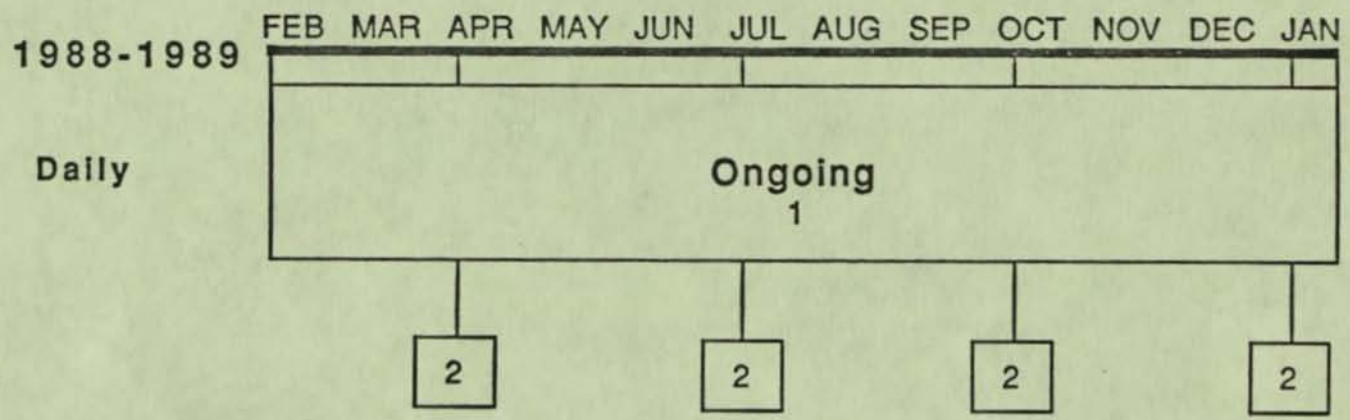
Recent Improvements

- MILNET and ARPANET now using same form
- More communication with net managers begun
- No more duplicate copies

6/14/88

Milestone Schedule

February 1988 through January 1989
Task 1g



Activities:

1. Name and Number Registration (daily)
   - IP networks
   - Autonomous systems
   - Domains
   - Hosts/gateways/TACs
2. Internet Numbers RFC (quarterly or as needed)

6/14/88

DDN GROWTH

NETWORK NAMING AND ADDRESSING STATISTICS

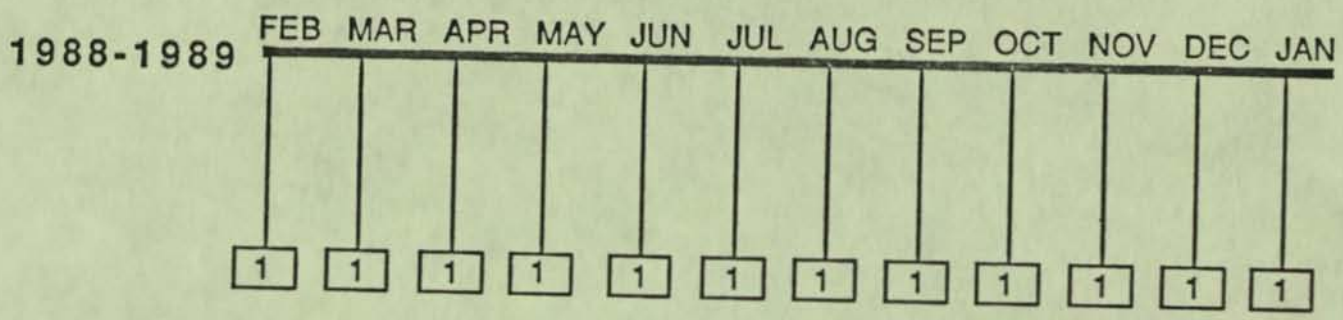
	May 1987	May 1988	Increase
ARPANET/MILNET Hosts	820	1717	110%
Internet Hosts (includes ARPA/MIL)	4,178	5,639	35%
ARPANET/MILNET TACs	148	189	28%
ARPANET/MILNET GWs	134	180	34%
Internet GWs (includes ARPA/MIL)	182	240	32%
ARPANET/MILNET Nodes	217	259	19%
Connected Networks	637	915	44%
Domains (top-level, 2nd-level)	328	546	67%
Hostmaster online mail	979	1526	56%
NCD online mail	252	819	225%

(Size of current host table = 607,577 bytes)

6/14/88

Milestone Schedule

February 1988 through January 1989
Task 1h



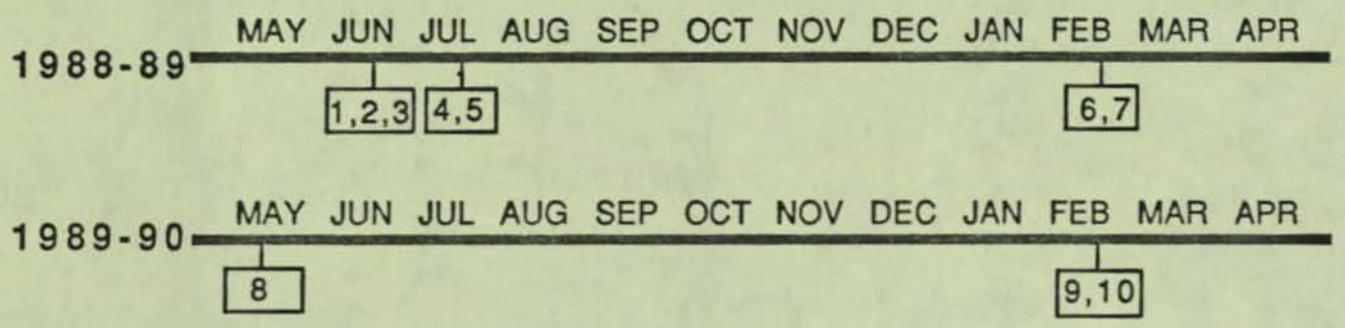
Activities:

Local Area Calling List (monthly)

6/14/88

MILNET Domain Name Transition

Task 5



Milestone Description

1. NIC preparations
2. Issue DDN Management Bulletin
3. Identify "MIL" subdomain groupings according to sponsoring agency
4. No new "ARPA" registrations accepted
5. Begin 7-month notification period; begin adding "MIL" nicknames
6. End HA notification period
7. Switch nicknames and primary names
8. "Exception group" name changes completed
9. Eliminate "ARPA" nicknames
10. Name transition completed

6/14/88

MILNET DOMAIN NAME TRANSITION

NIC Preparation for Transition

- Write RFCs
- Compose DDN Management Bulletin
- Identify all hosts by sponsor
- Specify new names for hosts
- Send email message to HAdmins
- Prepare input file for mass DB changes
- Modify and test MAKEZ program

6/14/88

MILNET DOMAIN NAME TRANSITION

During the Transition

- Maintain host tables
- Provide root domain name server tables
- Provide domain name service for net 26
- Continue to register domains

6/14/88

DOMAINS AND HOSTS
REGISTERED WITH DDN NIC

Top-level domains	=	33
2nd-level domains	=	513
Hosts in.CA	=	2
Hosts in.COM	=	421
Hosts in .EDU	=	2436
Hosts in .GOV	=	325
Hosts in .IL	=	1
Hosts in .IT	=	3
Hosts in .MIL	=	199
Hosts in .NET	=	20
Hosts in .NL	=	2
Hosts in .NO	=	3
Hosts in .ORG	=	21
Hosts in .UK	=	11
Hosts in .US	=	1
Hosts still in .ARPA	=	2642

143 (net 10)

1729 (net 26)

770 (other nets)

TASK 9 - DDN NIC COMPUTER FACILITY

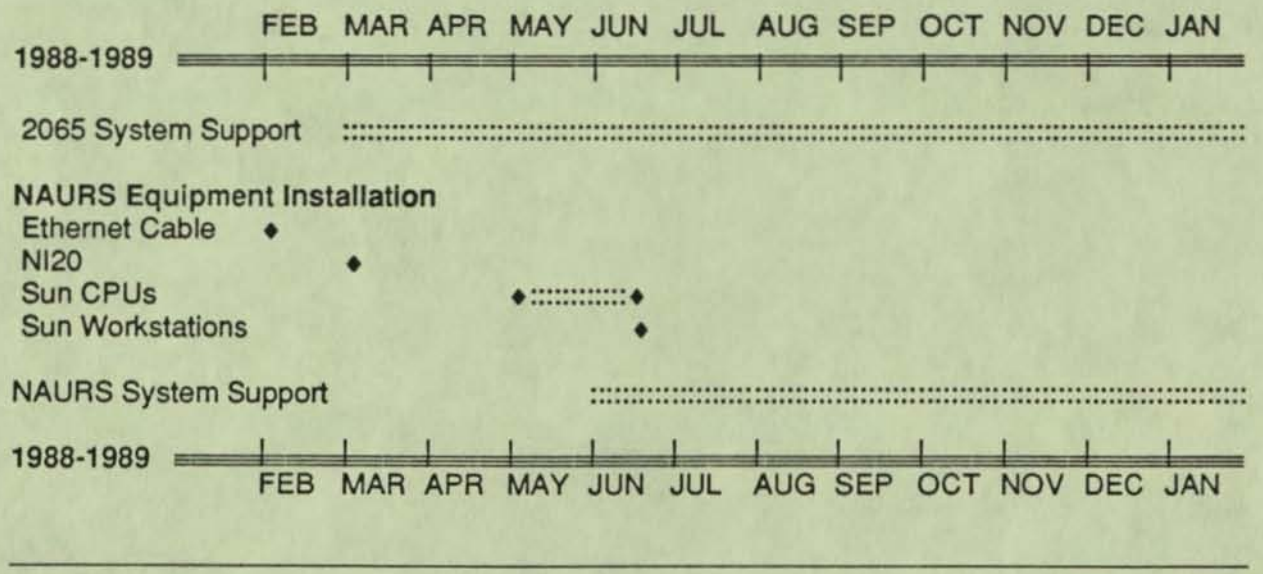
- 9a System Uptime
- 9b Access Control
- 9c System Services
- 9d GFE Equipment
- 9e Off-site Storage
- 9f Node Site Coordinator
- 9g TACACS System

6/14/88

Milestone Schedule

February 1988 through January 1989
Task 9 and Computer Facility

Legend:
♦ Start or Complete Work
: On-going Work



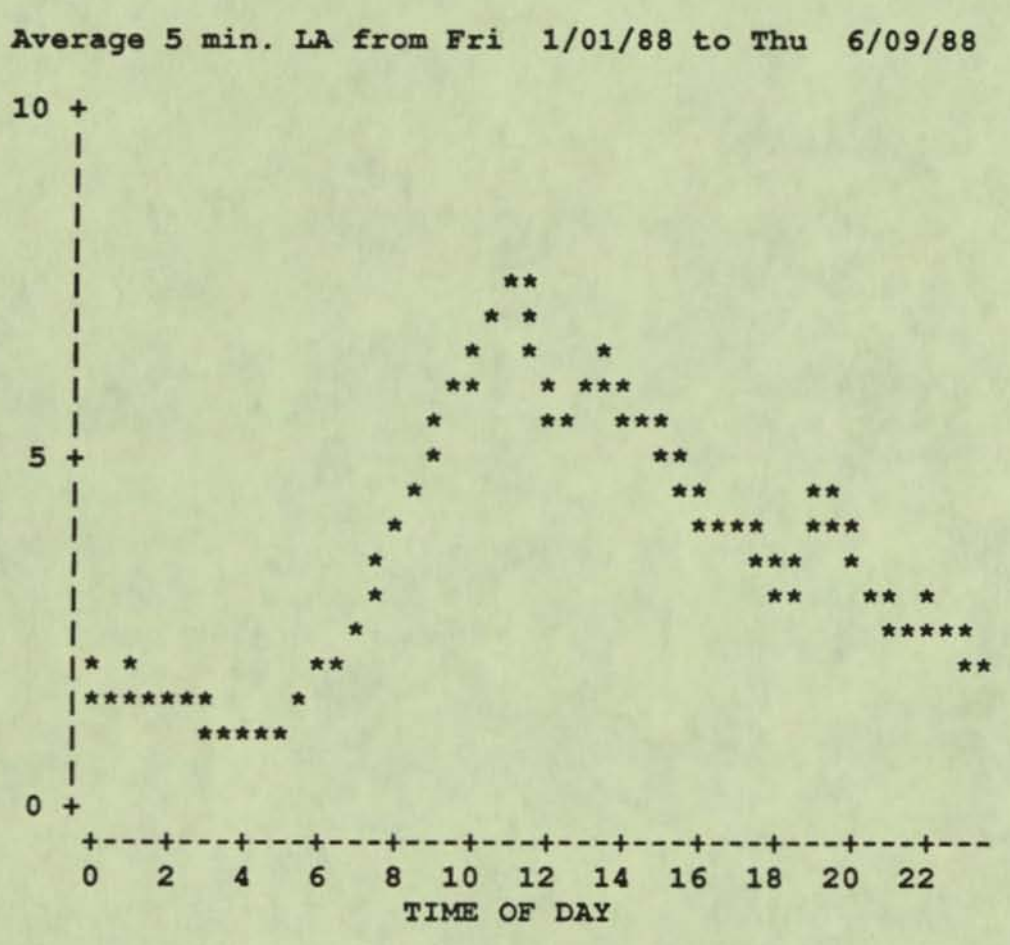
COMPUTER FACILITY ON-GOING TASKS

- Maintain operational facility. Includes SRI-NIC.ARPA and NAURS equipment (F4, Sun fileservers, workstations and CPUs).
- Support for GFE equipment. Includes: Mail Bridge, Login Host, Packet Switches, MicroVAX, and TAC
- Butterfly gateway support for DARPA. Butterfly is now part of the ARPANET backbone, and requires regular attention.
- Act as Node Site Coordinator for PSNs and TAC
- Provide off-site storage for copies of NIC software. Provide storage procedures as requested for CDRL A009.

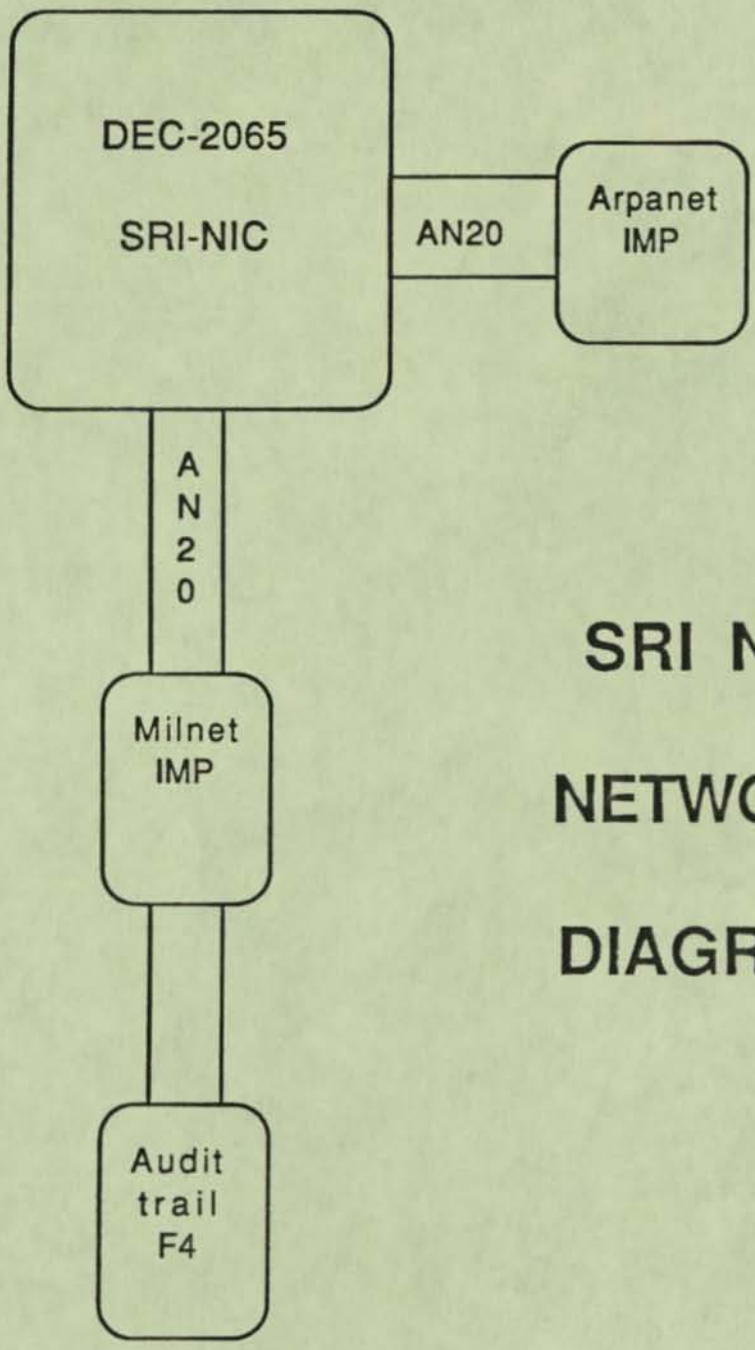
COMPUTER FACILITY ACCOMPLISHMENTS

- Installed SUN systems for SRI-NAURS replacement
- Installed new version of Domain software on SRI-NIC.ARPA
- Installed Ingres on MicroVAX. Working with BBN to bring up UDH system on MicroVAX.
- Installed CPU board upgrade on MILNET-ARPANET Gateway

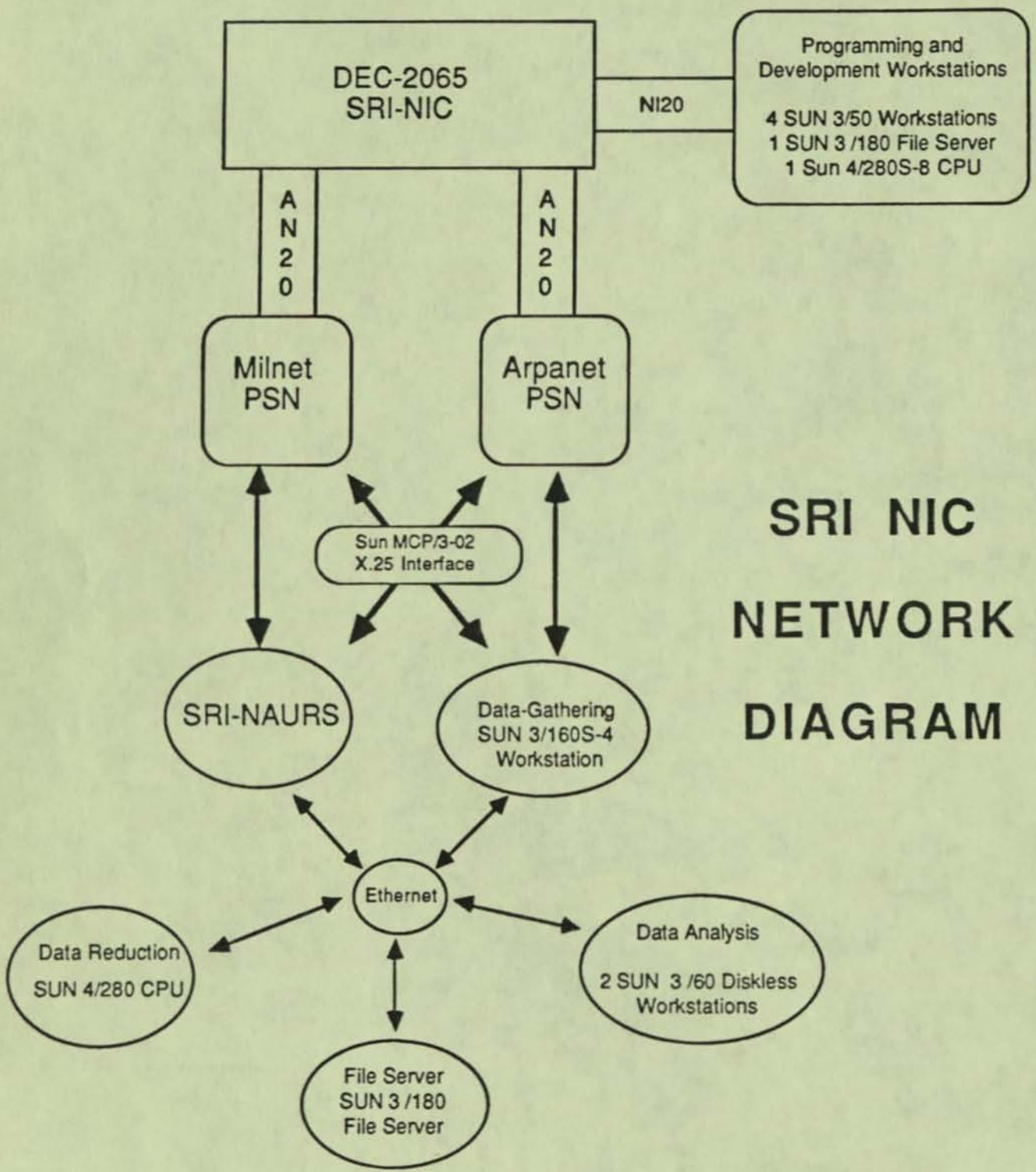
SRI-NIC IS OVERLOADED



- Increase the amount of memory by 1 MW. (~$9,000)
- Migrate some users to other systems.
- Move some of the servers to other systems.



SRI NIC NETWORK DIAGRAM



SRI NIC NETWORK DIAGRAM

NAURS (SUN EQUIPMENT) INSTALLATION PROBLEMS

The current NAURS system (F4) must be phased out by September. Maintenance support by McDonnell Douglas ends at that time.

- We are waiting for assignment of Milnet PSN ports.
- Sun 4OS has not yet been delivered. It is needed in order to install the Sun 4/280s.
- Sun Link software will currently only run under Sun 3OS, so it will be necessary to have two versions of Sun OS running on the network.
- Waiting for final approval to purchase Sun sources.

CURRENT NAURS (F4) PROBLEMS

Problem: Have not been able to consistently gather audit trail data or generate TAC Cards since May 24.

- Constant communication with the MMC over the past three weeks has not solved the problem.
- The personnel at the trouble desk do not track the problem in a consistent manner. We have had to reopen the call several times although final resolution was not reached.
- Field engineers have been dispatched 3 times. The boards relating to that port have been completely replaced three times.
- TAC cards that were generated while the system was working on June 2 were incorrect.
- Problem could have been caused by an upgrade to PSN 7. SRI was not given any advance warning that PSN 7 was being loaded.

2747-88

DEFENSE COMMUNICATIONS AGENCY

DEFENSE MESSAGE SYSTEM (DMS) TARGET ARCHITECTURE AND IMPLEMENTATION STRATEGY (TAIS)

DECEMBER 1988

The

Defense Message System (DMS)

Target Architecture

and

Implementation Strategy

Prepared By:

Defense Message System Implementation Group

Sponsored By:

Office of the Assistant Secretary of Defense

for
Command, Control, Communications and Intelligence
(Information Systems)
Pentagon, Washington D.C.

December 1988

TABLE OF CONTENTS

TABLE OF CONTENTS
Continued

TABLE OF CONTENTS
Continued

TABLE OF CONTENTS
Continued

TABLE OF CONTENTS
Continued

List of Appendices

TABLE OF CONTENTS
Continued

List of Figures

Preface

This document, the Defense Message System (DMS) Target Architecture and Implementation Strategy (TAIS), was initiated by the Defense Message System Working Group (DMSWG) which was constituted in January 1988 by ASD(C3I) to evaluate the future of DoD's messaging systems in light of the Inter-Service/Agency Automated Message Processing Exchange (I-S/A AMPE) Program termination. Primary DMSWG objectives were to define the baseline DMS and reliably estimate its cost to the DoD and to formulate a target DMS architecture and implementation strategy based on achievable technology that satisfies writer-to-reader requirements while reducing cost and staffing and maintaining services. Secondary objectives were improvements in functionality, survivability and security. This document is intended to demonstrate that the enclosed DMS target architecture will satisfy mission essential requirements, and that the accompanying implementation strategy will allow the DMS to be developed, tested and implemented in a resource constrained environment.

The recently established DMS Implementation Group has coordinated this document with all Services and agencies and obtained authorization to release it to Government and industry. Recommended changes and other comments to this document are welcome. The intent is that the DMS TAIS be a "living document" continually being updated as requirements, plans and technology change. Reproduction of this document in whole or in part is authorized but care should be taken to ensure that additional recipients are added to the Appendix D distribution list or that they receive subsequent updates by other means. Comments to the document and distribution list changes should be forwarded to the address provided below.

For industry recipients: This document is provided for information only and should not be considered a solicitation. Inputs from industry are welcome but will be used for planning purposes only. The Government does not intend to award a contract based on this document (to include subsequent updates) or otherwise pay for inputs submitted by industry as the result of this document. Inputs should be mailed to the address provided below. Written inputs will facilitate distribution and review by the proper Government audience. Subsequent to written inputs, presentations to the DMS Implementation Group (DMSIG) or its Working Groups may be arranged through the Points of Contact listed below. Scheduling of such presentations will be at the discretion of the DMSIG Chair.

DMS TAIS Office of Primary Responsibility:

Defense Communications Agency
ATTN: Code B604
Washington, D.C. 20305-2000

Points of Contact: Mr. Thomas W. Clarke (703) 285-5392
MAJ Paul D. Grant (703) 285-5131

DMS Architecture

Section 1

Introduction

1.1 Background.

A Multi-Service and agency Defense Message System Working Group (DMSWG) was formed by ASD/C3I (IS) in January 1988 to assess the future of DoD's messaging systems given termination of the Inter-Service/Agency Automated Message Processing Exchange (I-S/A AMPE) Program and the imposition of severe budget constraints. Primary objectives were to define the baseline DMS and reliably estimate its cost to the DoD and to formulate a target DMS architecture based on achievable technology that satisfies writer-to-reader requirements while reducing cost and staffing and maintaining services. Secondary objectives were improvements in functionality, survivability and security. As an initial task, a request for information (RFI) from industry was formulated and distributed to obtain industry comments on architectural alternatives and component availability. RFI responses, current Service and agency architectural plans, ongoing efforts such as NSA's Commercial COMSEC Endorsement Program (CCEP) and Secure Data Network System (SDNS) program, and protocol standardization initiatives such as the Government Open Systems Interconnection Profile (GOSIP), were reviewed and factored into formulation of a recommended target architecture and the transition phases necessary to evolve from the baseline to the target. The phased DMS implementation strategy specifies the objectives and actions for each phase of the evolution from the baseline to the target. A preliminary review of the DMS Target Architecture and Evolutionary Implementation Strategy was presented to the C3I Systems Committee of the Defense Acquisition Board (DAB) on 25 May 1988. The Committee approved, in concept, a management structure and implementation strategy outlined in this document as the basis for further work on the DMS, subject to a reevaluation when DMS requirements are validated and initial funding and schedule baselines are confirmed. On 3 August 1988, the Under Secretary of Defense for Acquisition issued DMS Program Guidance, providing conceptual approval of the DMS architecture, implementation strategy, test and evaluation strategy, and management structure, tasking the Defense Communications Agency with responsibility for overall DMS coordination, and providing initial tasking to the Services and agencies necessary to begin execution of the DMS implementation strategy.

1.2 Definitions.

The following terms, used frequently in this document, are defined as follows:

1.2.1 Defense Message System (DMS): The DMS consists of all hardware, software, procedures, standards, facilities, and personnel used to exchange messages electronically between organizations and individuals in the Department of Defense (DoD). The DMS must be interoperable with and provide

standard interfaces for tactical and allied systems but does not include those systems. The major components of the baseline DMS are the AUTODIN System, including the baselevel Telecommunications Centers (TCCs) and Electronic Mail (E-Mail) on the DoD Internet. Currently, the DoD Internet consists of the Defense Data Network and associated Local Area Networks.

1.2.2 DMS Projects/Components: DMS components are the hardware, software, procedures, etc. currently existing in the baseline and postulated hardware, software, procedures, etc., required to achieve the target architecture. DMS projects are efforts required to acquire the needed components, develop the needed procedures, etc. The DMS projects and components fall into one of the following three classes:

a. "Central": DMS "Central" projects and components are those that are acquired or developed to support the core architecture and all users of the DMS. In general, they can be characterized as backbone components or major policies and standards. Examples of "Central" projects and components in the baseline are Defense Communications System (DCS) Mode I protocol, Simple Mail Transfer Protocol (SMTP) and other DoD standard protocols, ACP 117 CAN-US SUPP-1, the Message Address Directory (MAD), the AUTODIN backbone and electronic mail service via the DDN. Since "Central" DMS projects and components support all users, the active participation and support of all Services and agencies in their development, testing and deployment is necessary.

b. "Joint": DMS "Joint" support projects and components are individual Service or agency projects or components that show maximum likelihood of satisfying operational needs within other Services and agencies and advancing the DMS architecture. Support of these projects will avoid duplication of development efforts and promote standardization of components. Examples of opportunities for "Joint" projects and components in the baseline are the replacements for the Standard Remote Terminal (SRT), Digital Subscriber Terminal Equipment (DSTE), and Digital Communications Terminal (DCT) 9000 equipments.

c. "User Unique": DMS "User Unique" projects and components are those which are developed or acquired by a single Service or agency to satisfy unique operational requirements. They will conform to the intent of DMS architectural guidelines, except where dictated by unique requirements. Examples of "User Unique" projects and components in the baseline include use of office codes in message preparation, procedures for message distribution, the Service and agency AMPEs, implementation of local area networks and Automated Message Handling Systems (AMHSs), Remote Information Exchange Terminal (RIXT) and Modular AMME Remote Terminal (MART) software for the SRT, all unique AUTODIN interfaces and terminals in use at TCCs, and electronic mail hosts on the DDN.

1.2.3 DMS Message: The term "message" is defined in ACP 167, "Glossary of Communications - Electronics Terms", to be "any thought or idea expressed briefly in plain or secret language, prepared in a form suitable for

transmission by any means of communications." In the DMS context, the means of communications is restricted to common-user electronic methods. DMS messages fall into one or the other of the following classes:

a. Organizational: This class includes command and control messages and communications exchanged between organizational elements. These messages require approval for transmission by designated officials of the sending organization and determination of internal distribution by the receiving organization. Because of their official and sometimes critical nature, such messages impose operational requirements on the communications systems for capabilities such as non-routine precedence, guaranteed timely delivery, high availability and reliability, and a specified level of survivability.

b. Individual: This class includes working communications between individual DoD personnel within administrative channels, both internal and external to the specific organizational element. Such messages do not generally commit or direct an organization. Information messages and those requiring only a basic transport service will be treated as a part of this class. The driving requirements on the communications system for this class of messages are connectivity down to the level of the individual and ease of use for the individual users.

1.3 Scope.

While the DMS is a system in the sense that its components work together to perform a function, it is, and will continue to be, the result of many separate development and acquisition activities. In the baseline, the DMS currently encompasses three different mission areas and over 100 separate projects. It is also important to note that many of the current physical components implement other major Automatic Data Processing (ADP) functions in addition to the DMS functions supporting DoD messaging.

From an architectural standpoint, the DMS includes all components involved in DoD messaging from writer to reader, with the exception of the transmission systems providing connectivity such as the Defense Data Network and the baselevel transmission facilities. From an organizational and management standpoint, further clarification is required. The baseline DMS contains both Defense Communications System (DCS) components such as the AUTODIN Switching Centers and non-DCS components such as the baselevel Telecommunications Centers (TCCs). As the DMS evolves from the baseline to the target, the current DCS/non-DCS distinction is subject to change with deployment of new components performing new architectural functions. Determination of operational direction and management control responsibilities will be required on a component-by-component basis.

In summary, the DMS is a DoD messaging architecture with an implementation strategy for evolution from the baseline to the target. Given it's broad scope, it cannot be managed either as a traditional DCS or traditional non-DCS Program. The primary DMS objective is coordinated DoD execution of the DMS implementation strategy. The management structure necessary to achieve this objective is outlined in Section 2, paragraph 2.6.

1.4 Requirement.

1.4.1 General. The DoD requires an improved message communications system based upon evolutionary upgrades to the current collection of systems. This system, the DMS, must be based upon a set of validated requirements and organized under a basic architectural context. The DMS is centered around the principles of standardization and interoperability, while preserving adaptability for implementing Service unique functionality and customization.

1.4.2 Problem. The major components of the current baseline are the AUTODIN system (to include the baselevel), providing message service between organizational elements, and E-Mail providing message service between individuals (staff personnel). While both components provide messaging service to DoD users, their disjointedness precludes the interoperability required to allow a rationalization of message traffic and needed migration of interactive data exchanges from AUTODIN to DDN. Further, functional deficiencies with both components cause the services provided to users to be less than optimum. At the AUTODIN baselevel, obsolete equipment results in high maintenance cost and service degradation. The current TCC method of providing service is staffing intensive and results in message service delays to writers and readers. E-mail suffers from a lack of standardization of the service provided to users. The Inter-Service/Agency Automated Message Processing Exchange (I-S/A AMPE) was aimed at resolving some of these problems and its recent termination has invalidated the Integrated AUTODIN System (IAS) architecture. At the same time, multiple Service/agency (S/A) architectures have been formulated to resolve baselevel problems. The result is that DoD currently has no overall future architecture.

1.4.3 DMS Requirements. The specific requirements for the DMS are quoted from the draft Multicommand Required Operational Capability (MROC) 3-88. The requirements are stated from the perspective of writers and readers, independent of specific implementations to allow the flexibility for multiple solutions and satisfaction of Service/agency unique applications.

a. Connectivity/Interoperability.

(1) The DMS should allow a user to communicate with any other user within the DMS community. The community of users includes organizations and personnel of the Department of Defense. In addition, the DMS must support interfaces to systems of other government agencies, allies, tactical and defense contractors. System users may be fixed, mobile or transportable.

(2) Connectivity must extend from writer to reader. Messages should be composed, accepted for delivery, and delivered as close to the user as is practical. Current efforts, such as extension of automation to users and improved base level message distribution systems, are responsive to this requirement.

(3) The DMS must be interoperable with and provide standard interfaces for tactical and allied systems. It should lead DoD's migration to international standards and protocols.

b. Guaranteed Delivery.

(1) The DMS must, with a high degree of certainty, deliver a message to the intended recipient(s). If the system cannot deliver a message, a method of promptly notifying the sender of the non-delivery must be available.

(2) For organizational message traffic, the DMS must have the capability to maintain writer-to-reader message accountability.

c. Timely Delivery. The DMS must recognize messages that require preferential handling. The urgency of the most critical information requires handling above and beyond simple priority. The DMS must dynamically adjust to changing traffic loads and conditions to provide timely delivery of critical information during peacetime, crisis, and war. Delivery time for a given message will be a function of message precedence and system stress level.

d. Confidentiality/Security. Confidentiality precludes access to or release of information to unauthorized recipients. The DMS must process and protect all unclassified, classified and other sensitive message traffic at all levels and compartments. The DMS must maintain separation of messages within user communities to satisfy confidentiality. Security is based upon requirements for integrity and authentication as well as confidentiality.

e. Sender Authentication. The DMS must unambiguously verify that information marked as having originated at a given source did in fact originate there. For organizational traffic, a message must be approved by competent authority before transmission.

f. Integrity. Information received must be the same as information sent. If authorized by the writer, the DMS may make minimal format changes to accommodate differences in capabilities between the component systems serving the writer and the reader. However, the DMS must ensure that information content of a message is not changed.

g. Survivability. The DMS must provide a service as survivable as the users it serves. It must not degrade the survivability of systems interfaced to it. Methods such as redundancy, proliferation of system assets, and distributed processing may be employed. Surviving segments of DMS must be capable of reconstitution.

h. Availability/Reliability. The DMS must provide users with message service on an essentially continuous basis. The required availability of the DMS should be achieved by a combination of highly reliable and readily maintainable components, thoroughly tested software, and necessary operational procedures.

i. Ease of Use. The DMS must be flexible and responsive enough to allow user operation without extensive training. Use of the DMS should not require the knowledge of a communications specialist.

j. Identification of Recipients. The sender must be able to unambiguously identify to the DMS the intended recipient organizations or individuals. The necessary directories and their authenticity are part of the DMS.

k. Message Preparation Support. The DMS must support user-friendly preparation of messages for transmission, to include services such as U.S. Message Text Format (USMTF) assistance.

l. Storage and Retrieval Support. The DMS must support storing messages after delivery to allow retrieval for such purposes as readdressal, retransmission, and automated message handling functions such as archiving and analysis, with the capability of incorporating segments into future messages. The minimum storage period for organizational messages will be specified by Allied Communications Procedures.

m. Distribution Determination and Delivery.

(1) For organizational message traffic, the DMS must determine the destination(s) of each message (in addition to the addressee(s) specified by the originator) and effect delivery in accordance with the requirements of the recipient organization.

(2) For individual message traffic, the DMS must effect delivery of each message to the individual(s) specified by the originator.

Section 2

Implementation Strategy

2.0 Introduction.

The current DMS is expensive, staffing intensive, and even with this expense and staffing, it does not provide optimum service to the users (writers and readers of messages). Previous efforts to improve DoD's messaging systems have met with limited success and this can be attributed in large part, to multiple, uncoordinated implementation strategies that have fostered maintenance of the existing DoD messaging structures. Examples are the current array of Service and agency projects and the recently canceled I-S/A AMPE Program which assume that existing formats, procedures (to include manual operations) and interfaces between systems must be maintained. The result of the current strategy is a type of paralysis that promotes continuation of "business as usual" and hinders DoD's ability to derive the economic and user service benefits that can be realized with migration to newer technology and international standards. Recently imposed DoD budget constraints mandate change. Rapidly advancing technology and industry movement to standards, coupled with needed improvement in DoD's acquisition strategy, can provide the opportunity to improve service to users at lower cost. The DMS Implementation Strategy must support rapid transition to less costly baselevel implementations of the DMS using existing, evolvable components shared among the Services and agencies. This will involve development of standard DMS policies, procedures, protocols, services, and components which rationalize the implementation of the DMS at a rate which the Services and agencies can absorb, while maintaining adequate Service and agency control of those components of the DMS which must differ to accomplish unique local missions. The DMS Implementation Strategy must be clear, and have agreed upon goals and visible benefits. It must include aggressive "operational" testing of new components, protocols, and procedures in live user environments to provide proof of purported benefits prior to widespread deployment. Implementation must be truly evolutionary with the concept of "releases" being fundamental, not only for software, but for policy, procedures and hardware as well. Although backward compatibility through multiple "releases" is essential to permit phased deployment of new DMS components, aggressive phase out of obsolete components, procedures, protocols, formats and media is also essential. An effective DMS Management Structure, to include oversight and execution of the DMS Implementation Strategy is crucial to the success of the DMS evolution.

2.1 DMS Component Development.

Components developed for the DMS must maximize the use of non-developmental items (NDI), Portable Operating System Interface (POSIX), Government Open Systems Interconnection Profile (GOSIP), commodity purchases, commercial off-the-shelf (COTS) products, and products endorsed

under the Commercial COMSEC Endorsement Program (CCEP). In addition, evolution to Integrated Services Digital Network (ISDN) compatibility is required to allow use of the ISDN as the DMS transport mechanism.

2.1.1 "Central" Components. Development of "Central" support components will receive a high priority from OASD/C3I in terms of funding support because of their critical importance to the success of the DMS.

2.1.2 "Joint" Components. Development of "Joint" projects and components will be encouraged. Those projects and components designated as "Joint" will enjoy a higher priority in terms of funding support than "User" unique projects and components because they will have the greater potential for cost reduction and/or widespread benefit for multiple Service and agency users.

2.2 Phase Out of Obsolete Elements.

When it is fully implemented, the major achievement of the DMS will be the transition from today's obsolete and DoD-unique equipment, protocols, procedures and media to the 2008 state-of-the-art, standard, interoperable elements. Some phase outs will be accommodated by conversion to an existing alternative. However, most element phase outs will be conditional based on the phase in of new (replacement or alternative) elements. The primary consideration is the essentially uninterrupted provision of communications to the users during the phased evolution of the DMS from 1988 through the achievement of the target architecture at the end of 2008.

2.2.1 Equipment. The phase out of obsolete Service and agency equipment is aimed at reducing maintenance costs and will be based on the phase in of equipments which are selected for their ability to implement or evolve to portable operating systems, standard high order languages, and other DoD or international standards.

2.2.2 Protocols. International protocol standards consistent with the Government Open Systems Interconnection Profile (GOSIP), will be phased in as the older AUTODIN and DoD standards are phased out. Migration to CCITT X.400 Message Handling System and X.500 Directory Services is a specific DMS objective.

2.2.3 Formats. To fully achieve the requirement for a user to communicate with any other user, an X.400 based Common Message Format (CMF) will be developed and phased in as X.400 is phased in. The CMF will facilitate the phase out of existing AUTODIN and E-Mail formats. Compatibility with the U.S. Message Text Format (USMTF) must be maintained.

2.2.4 Procedures. The procedures of the baseline AUTODIN, an outgrowth of the manual and semi-automated predecessors of AUTODIN, are staff intensive. The procedures originated when the least expensive resource in a communications system was the staff. Also, the procedures assumed that only communicators could perform the communication functions. Currently, the most expensive resource is the staff. Automation of the messaging function and user participation (given that the users or their administrative support personnel become computer literate) reduce the need for dedicated

communications personnel and staffing intensive procedures. Achieving the DMS Target Architecture will require significant changes to the procedures currently in effect as the DMS moves toward standard protocols, simplified user formats and the elimination of the current TCC based messaging service. Consistent with the overall DMS Implementation Strategy, procedural actions must be fully integrated into DMS project and component developments and testing activities.

2.3 Extension of Automation to Users.

As a means of reducing Telecommunications Center (TCC) staffing requirements, automation of TCC functions and extension of messaging service to the users will be a primary initial objective. Minimal impact to the users' resources (personnel and fiscal) will be a DMS implementation criteria.

2.4 Test and Evaluation Strategy.

An evolutionary developmental approach and rapid acquisition/deployment strategy is planned for the DMS evolution. To make this possible, a test and evaluation strategy containing both traditional and non-traditional test approaches is being developed by the DMS Test Planning Working Group (TPWG) in the DMS Test and Evaluation Master Plan (TEMP). The initial TPWG membership includes Service and agency representatives and Operational Test Agency (OTA) representatives from the USA, USN and USAF. Since the DMS baseline is an existing operational system, and its planned evolution contains many projects which, while they conform to an architecture, are largely autonomous in their development, testing of the DMS will be a continuous but coordinated activity. The scope of test and evaluation, application of T&E strategies and methodologies employed will be formulated by the TPWG for DMS projects and components. The T&E strategy will be designed to support an acquisition strategy that will employ advanced concepts of prototyping, Beta testing, and rapid deployment to the maximum extent possible.

2.4.1 Beta Testing. Beta testing is defined as the measurement of the favorable and unfavorable impacts to users in a baseline environment that result from the addition of a new component to that environment. Users of the planned component actively participate in the Beta test and provide feedback on operational and technical issues. Feedback may be incorporated as changes to a future Beta version based on feasibility and need for such a change. Beta testing results are ultimately considered in deployment decisions.

2.4.2 Testbeds. To support the DMS test strategy, a number of new testbeds (depicted in Figure 2-1) are planned.

a. Research and Development (R&D) Testbed. This testbed will be required to gain confidence in the approaches planned for advanced DMS phases (e.g., X.400/X.500 components with SDNS protection). Specifically, in keeping with the DMS objective of maximizing the use of commercial off-the-shelf (COTS) products, R&D efforts during Phase I will be aimed at

DMS Testbeds

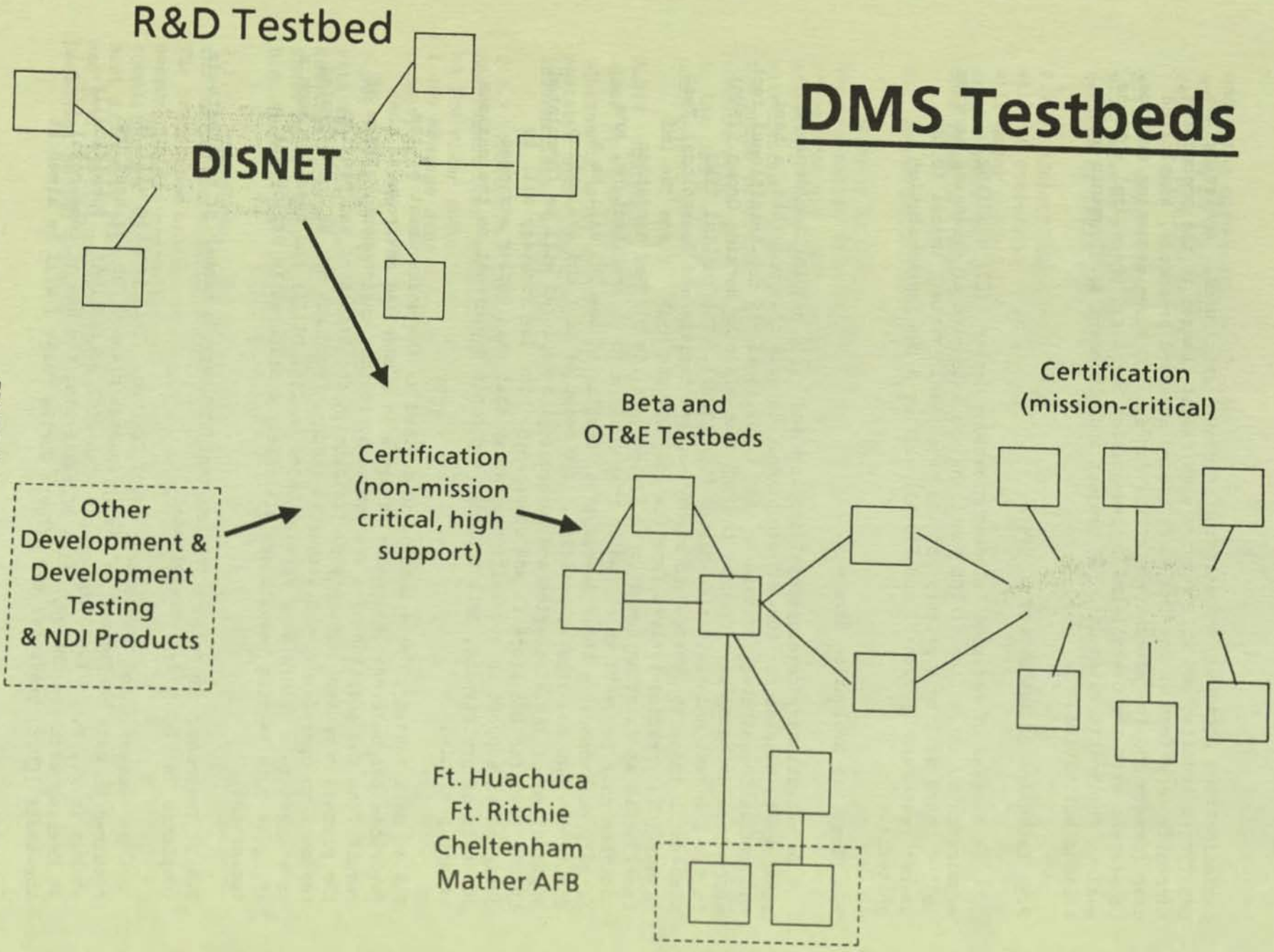


FIGURE 2-1
PAGE 2-4

ensuring that commercial products planned for the Phase II timeframe (e.g., SDNS) will indeed satisfy DMS requirements. The R&D Testbed will serve as the vehicle for testing early R&D solutions for feasibility and compatibility with other DMS components.

b. Beta/Operational Test and Evaluation (OT&E) Testbeds. In addition to the development and certification testbeds currently in use, combined OT&E and Beta testbed capabilities will be provided. Where feasible, existing testbeds will be expanded to provide these new capabilities which will be used to place new DMS components in an on-line operational environment as quickly as possible to gain confidence in their operational effectiveness and to obtain early feedback from the users. Initial plans are for DCA to provide a Beta/OT&E testbed capability for "Central" support DMS component testing and for each of the Services and agencies to provide a Beta/OT&E testbed capability for "Joint" DMS component testing. These testbeds will be used to test both developmental and non-developmental components.

2.4.3 Test Approach. In addition to the testbeds, which will provide a complete system environment for new DMS components, development and certification testing will be performed on individual DMS components. To minimize the time required to field components and to gain confidence that components are likely to be operationally effective and useful, certification will normally take place in two steps.

a. Initially, components will be certified to operate on the DMS in the non-mission critical, high support environment provided by the Beta/OT&E testbeds. Although this will be a true operational environment (i.e., real users and live message traffic), steps will be taken as necessary to reduce risks associated with such early use. For example, components might be restricted to unclassified, low-precedence operational traffic with test traffic providing the stress testing required for full OT&E. Further, technical support from the component developers would be readily at hand and the ability to revert back to normal (old system) operations, if necessary, would be provided. Components that are developed to handle high precedence and extremely sensitive information will require more strenuous testing before being placed in a live environment.

b. After proof of the effectiveness and usefulness of components, certification testing will be performed, if required, to qualify the components for operational use in a normal support, mission critical environment.

2.5 Acquisition Strategy.

With the current speed of technology advances, DoD acquisition policies and procedures frequently result in a new component being obsolete before it can be acquired and fielded. New procedures to provide for rapid deployment of both developmental and non-developmental items (NDI) after successful Beta/OT&E testing are required to ensure that cost-saving new technology and needed capabilities are provided to users in a timely manner. DMS use of requirements contracts for hardware, standards for protocols and operating

system interfaces, are part of the rapid deployment strategy. Further definition of this strategy is required to ensure that objectives are met and it is evident that realization of rapid deployment objectives will require not only innovative testing methods but a compatible acquisition (funding and contracting) strategy. A DMS Aquisition Strategy Working Group (ASWG) is being formed to formulate the funding and contracting strategy necessary to accelerate acquisition and fielding of DMS components.

2.6 Management Structure.

The DMS Management Structure, depicted in Figure 2-2, is designed to ensure a fully coordinated DoD evolution from the baseline to the target architecture while minimizing the resources necessary to manage the evolution. Since the target architecture is a significant departure from the baseline, reevaluation and redefinition of operational direction and management control responsibilities for new DMS components (as required) is an additional aspect of the evolution that must be addressed by the management structure. Management of the DMS falls into two major categories "oversight" and "execution" which are outlined in the following paragraphs.

2.6.1 DMS Oversight. The oversight of the DMS evolution will be accomplished within existing boards and committees to the maximum extent possible. The Defense Acquisition Board, the C3I Systems Committee, and a newly formed DMS Panel will be the oversight bodies responsible for establishment of DMS policy and resolution of DMS issues. Normally, issues are expected to be resolved at the DMS Panel level. Procedures guidance will be provided by the Military Communications Electronics Board (MCEB) through membership on the Panel. Policy guidance will be provided by the Assistant Secretary of Defense for Command, Control, Communications, and Intelligence, ASD(C3I). Requirements guidance will be provided by the Organization of the Joint Chiefs of Staff (JCS) through membership on the Panel. Acquisition guidance is received from the C3I Systems Committee of the Defense Acquisition Board (DAB). The DMS Panel will be chaired by the Director, Information Systems, or designated representative, for ASD(C3I). Members of the DMS Panel will be from the Services and agencies, the MCEB, and OJCS(J6) at the O7 level. Meetings will be held when called by the Chairman, when requested by Panel members, or when unresolved issues are identified by the DMS Coordinator (this position is described in the following paragraph).

2.6.2. DMS Execution. Execution of the DMS program requires the establishment of a DMS Coordinator, DMS Project Managers, Service and agency Testbed Managers, a DMS Support Staff, and a DMS Implementation Group.

a. DMS Coordinator. The DMS Coordinator is responsible for providing day-to-day coordination of all DoD DMS activities through management of the DMS Support Staff (described below), and for providing the Chairman of the DMS Implementation Group (described below). The DMS Coordination role is assigned to the Defense Communications Agency (DCA) and the DMS Coordinator designated by DCA is the normal interface point with the DMS Panel.

DMS Management

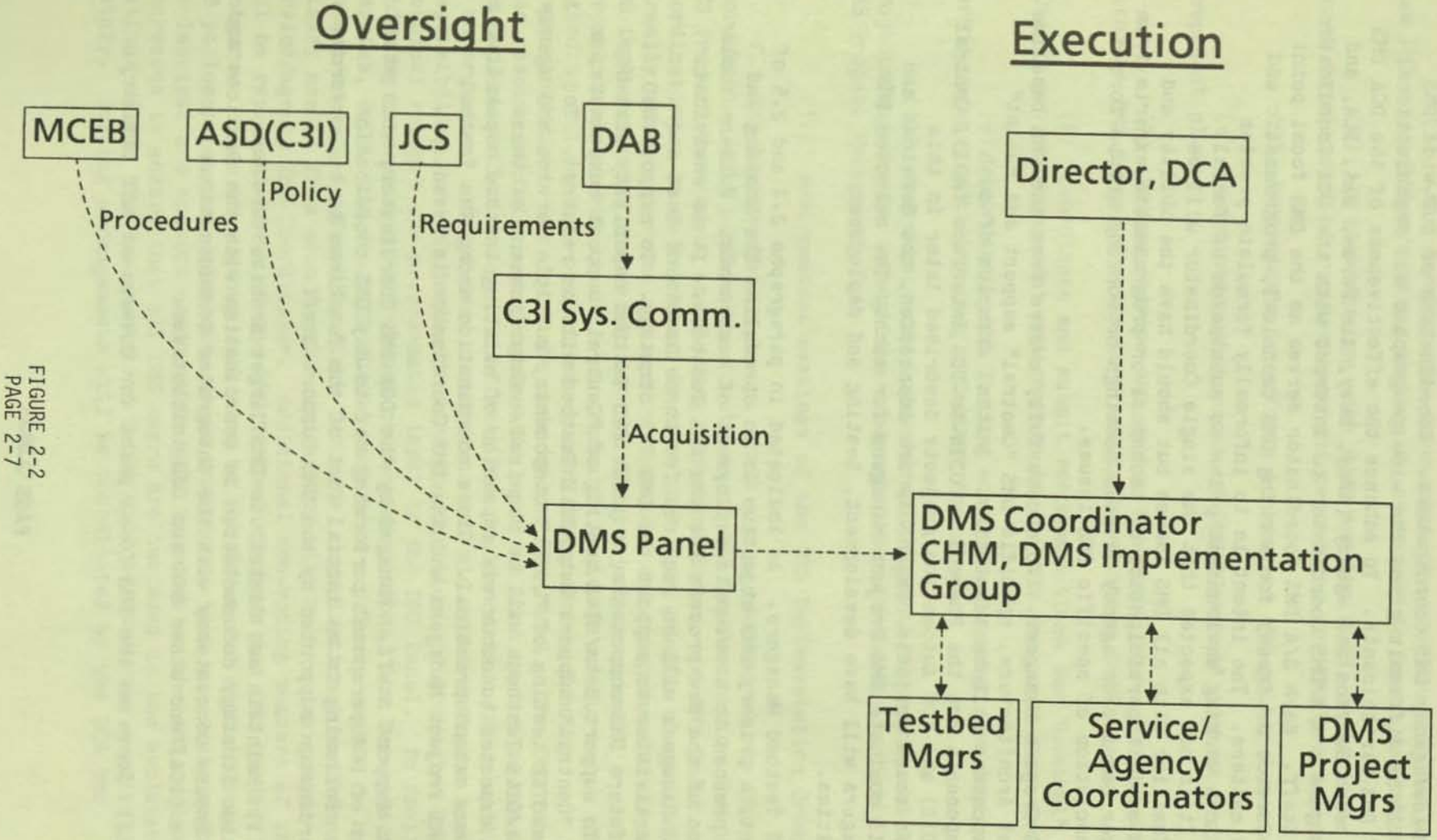


FIGURE 2-2
PAGE 2-7

b. Service/agency DMS Coordinators. Coordination of DoD-wide DMS activities will be difficult given the wide geographic and organizational disbursal of DMS participants. To enhance the effectiveness of the DCA DMS Coordinator, each Service and agency (Army, Navy, Air Force, DIA, DLA, and NSA) has assigned a S/A DMS Coordinator to interact with the DCA Coordinator and Support Staff. Each S/A DMS Coordinator serves as the DMS focal point for his/her Service or Agency for working DMS technical, programmatic and coordination matters. The intent is to informally formulate problem resolutions in a working environment prior to submission of formal solutions. It is not expected that the single Coordinator will be intimately familiar with all DMS issues but should have the ability and authority to solicit participation of technical or programmatic experts from within his/her Service or agency in side meetings or working groups formed to obtain resolution of specific DMS issues.

c. DMS Project Managers. To successfully evolve from the DMS baseline to the Target Architecture, specific DMS "Central" support and "Joint" projects/components will be identified. Initial examples of such projects/components are the Phase I AUTODIN-to-DDN Interface (ADI), Central Directory (DIR) and TCC Automation projects described later in this document. As these projects/components are identified, the Services and agencies will nominate DMS Project Managers for each. The selected DMS Project Managers will have development, testing and deployment responsibilities.

d. DMS Testbed Managers. As indicated in paragraphs 2.4 and 2.5 of this document, a primary DMS objective is to streamline the testing and acquisition process to accelerate deployment of components. Primary tools for execution of the new process are the DMS Testbeds. It is envisioned that Testbed Managers will be required for three levels of test and evaluation activities to support the DMS T&E Strategy. To support R&D testing of future DMS components, a joint R&D Testbed capability will be required. To support Beta/OT&E testing of "Central" support components, a DCA managed "Central" support Beta/OT&E Testbed will be required. To support Beta/OT&E testing of "Joint" components, multiple Service and agency managed Beta/OT&E Testbeds will be required. Establishment of these testbeds is expected to occur via expansion of existing testbed capabilities to the maximum extent practical. Close coordination among the Testbed Managers, DMS Project Managers and the DMS Coordinator is essential.

e. DMS Support Staff. Managed by the DCA DMS Coordinator, this staff will consist of DCA personnel performing day-to-day DMS coordination activities. Following is an initial list of the functions to be performed by the DMS Coordinator supported by the DMS Support Staff:

(1) Maintain and distribute DMS Target Architecture and Implementation Strategy documentation in coordination with the Services and agencies. Ensure consistency with the Integrated Communications Architecture (ICA) and other DCA and OSD initiatives.

(2) Serve as the DMS focal point for Government and Industry.

(3) Lead development, documentation, coordination and approval of new DMS acquisition/testing strategies necessary to speed deployments.

(4) In coordination with OJCS and the MCEB, participate in or lead joint development of requirements and procedures for DMS projects/components.

(5) Participate in efforts to resolve DMS policy issues.

(6) Coordinate development of DMS "Central" support project and component plans.

(7) Review Service and agency baselevel plans for consistency with the DMS Target Architecture and Implementation Strategy.

(8) Coordinate and submit recommendations for "Central" and "Joint" project/component assignments to the DMS Implementation Group.

(9) Coordinate DMS Testbed activities through the designated Service/agency activity (e.g., Testbed Managers).

(10) Coordinate development/deployment of "Central" and "Joint" projects/components through the designated Service/agency activity (e.g., DMS Project Managers).

(11) Host/conduct meetings of the DMS Implementation Group.

f. DMS Implementation Group. This group, chaired by the DMS Coordinator, will perform the functions of DMS Implementation Coordination, DMS Project Management and Funding Recommendations, and DMS Issue Coordination. It is important to note that this group's charter will be to formally achieve Service and agency technical and programmatic consensus on DMS implementation issues (to include DMS project management recommendations) but is not a programmatic decision making body. Decisions regarding DMS policy, project management assignments, funding responsibilities, etc., will be made by the DMS Panel. The DMS Panel will also resolve technical or programmatic problems that cannot be resolved by the Implementation Group. In effect, the Implementation Group will function as an organized body of lead technicians and mid-level managers having responsibility for DMS Implementation Coordination and provision of technical support and programmatic input to the DMS Panel. To facilitate achieving consensus on DMS issues or recommendations, the Services, agencies, OJCS, and the MCEB should each have a primary member or spokesman at each meeting to formally state (or vote) organizational positions. The primary member from each Service and agency will be the designated Service/agency DMS Coordinator. Additional non-voting members of this group will be representatives of the DMS Testbed Managers and DMS Project Managers. Since this group will also be the forum for distributing overall DMS philosophies and practices, it is envisioned that associate members from the Tactical and non-DoD communities will be added as the DMS evolution progresses to ensure that all DMS users are included in the evolution. Meetings of the DMS Implementation Group will be conducted regularly; e.g., monthly. Hosting arrangements will be coordinated by the DCA DMS

Coordinator and the DMS Support Staff. Working Groups will be assigned as required to develop specific DMS plans/strategies and to work specific DMS issues. All plans, strategies, and recommendations formulated by the working groups will be submitted to the DMS Implementation Group for adoption or submission to the DMS Panel, as appropriate.

(1) Implementation Coordination. To facilitate formal coordination of DMS implementation activities, representatives of the Service and agency DMS Project Managers and Testbed Managers should be present as required to provide status and advise of any issues.

(2) DMS Project Management. This group will serve as the forum for coordinating recommendations for DMS "Central" and "Joint" Project Management and funding recommendations. These coordinated recommendations will subsequently be submitted to the DMS Panel for approval. The need for DMS Projects and Project Managers may very well originate from the DMS Panel. In this event, the Implementation Group will serve as the body to perform further analysis and provide technical and/or programmatic input to the DMS Panel, as directed, to support DMS decisions.

(3) DMS Issue Coordination. This group will also be the initial forum for obtaining joint positions on DMS issues. Issues that cannot be resolved by the DMS Implementation Group will be submitted to the DMS Panel for resolution. The intent is to obtain coordinated joint positions on DMS issues (to include recommended solutions) to the maximum extent possible within the DMS Implementation Group. Procedural issues will be referred to the MCEB for development, coordination and promulgation, and requirements issues will be referred to OJCS for formal validation.

2.7 Phased Implementation.

To achieve the DMS Target Architecture, there must be a clear, comprehensive understanding of the baseline, the terminology, and the three evolutionary implementation phases. The baseline architecture, the two intermediate architectures, and the target architecture are snapshots of a continuing, evolving, achievable phased implementation of the DMS.

2.7.1 Baseline DMS. AUTODIN and E-Mail are the baseline systems for the DMS (depicted in Figure 2-3). AUTODIN and E-Mail are disjoint, existing operational capabilities, each using its own backbone, procedures, formats, etc. See Section 3 for a more comprehensive baseline DMS presentation.

2.7.2. DMS Terminology. As part of the DMS architectural formulation process, it was necessary to define physical components and logical functions that could be applied to the baseline, target, and all intermediate implementation phases.

a. CCITT Recommendation X.400 Messaging. To derive the economic and interoperability benefits associated with migration to international standard protocols, DoD intends to use International Standards Organization (ISO) protocols conforming to the Open Systems Interconnection (OSI) Model. The OSI application level for messaging is X.400 and DMS will conform to the

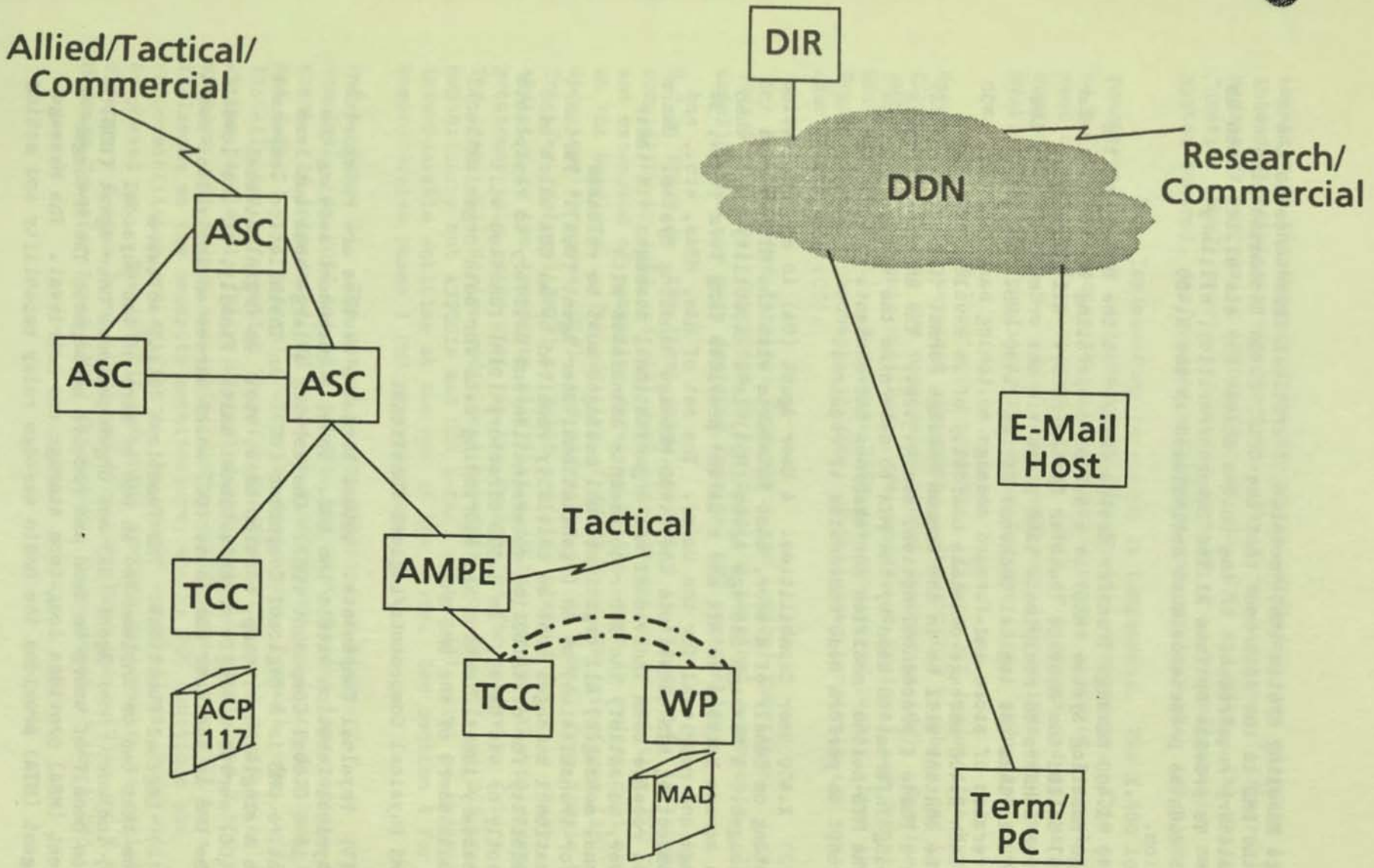


FIGURE 2-3
PAGE 2-11

Baseline Architecture
1988

X.400 Message Handling System (MHS) model. Of critical importance to the success of the DMS is the assurance that the CCITT X.400 Recommendation documents military requirements of the United States and its allies, such as precedence. To provide optimum Allied interoperability, military requirements such as precedence must be included in the X.400 Recommendation.

(1) X.400 Message Transfer System (MTS). At the center of the X.400 Message Handling System (MHS) is a set of cooperating Message Transfer Agents (MTAs) called the Message Transfer System (MTS). All message transfers from senders to recipients take place via one or more MTAs in the MTS. The MTS is thus the logical backbone of the X.400 MHS. The MTS performs a version of store-and-forward message switching based on the X.400 envelope. Each X.400 message consists basically of an envelope and its content. The content will be in the Common Message Format (CMF) of ACP-XXX. (ACP-XXX is a Phase I procedural action, see 4.3.2e.) The envelope carries the addressing information used by the MTA to determine the routing through the MTS. The MTS neither modifies nor examines the contents of an X.400 envelope except to perform code conversion if required.

(2) X.400 User Capabilities. A User Agent (UA) is an application process, acting on behalf of a user, that interacts with the MTS to send and receive messages. A Message Storage Agent (MSA) is a capability that, when used, is in series between an MTA and a UA and provides long term (e.g., 30 days) storage and retrieval for the UA(s). The set of UAs, MSAs, etc., and the interconnecting MTS constitute the X.400 Message Handling System. Users may send and receive both individual and organizational messages via their UAs. However, to satisfy the DoD requirements associated with organizational messages, all organizational messages must be released (approved for transmission) by an Organizational User Agent (OUA). Further, the organizational messages must be initially received by an OUA which also has responsibility for distribution determination and delivery to recipients either directly or via UA(s). An X.500 Directory (DIR) function will provide necessary identification and addressing data for both organizational and individual users of the DMS MHS.

b. DMS Physical Components/Logical Functions.

(1) Physical Components. Actual hardware devices are categorized by their physical location within the DMS. Thus, a component serving the entire DMS is a Global Component (GC). One serving a large area but less than the entire DMS is a Regional Component (RC). An Installation Component (IC) serves a single post, camp, station base, etc. An Organizational Component (OC) serves a single organizational unit. Finally, at the lowest level of the DMS is the User Component (UC) which serves an individual user.

(2) Logical Functions. The functions (e.g., software applications that can be implemented in one or more of the physical components) include: User Agent (UA) and Organizational User Agent (OUA) which act on behalf of users to send and receive messages. The Message Storage Agent (MSA) provides long-term storage and retrieval. The Message Transfer Agent (MTA) provides the basic message relay capability and acting

together as the Message Transfer System (MTS) delivers messages to the intended recipients via UAs/OUAs. The X.500 Directory (DIR) provides necessary addressing information to UAs, OUAs and MTAs. The Management function (MGMT) provides features such as network configuration management, system control, performance monitoring and cryptographic key management.

(3) Implementing Functions as Components. The X.400 logical functions must be implemented in DMS physical components. This mapping will be a flexible process that will be based on the state of technology, the need to use non-developmental items (NDI) of hardware and software from commodity buys (e.g., AFCAC 251), workload, user unique requirements, availability of facilities and other factors (e.g., reduction of staffing).

c. Baseline Physical Components. Figure 2-4 depicts the baseline in terms of its DMS physical components. The AUTODIN backbone and the DDN Directory function are considered Global Components (GC). Service/agency AMPEs and Electronic Mail Hosts are considered Regional and Organizational Components (RC/OC). Baselevel TCCs are considered Installation and/or Organizational Components (IC/OC). E-Mail user terminals are considered User Components (UC).

d. Baseline Physical Components and Logical Functions. Figure 2-5 adds DMS logical functions to the baseline physical components. The baseline has now been depicted from the DMS perspective.

2.7.3 Phase I. The first phase, depicted in Figure 2-6, is targeted for completion by 1993 and will emphasize automation of existing TCC functions and extension of messaging services to the users to reduce cost and manning at the baselevel. The addition of AUTODIN-to-DDN Interfaces (ADI), improved directory services (DIR), and migration of DDN E-Mail from Simple Mail Transfer Protocol(SMTP) to X.400 are also planned for this phase. In addition to the immediate alleviation of the severe TCC obsolescence problems, this phase will lay the foundation for achieving future changes. The users will derive additional benefits from the ADI and DIR transition capabilities but AUTODIN and DDN E-Mail will still exist as separate but interoperable entities at the end of the phase. See Section 4 for a more comprehensive Phase I DMS presentation.

2.7.4 Phase II. The second phase, depicted in Figure 2-7, is targeted for completion by 2000 and will produce the most obvious improvements for the users. An integrated DMS based on X.400 messaging (vice distinct AUTODIN and E-Mail) will emerge; protocols, procedures, formats, etc., will change; Installation Information Transfer Service (IITS) will begin to be deployed at the baselevel; fully integrated and centrally maintained X.500 directory service will become available; SDNS and CCEP technology will have a major influence on the security architecture; and as TCC functions and responsibilities are shifted to the users' workstations, TCCs will begin to be phased out. The AUTODIN Switching Centers will evolve to regional X.500 directory System Agent (DSA) and Directory User Agent (DUA) and X.400 Message Transfer Agent (MTA) functions. Development of the X.400 OUA and UA

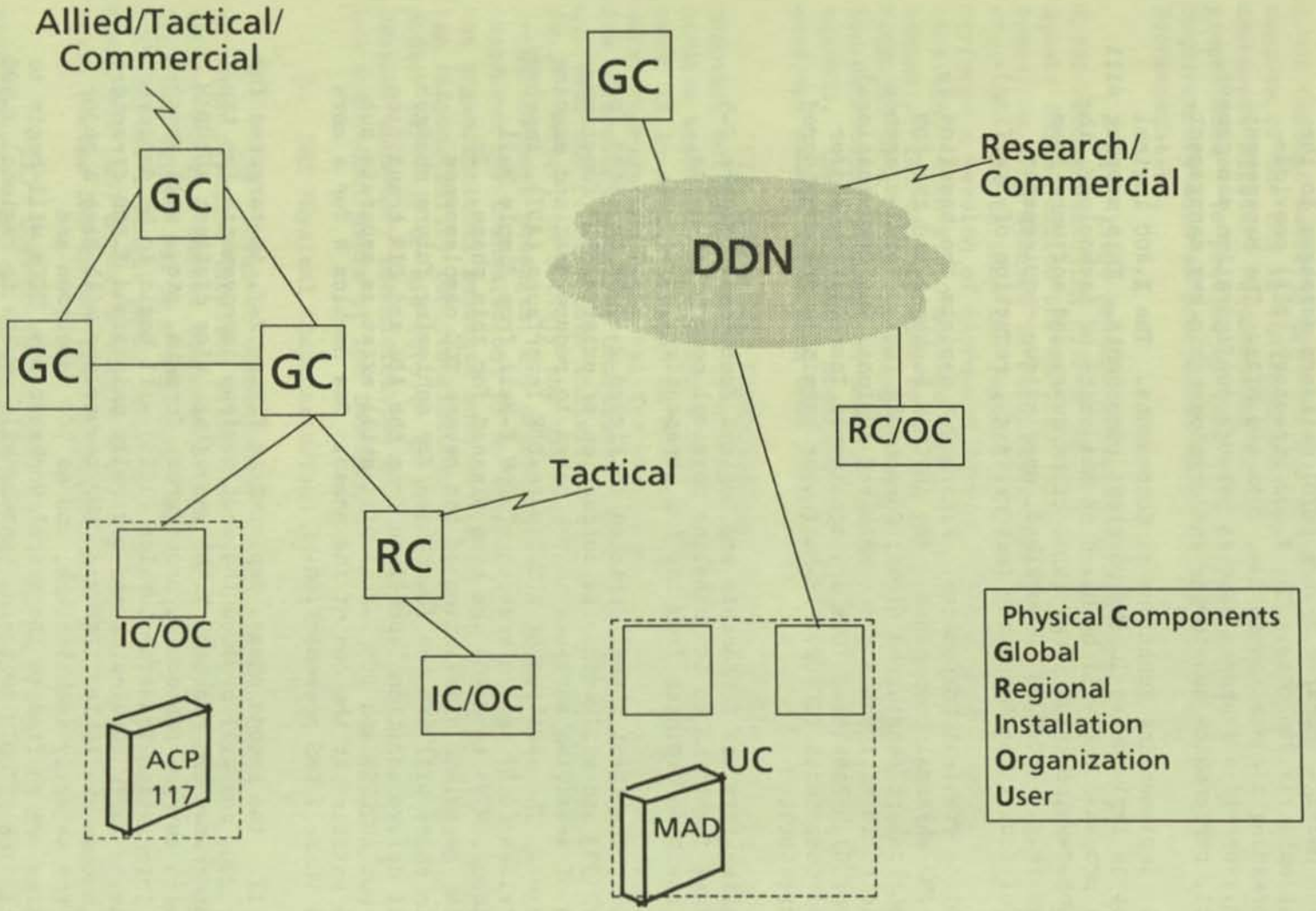


FIGURE 2-4
PAGE 2-14

Base Line Physical Components

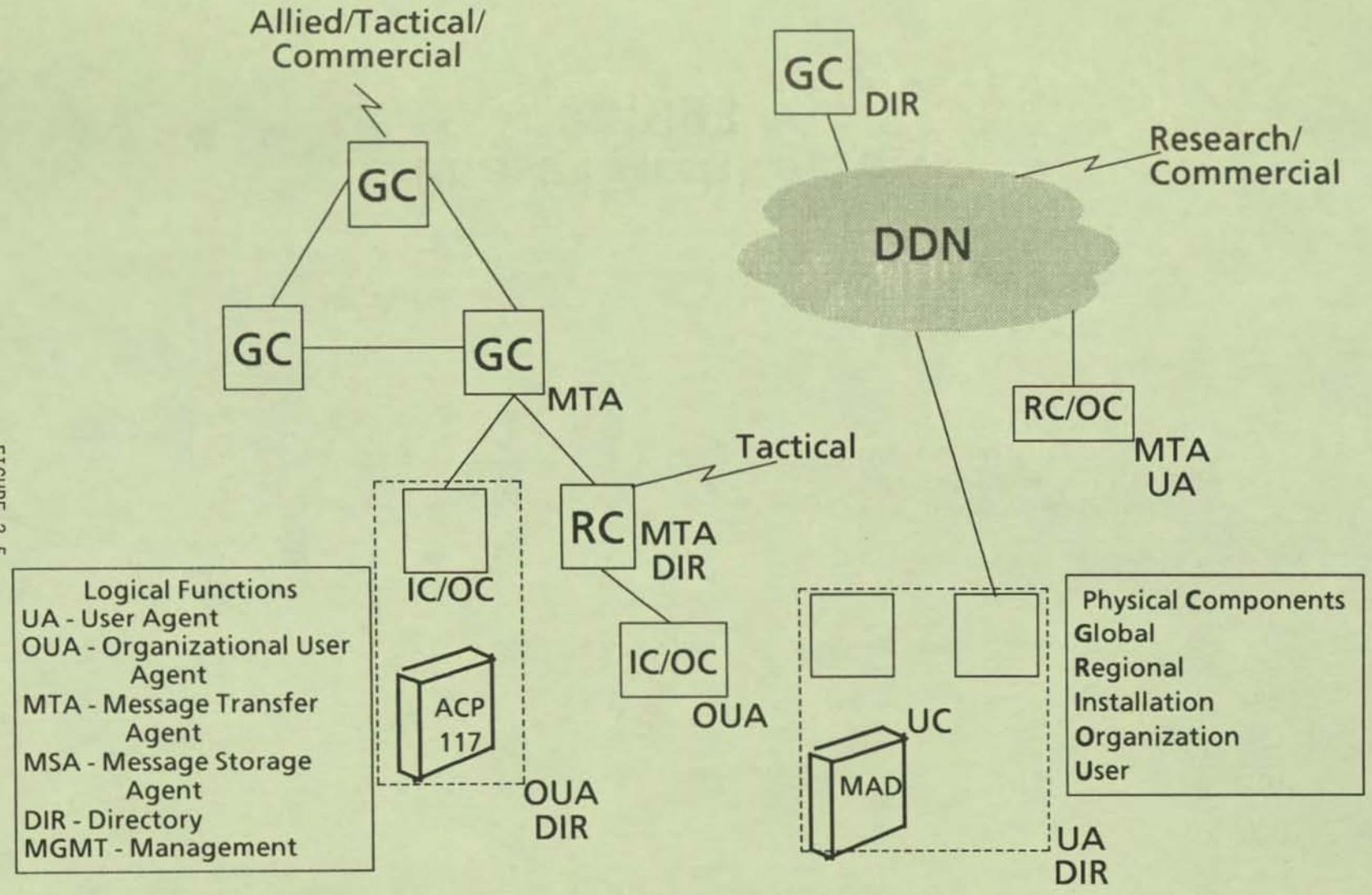


FIGURE 2-5
PAGE 2-15

Base Line Physical Components and Logical Functions

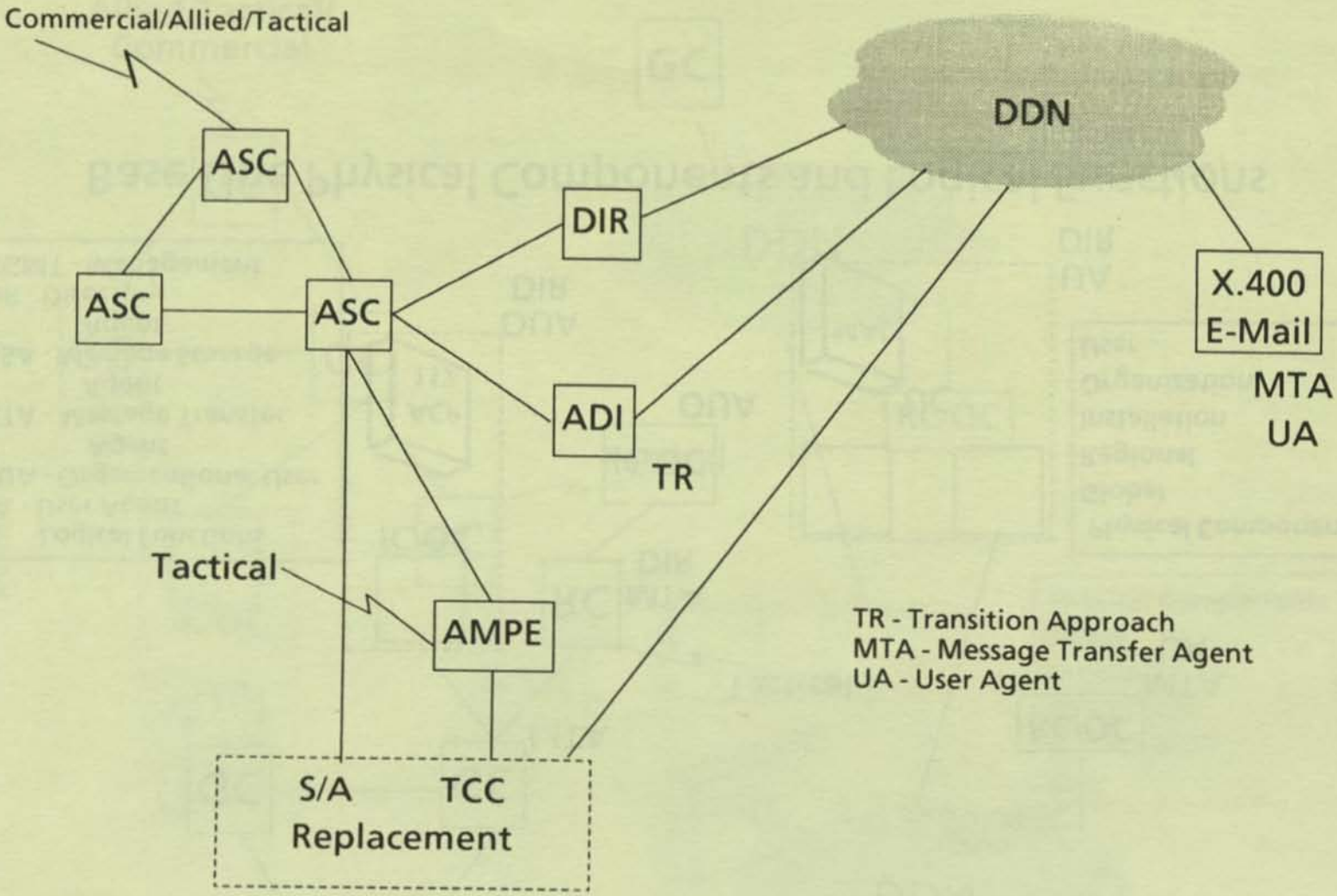


FIGURE 2-6
PAGE 2-16

Phase I Architecture
1993

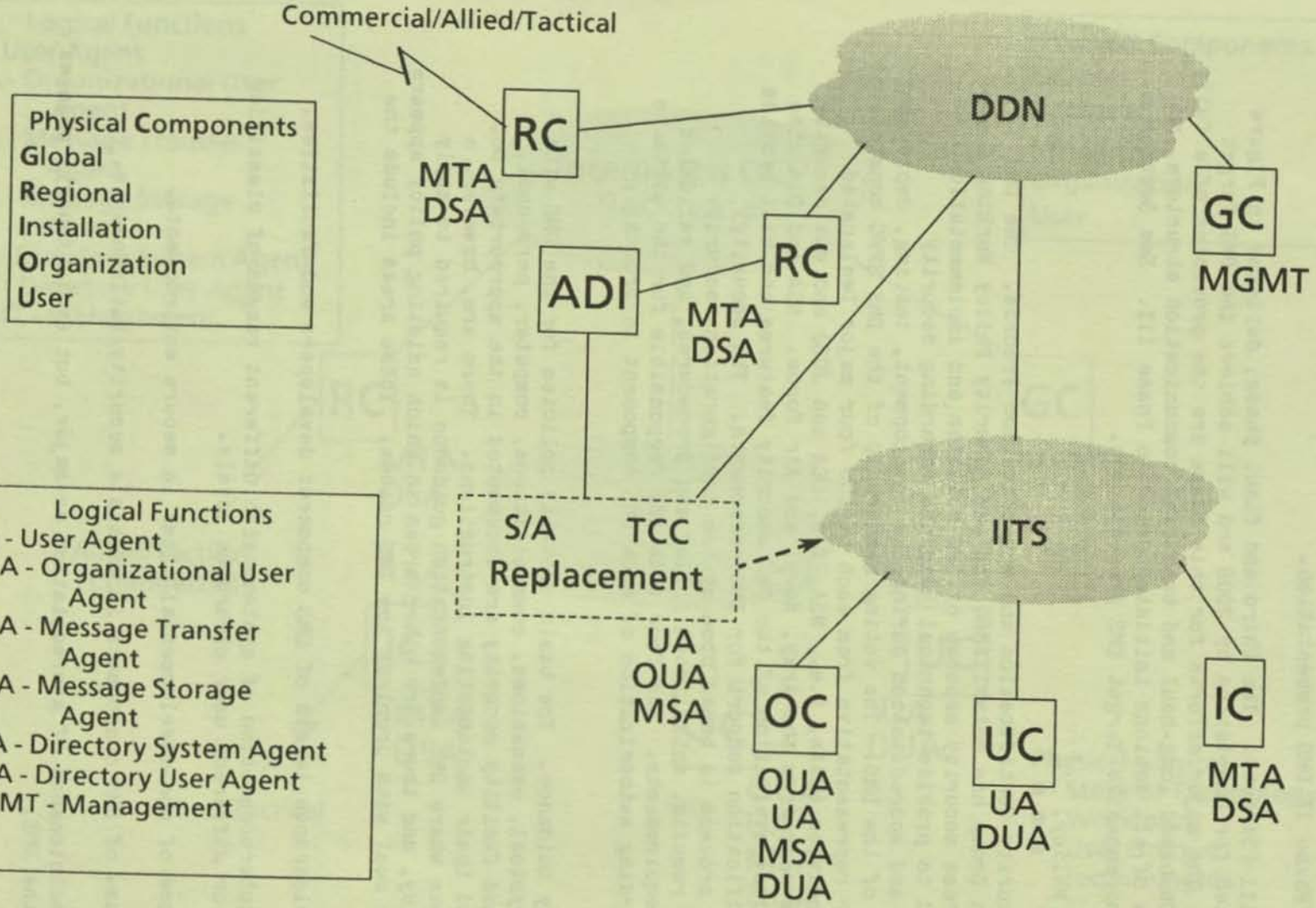


FIGURE 2-7

PAGE 2-17

Phase II Architecture 2000

components will provide a common user interface to the DMS for both organizational and individual messaging. See Section 5 for a more comprehensive Phase II DMS presentation.

2.7.5 Phase III (Target). The third and final phase, depicted in Figure 2-8, is targeted for completion by 2008 and will achieve the DMS Target Architecture. The major efforts for this phase are the provision of a fully integrated ISDN-based long-haul and baselevel communication structure, and the completion of all actions initiated prior to Phase III. See Section 6 for a more comprehensive Target DMS presentation.

2.8 Security Policy.

2.8.1 DMS Security Certification and Accreditation Process. The DMS Implementation Group has established the DMS Security Policy Working Group (SPWG) to address security aspects of DMS policies and implementation strategies and to provide technical guidance regarding security certification and accreditation during the development, testing, deployment and operation of the DMS. The voting membership of the DMS SPWG consists of one accreditor representative from each of the four major Designated Approval Authorities (DAAs, i.e., NSA, DIA, DCA and JCS) and one security representative each from the Army, Navy, and Air Force. NSA and DIA also provide technical evaluation of the DMS security features and will provide security certification support for DMS components. The security accreditation process is based upon system configuration, security certification results, established policy and procedures, and validated operational requirements. The four DAAs are responsible for the ultimate decision regarding authorization of each DMS component to process information.

2.8.2 Policy Guidance. The basic security policies for the DMS with respect to physical, emanations, communications, computer, personnel, procedural, and facility security are documented in the appropriate DoD directives and their implementing instructions. There are, however, a number of areas where DMS implementation guidance is required to apply existing policy, and there are other areas in which existing policy appears inadequate to deal with problems the DMS raises. These areas include the following:

- clearance levels of DMS component developers and facilities.

- interconnection of systems with different ranges of classified information, or different user clearance levels.

- use of non-developmental items in secure environments.

- use of DMS components in multiple security environments.

- maintenance of accreditation as major, but evolutionary, changes are made to the DMS.

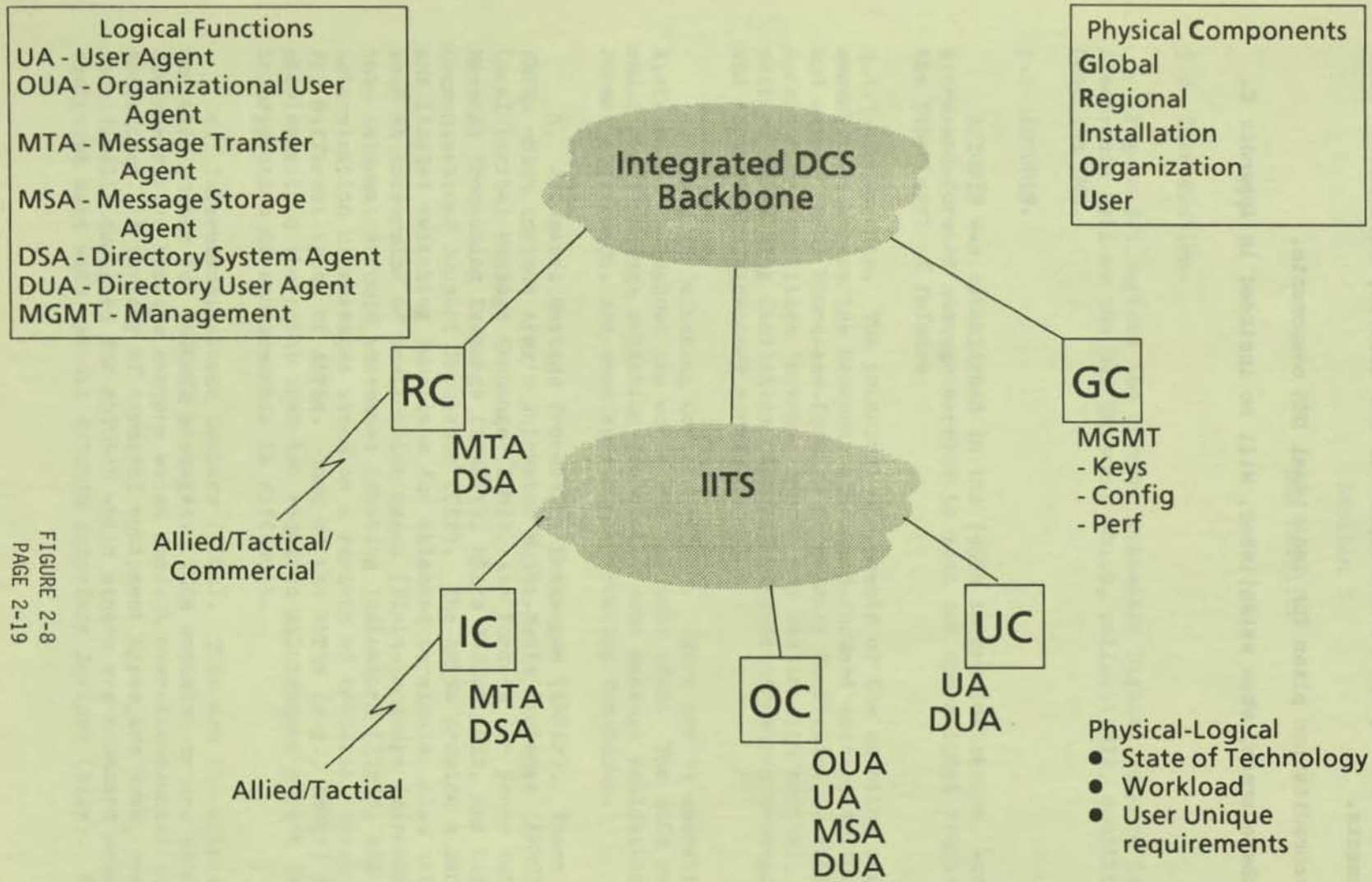


FIGURE 2-8
PAGE 2-19

Target Architecture 2008

- use of DMS equipment developed for one security environment in other environments.

- accreditation plans for individual DMS components.

Guidance in these areas, when established, will be included in Appendix C.

Section 3

DMS Baseline

3.0 Introduction.

Figure 3-1 depicts the current Automatic Digital Network (AUTODIN) and Electronic Mail on the DoD Internet which, collectively, constitute the baseline DMS.

3.1 AUTODIN.

AUTODIN was established in the 1960s to provide secure, automated store-and-forward message service to meet the operational requirements of the Department of Defense.

3.1.1 Components. The principal components of the existing organizational message system are the backbone store-and-forward message switches, Service and agency (S/A) store-and-forward processing facilities, a variety of terminating facilities (message source and destination points), special data pattern processing facilities, special purpose narrative message facilities, and paper-based directory services.

a. AUTODIN Switching Centers (ASCs). There are 15 operational ASCs distributed throughout the world and two test ASCs. The ASCs perform store-and-forward message switching functions, some message validation functions, format conversion, and some specialized routing functions.

b. Automated Message Processing Exchanges (AMPEs). There are over 100 AMPEs which include Army's Automated Multi-Media Exchange (AMME), Navy's Local Digital Message Exchange (LDMX), Air Force's Air Force Automated Message Processing Exchange (AFAMPE), NSA's STREAMLINER, and DIA's Communications Support Processor (CSP). The AMPEs provide a concentrator and limited switching functions for attached terminals, plus other functions such as conversion of destination names (Plain-Language Addresses [PLAs]) into internal AUTODIN addresses (Routing Indicators [RIs]), and distribution determination of messages based on a variety of criteria, which may differ for different types of AMPEs. Some of the AMPEs (e.g., AMMEs) are obsolescent to the point that the required maintenance effort is costly and incorporation of enhancements is difficult.

c. Telecommunications Centers (TCCs). TCCs are the principal entry and exit points for AUTODIN messages. TCCs contain, or are associated with, administrative message centers which conduct over-the-counter (OTC) operations. A variety of terminal equipment types are used, some specifically designed for AUTODIN while others are standard commercial equipment used with special AUTODIN Interface Devices (AIDs). Narrative

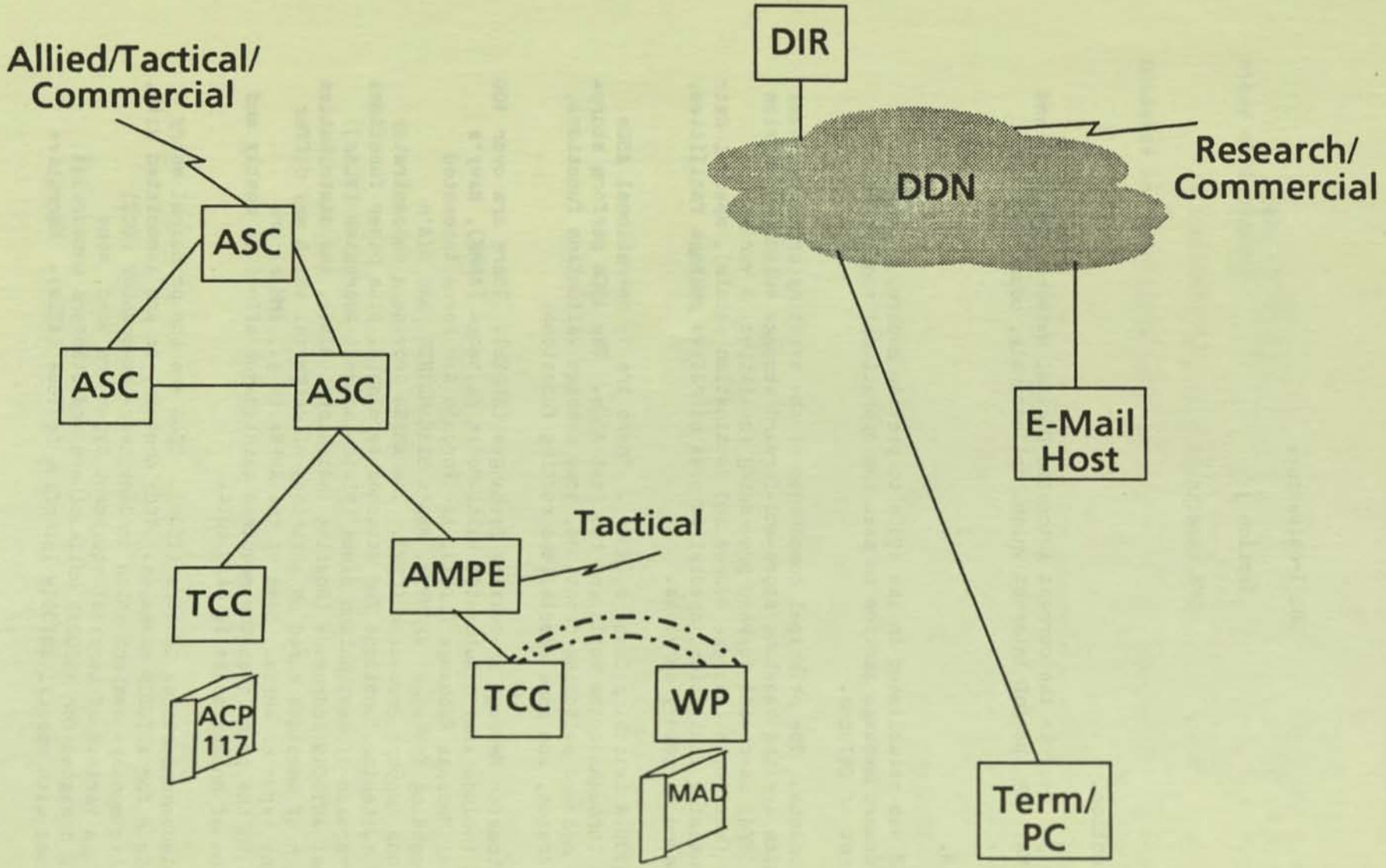


FIGURE 3-1
PAGE 3-2

Baseline Architecture
1988

messages are generally entered from paper DD Form 173 originals via optical character readers, though some TCCs manually prepare messages on Video Display Terminals (VDTs), punched paper tape or 80 column cards. Additionally, automated message preparation and entry support (including preformatted messages, message masks, etc.) is provided by some systems, by means of VDTs either in the TCC or in the user's work area. Data pattern messages which are transmitted by a TCC (as opposed to those entered directly into AUTODIN from a data processing center) are generally entered from magnetic tape. Some TCCs are beginning to phase in floppy disk as an input/output media for both narrative and data pattern messages. Much of the equipment in the TCCs is obsolescent to the point that the required maintenance effort is costly and the age of many of the systems makes it difficult to implement modifications and enhancements to the system hardware or software. As a result, enhancements to extend automation to users and to reduce the manual, staff intensive, operations within the TCCs have been limited.

d. Data Processing Installations (DPIs). Some DPI computers have automated interfaces to AUTODIN (either directly to an ASC or via an AMPE). These interfaces are generally used to send and receive data, rather than narrative messages.

e. Automated Message Handling Systems (AMHSs). Some users have implemented or are implementing components which assist in the automated processing of messages, including message coordination and release, storing, sorting and retrieving messages for various purposes after receipt, and electronic mailbox distribution schemes.

f. Directories (DIR). Directories are distributed as documents. The Message Address Directory (MAD) contains organization names and associated Plain Language Addresses (PLAs). ACP 117 CAN-US Supp-1 includes PLAs with assigned routing indicator listings.

g. Specialized User Terminals. Below the level of TCCs, AUTODIN has a number of user terminals which support a limited work center (as opposed to a TCC which may support one or more organizations), and which generally are operated by the users themselves (as opposed to being operated by communications personnel). These terminals often support missions which have limited communications requirements, in terms of volume and distribution of traffic. As a result, relatively slow and inexpensive terminal equipment can be utilized to support these requirements.

3.1.2 Connections. Essentially, all equipment connection in AUTODIN is via dedicated transmission lines protected with separate link encryption equipment. ASCs are multi-connected, with a total of 64 trunk lines connecting the 15 ASCs. Trunk line speed is usually 4800 bps with 2400 and 1200 bps also used. There are currently about 1400 terminals (including AMPEs and DPIs) directly connected to the switches. There are about 600 additional terminals connected to the backside of AMPEs. Terminal line speeds vary from 45 to 4800 bps. ASC connectivity with the Allied, Tactical and Commercial Refile communities is via tailored interfaces. Further, tactical units such as Navy afloat commands, communicate with AMPE systems

via tailored interfaces.

3.1.3 Concept of Operations. The following is a typical message processing scenario. A message is prepared off-line on a DD Form 173 with a special OCR font. If not already known from previous messages, the preparer determines the PLAs of the intended recipients from the MAD. The message is signed by a designated release authority for the sending organization and carried to the local TCC. The TCC operator checks the DD Form 173 for a signature authorizing release. If the terminal is not connected to an AMPE (which does PLA to RI conversion), the operator looks up the PLAs in ACP 117 and enters the RIs onto the message, together with the Originating Station Routing Indicator (OSRI), Originating Station Serial Number (OSSN), and Time of File (TOF). The message is then entered into the terminal via the OCR where it is reformatted in accordance with JANAP 128 or ACP 126/ACP 127 (manuals describing the detailed format of electronically transmitted messages). Some OCRs are also capable of performing PLA-to-RI conversions. If there is no OCR, the operator may manually reformat and key in the message. The message is then transmitted electronically using an AUTODIN specific protocol. At either the AMPE or ASC, the first several lines of the message are validated, and messages (known as service messages) are returned to the TCC operator, indicating the nature of any errors encountered. If the receiving device is an AMPE, PLA-to-RI conversion is performed and the message is sent to an ASC, and any local deliveries are made. The ASC makes delivery to its directly connected terminals, determines the destination ASCs and makes delivery to the "next hop" ASCs. One copy of the message is sent to each "next hop" ASC, together with only those RIs which each "next hop" ASC is responsible for routing to. This process is repeated until the message is delivered to all recipient terminals. At the recipient terminal, multiple copies of the message may be produced based on a number of criteria, such as office codes indicated by the preparer as additions to the receiving organization's PLA, the subject matter of the message, content indicator codes, NATO Subject Indicator Codes, or even the contents of the message text, dependent upon the operational requirements of the users supported by the recipient terminal. This message distribution determination may be done manually or may be automated in the receiving AMPE or terminal, depending upon the volume of traffic handled by the AMPE/terminal. The messages are then distributed to the actual recipients through normal administrative channels. While this is the basic concept of operations, there are a number of special actions which may occur, and many details that support user unique operational requirements have been omitted. The most important of these will be described in comparing the AUTODIN service to the DMS requirements.

3.1.4 Estimated Cost. The principal costs of the complete AUTODIN system include the backbone and the subscriber regional and/or organizational facilities operation and maintenance, personnel (military and civilian), connectivity, as well as equipment upgrades, replacements, software enhancements, and associated cryptographic equipment and peripherals. Also, equipment and installation for planned new sites is included. An estimate of the associated costs for FY88 is roughly $2 Billion which does not include costs associated with originator message preparation (external to the TCC) and conveying messages back and forth to TCCs.

3.1.5 Estimated Staffing. The total staffing effort directly associated with the annual operations and maintenance of the AUTODIN system is approximately 38,000 staff-years.

3.1.6 Comparison to Requirements.

a. Connectivity/Interoperability. The roots of AUTODIN as a military system cause it to place heavy emphasis on "commander-to-commander" communications, and the MAD, the official AUTODIN directory, extends only to that level of addressing. For example, the Secretary of Defense, together with the Office of the Secretary of Defense (OSD) (about 1900 people), has a single entry: SECDEF WASHINGTON DC. Since the number of messages received daily by the Secretary and OSD is on the order of 1200 to 2000, it is clearly impractical to expect the personal attention of the Secretary or even his immediate staff. A similar situation exists at any large military command. As a result, a number of locally standardized approaches are taken to reach the appropriate recipients. The most common of these is to include staff element identifiers with each PLA. This approach is specified by Service/agency message preparation formats and instructions, and is generally used as one of the methods to distribute messages. The staff element identifiers (office symbols) are not standard across Military Services and Defense Agencies, and their use may be difficult on messages which cross S/A boundaries. The result is that connectivity between commanders is essentially complete, although generally handled manually at both ends. Connectivity between lower elements of the organization, and even individuals, via "for" instructions in the message text, is accommodated. However, the manual operations and distribution efforts required at most TCCs can introduce substantial delays in communications between organizational elements.

b. Guaranteed Delivery. From entry into the sending TCC to initial delivery at the receiving TCC, AUTODIN takes many measures to avoid losing messages, and, in the unlikely event a message is lost, to inform the sender so that the message can be retransmitted. Messages are initially logged at the TCC, stored redundantly at the ASC or AMPE at which they are first received, and not acknowledged to the TCC until such storage is complete. Similar positive acknowledgments are required on each store and forward stage until final delivery to a TCC. Finally, if any destination TCCs are unable to deliver the message, the originating TCC is notified. There are problems, however, in the manual stage of the process at the sending and receiving ends. Feedback on errors may not be immediate, dependent upon the priority of the message. As a result, format errors may cause the messages to be sent back to the originator through normal distribution channels, and messages will be delayed or even lost in this process. On the receive end, the limitations in connectivity discussed earlier, and the lack of extension of automation, may cause messages to be distributed to the wrong user(s) within the recipient organization, with the potential for delays or even loss of some messages.

c. Timely Delivery. AUTODIN uses multi-level precedence to assure timely delivery of high priority messages. Many special actions are taken

to assure very rapid delivery to the actual user (rather than a distribution box at the TCC) for the highest precedence messages: (1) alternate routing (including to alternate destination TCCs) is used to bypass failed components; (2) preemption of messages in process is employed on input/output lines, and internally if necessary; (3) messages which would otherwise be rejected are marked as potentially flawed and delivered anyway; (4) alarms ring on receipt to get the operator's attention; (5) twenty-four hour a day staffing of the TCCs is provided to assure rapid response; (6) procedures at the receive end assure that the commander or duty officer is immediately notified of receipt. Total TCC-to-TCC time for high precedence traffic is no more than a few minutes. However, manual procedures at both ends may add substantially to the actual writer-to-reader time. Also, lower priority messages are given less extraordinary service, and a large volume of high precedence messages may delay the receipt of the lower priority messages at the TCC. Under extreme circumstances (e.g., high traffic volumes and a large number of high precedence messages) AMPEs or TCCs may remove routine messages from the system and mail them to the recipients. Portions of the AUTODIN also support perishable traffic, e.g., traffic (such as time-sensitive weather data) which the originator has requested to be removed from the system without delivery if it is not delivered within a certain time frame.

d. Confidentiality/Security. With a few exceptions for some unclassified access lines, all transmission lines in AUTODIN are protected with military encryption equipment. Terminals are identified by community of interest and classmarked with the security levels they are allowed to process. Messages in ASCs, AMPEs, and some terminals are checked for valid security levels prior to acceptance and before delivery. A variety of measures, including parity and block checksums and header/trailer sequence numbers on messages, are taken to maintain separation of messages. Software in the ASCs is extensively tested before release. Software, hardware, and procedures for AMPEs and TCCs are subject to a standard independent test before they are connected to AUTODIN, in addition to accreditation procedures of the owning organization. The resulting AUTODIN system is accredited for all levels of classified information although some terminal equipment and many TCCs are only authorized to receive certain levels of information. Much of the security is provided by procedures and by personnel security (e.g., TCC operators are typically cleared for the highest level of information authorized the TCC). Equipment is generally dedicated to AUTODIN. On-line programming and interactive access is not permitted, except in the case of AMHSs, which have on-line access.

e. Sender Authentication. TCC operators check for signature of the release authority on a message before it is transmitted. In most cases, physical access to a TCC is controlled, and appropriate identification is required.

f. Integrity. Within the system, and on most access lines, integrity is maintained by matching header and trailer sequence numbers, and character and block parity checks. Some code conversion will occur, e.g., from 8-level ASCII to 5-level ITA-2, unless prohibited by the sender. Asynchronous lines, especially those using ITA-2 line code (which includes no character

parity) may introduce errors which go undetected by the system. Another source of errors are the OCRs which occasionally misread a character on the DD Form 173.

g. Survivability. The AUTODIN backbone (15 ASCs and their interswitch trunks) incorporates redundant interswitch routing, with each ASC multiply connected to other ASCs. The routing between ASCs is switchable (under the control of the ASC operators) to deal with the failure of one or more ASCs. However, the backbone is not considered survivable and almost every stress scenario presumes the loss of some to all of the backbone, isolating surviving AMPEs and terminals. The AMPEs and terminals depend upon the AUTODIN for long-haul communications. Therefore, selected AUTODIN terminals and most AMPEs are connected to multiple ASCs. Additionally, selected AMPE subscribers are also multiply connected.

h. Availability/Reliability. Substantial equipment redundancy, 24-hour staffing, back-up power, alternate routing, multiple connectivity of ASCs, multiple connectivity between ASCs and AMPEs/TCCs, and redundant storage of messages are employed to provide very high availability and reliability in peacetime. The AUTODIN availability under stressed conditions is subject to its survivability.

i. Ease of Use. A few hours of training is required to prepare the usual AUTODIN message on a DD Form 173, and the actual entry of messages into AUTODIN at a TCC is normally done by trained operators. However, increased automation of TCCs, and extension of automation to users (in the form of pre-prepared message masks and other message preparation support) can reduce the amount of training required for users and can reduce the number/training level of TCC operations personnel. The TCC and other AUTODIN communications and cryptographic equipment is maintained by trained maintenance personnel, though the use of more modern equipment is reducing the numbers and training levels of these maintenance personnel.

j. Identification of Recipients. As indicated earlier, the MAD provides the address information required for commander-to-commander messages. While organizational element identifiers (office symbols) are widely used, there is no DoD-wide standard method for identifying recipients below the commander level. Users tend to build up a list of organizational element identifiers for those elements with whom they communicate routinely, and use those identifiers to address the majority of their messages. In other cases, the message is sent to the intended recipient's commander for further distribution determination and delivery. While the intent is to give the receiving commander the flexibility to determine the appropriate organizational elements for action and information, the practical effect is that two types of possible errors may occur; some messages are delivered to recipients who have no interest in the message and some messages are not delivered to interested organizational elements. Additionally, extra copies of messages may be distributed to ensure delivery to interested elements. Procedures are in place to prevent delivery of copies to users not cleared for them.

k. Preparation Support. The amount of message preparation support provided to users varies from virtually no support (other than the use of preprinted DD Forms 173), to office automation equipment/software which supports the proper placement of fields on DD Forms 173, to message editing/preparation terminals (connected to AMPEs) which provide the user with menu-oriented or mask-oriented support of message preparation. While there are no inherent limitations to such user support within the system, at the present time much of the support comes only at the level of office automation equipment/software. AMHS type systems may also be used for message preparation.

l. Storage and Retrieval Support. The ASCs and AMPEs store messages for retrieval. The ASCs may retrieve messages only for redelivery to the original recipients. The AMPEs may retrieve messages for redelivery to the original recipients and for readdressal to other recipients. AMHSs store messages and permit a range of operations, such as sorting, analysis, and editing into new messages. Full integration of AMHSs into AUTODIN is not complete.

m. Distribution Determination and Delivery. At many TCCs, especially lower volume TCCs, message distribution is determined manually. Messages are examined for staff element identifiers, subject matter, key words in a key word field (a NATO requirement), and key words in the text. The next step is to make copies of the messages and put them into distribution bins. At some AMPEs and TCCs, the above procedures are automated. Finally, administrative personnel pick up and deliver the messages to the intended recipients. AMHSs take a somewhat different approach. Users have profiles based on the same elements used by AMPEs, but rather than using these to cause delivery of the messages, only a notification of receipt is placed in a user accessible file. The user can then choose to read the message at a CRT, print it, or delete it based on no interest.

3.2 Electronic Mail on the DoD Internet (E-Mail).

The Defense Data Network (DDN) was established in 1982. It is a set of world-wide networks based on technology developed by the Defense Advanced Research Projects Agency (DARPA) as the ARPANET in the early 1970s. A major use of the ARPANET was providing electronic mail to the DoD research community. This capability was extended to other operational users on the DDN. At about the same time the DDN was established, the protocols in use were expanded to facilitate connection of baselevel transmission facilities (including local area networks) to wide-area networks such as the ARPANET and the new DDN networks. Collectively, the long-haul and baselevel transmission facilities are termed the DoD Internet.

3.2.1 Components.

The principal components of the E-Mail system are host computers supporting electronic mail, user terminals, on-line directories, and the DoD Internet. Except for some E-Mail hosts, all of these components may be used for many other purposes besides electronic mail, such as general purpose ADP, access to remote data bases, and general computer-to-computer communications.

a. Electronic Mail (E-Mail) Hosts. An electronic mail host is a computer which has (1) an application program which interfaces with users on terminals to compose, send, and receive messages; and (2) an instantiation of the Simple Mail Transfer Protocol (SMTP) and the necessary underlying protocols which allow it to send mail to and receive mail from other E-Mail hosts. Storage to keep received mail until users have read it is also required. Additional support, such as editors for composing messages, and sorting, storing, and retrieving messages after they have been delivered, may also be provided.

b. User Terminals. Almost any computer terminal or PC with terminal emulation software can be used for electronic mail.

c. Directories (DIR). The DDN Network Information Center (NIC) computer contains a directory of over 50,000 users of E-Mail. The directory contains the user's name and mailbox address consisting of an identifier for the user and an identifier for the E-Mail host; e.g., SMITH@DDN1.ARPA. Inquiries are made by users from their terminals. A second directory, which contains host names and corresponding internet addresses, used in the DoD Internet Protocol, is also located at the NIC. This directory is in the process of being distributed throughout the DoD Internet with only the "directory of directories" at the NIC. Processes internal to the mail hosts normally access this directory.

d. DoD Internet. This is not a DMS component per se, but is included for completeness. The baseline DoD Internet has three major divisions:

(1) Classified DDN. A set of physically, procedurally and cryptographically secured packet switching segments providing the backbone for classified E-Mail (e.g., DSNET 1, DSNET 2, DSNET 3).

(2) Unclassified DDN - A set of packet switching segments providing the backbone for unclassified E-Mail (e.g., MILNET, ARPANET).

(3) Baselevel Transmission Facilities. The baselevel transmission facilities consist primarily of the base cable plant including the main distribution frame(s) and dial central office(s). These facilities traditionally support switched voice circuits, dedicated point-to-point communications and simple star networks. Many digitization programs upgrading the baselevel transmission facilities are underway to allow more flexibility in the use of newer automation technologies for local area networking.

3.2.2 Connections. Asynchronous terminals may connect to DDN Terminal Access Controllers (TACs) directly or via dial-up circuits (for unclassified terminals). They may also connect to a host computer directly or through a LAN. Synchronous terminals currently connect directly to hosts, which then connect to the DDN. Computers, including those which act as E-Mail hosts, may connect to either a DDN network or a LAN network. The LANs are connected to the DDN by gateways or hosts using the DoD Internet Protocol. In a like manner, intropera bility with the research community (ARPANET) and the commercial community is accomplished by the use of gateways.

3.2.3 Concept of Operations. The following is a typical E-Mail scenario. A user logs onto an E-Mail host with a user ID and password. The sending user either uses a local list of commonly used addresses or requests the address of the intended recipients by typing, for example, "Who is Smith, John C.". The E-Mail host makes an inquiry to the NIC directory, and returns the address of the requested name. The user then requests the mail host to send a message by issuing a command, e.g., "send". The mail host then prompts the user for the addresses (usually with "TO" and "CC" prompts), the subject, and the text of the message. If the user is using a PC or workstation, a file on the workstation may be included as all or part of the text, so the message does not have to be composed while on-line to the mail host. Once the message is composed, some systems may permit the user to edit it. After the user is satisfied with the message, the user requests that it be sent by typing a command, e.g., "mail" or a message termination character. The mail host then immediately checks the addresses for proper format and correct host names (which may require inquiries to the NIC host directory, if the names are not already in the mail host's cache of host names and internet addresses), and informs the user of host addressing errors before returning control to the user. The mail host then adds "from", date and time fields to the message and sends the message to all of the recipient mail hosts through the DDN employing DoD standard protocols. Normally, only one copy of the message will be sent to each receiving E-Mail host, even though several addressees may be served by one host. If a receiving host is unavailable, the message is stored at the sending host for a period of time and periodic attempts are made to deliver it. After some time-out period, an undelivered mail notice is placed in the sender's mailbox, together with the unsent message. The receiving mail host checks the names of the intended recipients against those of the users it serves. If the recipient is registered, the message is placed in the appropriate mailbox. If the recipient is not on that host, it may check for users on a forwarding address list. If the recipient is not on either list, the sending host is notified, and a non-delivery notice is put in the sender's mailbox. When the recipient signs onto the mail system at some later time, the system indicates mail has been received. The recipient can normally scan through the message subjects and senders (and on some systems, search the text and other fields for key words) and read, save or discard the messages based on the results. If the recipient has a printer available, the message may be printed. In some cases, if requested by the sender, the receiving system may deliver a notification message to the sender when the receiving system has sent the message to the user's terminal. If the user wishes to reply to the message, the user issues a command, e.g., "reply". In this case the user need enter only "cc" addressees and the text of the reply because the system enters all other fields. The recipient may also forward the message to other recipients. Finally, the user may keep some number of messages on file at the mail host for whatever purposes needed, for example, to maintain history files on different subjects. Alternately, messages may be stored at the user's PC, although the ability to manipulate messages based on field contents may be lost unless the user has applications software for that purpose.

3.2.4 Estimated Cost. The principal costs of E-Mail are the operation and maintenance of the related equipment. Operation and maintenance of the DDN itself currently costs approximately $100M annually. This includes the backbone, directory services, access lines, and cryptographic equipment. Since the DDN is still expanding rapidly, annual operations and maintenance costs are expected to rise. Most DDN host computers perform many functions and are not dedicated to E-Mail. Considering backbone and host costs, electronic mailboxes are currently available for an estimated annual average cost of $1000 per mailbox. Assuming one mailbox per registered user, costs associated with DDN E-Mail hosts are approximately $50M per year.

3.2.5 Estimated Staffing. Total DDN staffing, government and contractor, is about 300. A current estimate of manpower for E-Mail hosts is one person per 500 mail accounts. With the 50,000 user estimate, another 100 people are committed to support them. Therefore, total current staffing is estimated at 400. Personnel maintaining base LANs and COMSEC are not included.

3.2.6 Comparison to Requirements. User requirements are not uniformly satisfied by E-Mail, because the host software supporting the user is not standard. With the exception of the DDN's Simple Mail Transfer Protocol (SMTP), the remainder of the user service is provided by the host hardware, software and cable distribution. The user's perception of the service is determined primarily by the host's capabilities and limitations.

a. Connectivity/Interoperability. E-Mail service is provided on several disjointed network segments which are physically separated by security classification. For purposes of electronic mail, the unclassified segment of the DDN is a single open system. Any unclassified mail user can communicate with any other unclassified user. The number of users registered in the DoD Internet Directory is over 50,000. These users have mailboxes (which may be shared) and most have individual directory entries. There are many other users with mailboxes who are not entered in the directory, usually because they communicate only with other users or an individual host or a set of hosts with its own directory. Such users may still send and receive mail, but identifying them is more difficult. Mailbox owners also are generally willing to pass messages to other individuals, but no formal procedure is in place. The classified segments of the DDN are not connected to the unclassified segments nor to each other, and messages cannot be sent between them without a manual extraction from one and reentry into another.

b. Guaranteed Delivery. The source mail host keeps outgoing messages until it has confirmation of receipt from all destination mail hosts. In general, messages are stored on disk only once at the source and destination, so there are windows in which a single disk crash can cause the loss of a message, e.g., between back-ups and before transmission (at the source) or delivery (at the destination). In such cases, users are rarely notified that a message may be lost. If a sender is particularly concerned that a message has been delivered and read, the recipient can be requested to reply (acknowledge) in the body of the message. Since replies are extremely easy (see concept of operations), this approach provides a manual

technique to work around the message loss problem, but only if the sender is aware of the potential loss. Again, no standard procedures are available to cover this potentially serious problem.

c. Timely Delivery. Since critical command information is not passed using E-Mail, timely delivery in E-Mail may be expressed in terms of fractions of hours and hours rather than in minutes. As a result, many mail hosts have a process which "wakes up" from time to time to deliver mail. There are no set standards, but, in general, the process is activated at least every fifteen to thirty minutes. On some systems, the user can cause the process to "wake up" immediately (i.e. interrupt) upon receipt of a message. As a result, mail messages are generally sent and received at the destination mail host, and put in the recipient's mailbox, within half an hour. Once mail is delivered to a user mailbox, it remains there until the recipient reads it. Generally, this is dependent upon the recipient's work schedule, and there is no assured time by which it will be read. Some organizations may procedurally require frequent reading of mail; most currently do not.

d. Confidentiality/Security. Limiting recipients to those cleared for the information is accomplished by physically segregating the DDN by different classification levels. The classified segments of the DDN are protected by encryption on all lines and by facility, personnel, and procedural measures appropriate for the level of classification of the segment. Generally, "system high" computer environments are used and computer security measures are those appropriate to the environmental security level. In the unclassified segment, more limited measures are provided such that the users must know who has access to addressee mailboxes before sending sensitive unclassified information. These security measures are increasing, as described in the DDN Subscriber's Security Guide.

e. Sender Authentication. There are few restrictions on senders of electronic mail, hence sender authentication is a weakness of current E-Mail. While the system normally enters the sender's identifier in the mail message, it is possible to override this mechanism on many E-Mail host systems. Sender authenticity is therefore usually determined by the reasonableness of the message. In case of doubt, the purported sender can be contacted by other means for verification.

f. Integrity. Protocols used internally in the internet provide excellent integrity between the sending and receiving mail hosts. Cyclic redundancy checks are provided on links, and end-to-end checksums are used in the DoD Internet Protocol and Transmission Control Protocol. Similar capabilities are present in the equivalent OSI protocols. There is still the potential for undetected problems between the mail hosts and user terminals at both the source and destination. These access lines tend to employ asynchronous transmission with only character parity checks and limited start/stop flow control. Data overruns are not uncommon. A variety of non-standard approaches are being taken to overcome this problem. They include slowing down transmission rates, using asynchronous line protocols (such as KERMIT and X.MODEM), and employing print spoolers.

g. Survivability. The DDN, the long distance communications for the DoD Internet, contains over 150 packet switches in the unclassified MILNET, and over 60 packet switches in the classified segments. The switches themselves are each multiply connected to other switches, and routes between switches are automatically and dynamically computed. The number of subscribers per switch is relatively small and they are usually near the switch. These features result in high survivability against threats other than nuclear or massive conventional attacks.

h. Availability/Reliability. Extraordinary measures to assure availability, such as uninterruptible power supply (UPS), redundant systems, and on-site maintenance, are generally not provided for E-Mail due to its noncritical, administrative nature. Mail hosts generally have good availability during normal office hours and under normal conditions. The principal cause of downtime appears to be for host system back-ups, which are usually performed at off-peak hours. Host availability and speed of service for the users are also influenced by such items as local power, local weather, and local prioritization of other jobs on a multi-function host. Users with high availability requirements may have several mailboxes on different mail hosts. This approach helps on outgoing messages, but is of limited use on incoming messages, and of no use for accessing messages already delivered to the unavailable mail host.

i. Ease of Use. Users generally can send and receive typical messages after a half hour of training. System feedback for most errors is immediate, and on-line help facilities are provided. In case of difficulties, either the mail host administrator, or a network help facility can be contacted. Use of capabilities, and extended retrieval capabilities (such as by key word search, subject, or sender) require some additional training, but also tend to be easily mastered. Because the host mail software is not standard, users moving from one host to another may need to learn another system for handling mail.

j. Identification of Recipients. The sending user either uses a local (personal) list of commonly used addresses or requests the address of the intended recipients by accessing the NIC directory ("WHOIS" function). The E-Mail host makes an inquiry to the NIC directory, and returns the address of the requested name. If there are multiple instances of the name, or if the user only knows part of the name (Smith or Smith, John) then all the matches are returned with the full name and a unique identifier for each name. By entering the unique identifier, more information about the individual is given to the user, such as street address and telephone number. With this information, the user can determine the correct recipient, if the recipient is in the directory. Users are registered in the directory by their E-Mail host administrator who uses E-Mail to register them. The existing directories are adequate for the current user population. However, as the number of users grows, it is expected that a more decentralized directory system will be needed, and work has been initiated to provide for this. A major issue in expanded, decentralized directories, is access control for entering information in the directories themselves. Another problem, which is likely to grow under the current approach, is misidentification of recipients. Since user mailboxes tend to

employ user names, a message to SMITH@DOD1.IL is likely to be delivered. Unfortunately, there is no guarantee it will be delivered to the right Smith.

k. Preparation Support. Message preparation may be done on-line with substantial support by the system, including limited editing capabilities. Feedback on errors is provided as soon as the system can identify them. Some host mail systems allow users to build messages by merging notes prepared with word processing software either resident on the host or on the user's workstation.

l. Storage and Retrieval Support. There are neither standard nor mandated message storage capabilities, but most systems provide some amount of on-line storage under the control of the user. Some host systems provide capabilities to retrieve messages, either on initial delivery or after they have been saved, using a number of criteria. Messages, in some systems, may be filed into categories for future reference. Stored messages may be included in forwarded messages. The sender address, courtesy copy addressee(s), and subject field of saved messages may be used to build "reply" messages, to avoid the look-up of recipient addresses in many cases.

m. Distribution Determination and Delivery. Automated distribution determination and delivery of messages based on subject or other criteria is not supported. The responsibility for distribution (and redistribution) of messages rests with the users. Pre-established mailing lists based on interest groups may be used, however, to assist in both initial distribution by the sender and redistribution by any holder of the message.

DMS Architecture

Section 4

Phase I Implementation

4.0 Introduction.

Figure 4-1 illustrates the architecture at the end of Phase I (CY1993). This section presents the objectives, a description of the architecture and an overview of the actions planned to implement the Phase I DMS Architecture. It should be noted that the Phase I actions have the effect of providing the foundation for the major advances which take place in Phases II and III.

4.1 Phase I Objectives.

4.1.1 Decrease Cost and Staffing. Reduce TCC cost and staffing requirements and extend service to users.

4.1.2 Improve Writer-to-Reader Service. Originator to recipient service will be improved by extending the messaging interface to the user level.

4.1.3 Equipment. Begin to phase in evolvable equipment and phase out obsolete equipment.

a. Phase In. Phase in replacement equipment that will be maximized for ability to evolve through successive transition steps in support of the DMS architecture. In addition, there will be new transitional components to initiate the integration of AUTODIN and E-Mail and allow migration of AUTODIN data pattern traffic to the DDN.

b. Phase Out.

(1) Digital Subscriber Terminal Equipment (DSTE)

(2) DCT-9000 TCC systems

(3) Standard Remote Terminal (SRT) equipment

(4) Automated Multi-Media Exchange (AMME) Systems

(5) Teletype Models 28 and 40

(6) Honeywell CCT-07 TCC systems

(7) Control Data Corp CDC-1700 systems

(8) AF RAIDS (Univac 418 III systems)

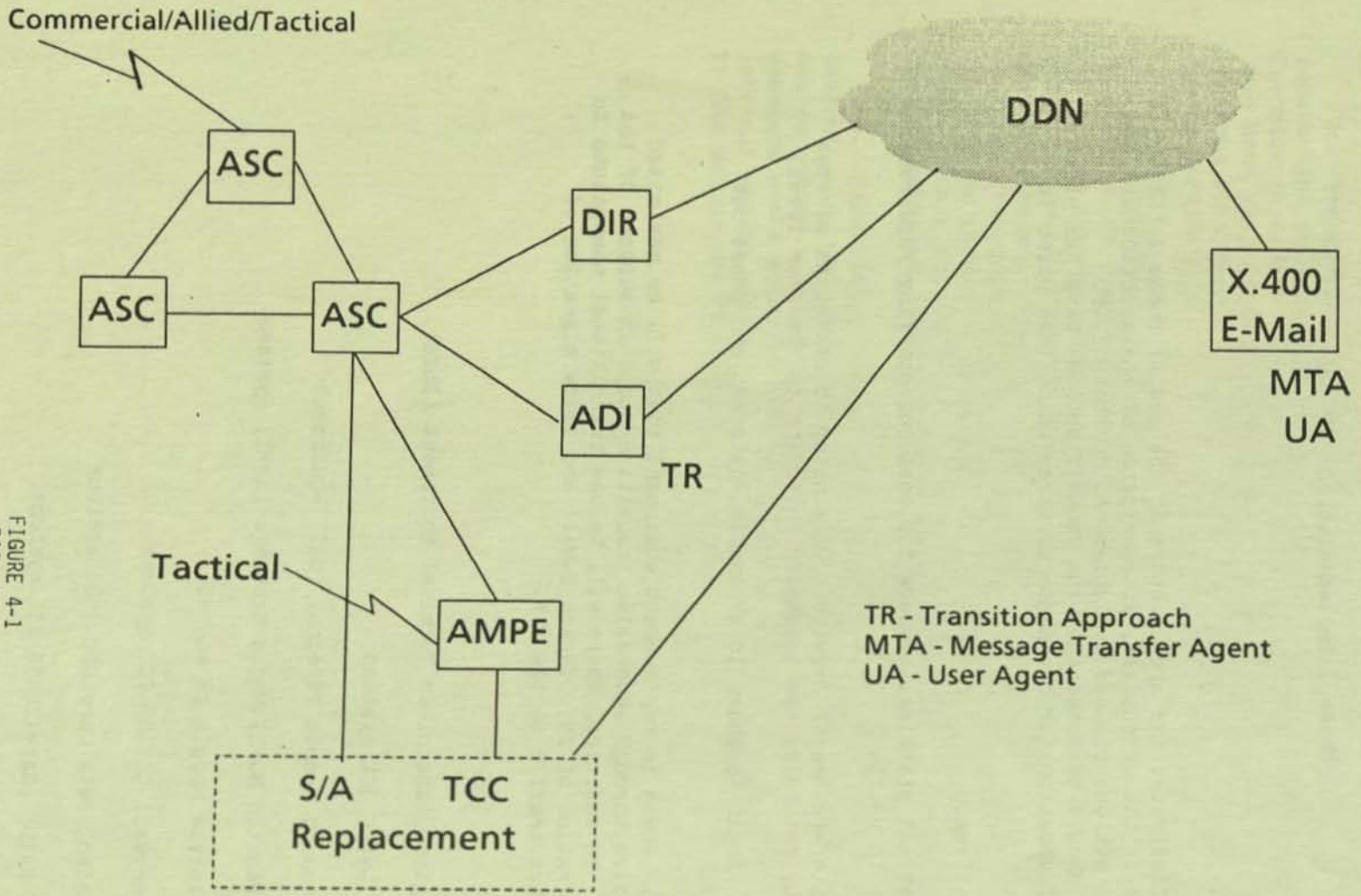


FIGURE 4-1
PAGE 4-2

Phase I Architecture
1993

4.1.4 Protocols/Services. Begin to phase in new protocols/services and phase out obsolete protocols/services.

a. Phase In.

(1) Government Open Systems Interconnection Profile (GOSIP)

(2) X.400 Message Handling Systems

(3) High-level Data Link Control (HDLC) for subscribers

(4) New asynchronous protocol(s) with reliable transfer for subscribers.

(5) X.500 Directory Systems

b. Begin Phase Out of the Following Protocols/Services.

(1) FIELDATA line code

(2) ITA2 line code

(3) DCS Mode I, II and V protocols

(4) AUTODIN Sequential Delivery Service

(5) AUTODIN Query/Response Service

(6) Hybrid AUTODIN Red Patch Service (HARPS)

(7) Simple Mail Transfer Protocol (SMTP)

(8) Transmission Control Protocol (TCP)

(9) DoD Internet Protocol (IP)

(10) Extended Binary Coded Decimal Interchange Code (EBCDIC)

4.1.5 Formats/Procedures. Begin to phase in new formats/procedures and phase out obsolete formats/procedures.

a. Phase In. Begin development of a simplified Common Message Format (CMF) under the aegis of the MCEB's ACP XXX effort. A CMF is needed to fully realize the DMS requirement to allow a user to communicate with any other user. The CMF is intended specifically for both organizational and individual messages in the X.400 messaging environment of the DMS. It is important to note that transition from the AUTODIN specific formats and procedures to the X.400 based CMF will require that the existing formats be accurately mapped to the CMF. Particular emphasis will be placed on ensuring that the security requirements associated with the existing formats (ACPs, JANAPs, DOIs) are fully satisfied as part of this mapping. A thorough review of the format and procedural requirements associated with

the existing TCC oriented messaging service will be required to determine their applicability or need for modification as messaging service is extended to the user.

b. Begin Phase Out of the Following Formats/Procedures.

(1) Non-Standard E-Mail Formats/Procedures

(2) ACP-127 US SUPP-1

(3) ACP-126 Modified (NTP-4) (for DMS)

(4) JANAP 128

(5) DOI-103 (to include DOI-103 Special and evaluation of indefinite use of the existing CRITIC format)

(6) STREAMLINER Abbreviated Message Format (AMF)

(7) Abbreviated SI format

4.1.6 Media. Media that is costly, bulky or staffing intensive will be phased out. Examples include punched card and paper tape.

4.1.7 Transfer Data Traffic to DDN. Special emphasis must be placed on the migration of data traffic away from the messaging system and toward direct data transfers across the DDN.

4.2 Phase I Architecture.

Figure 4-1 illustrates the Phase I architecture. The major emphasis in Phase I is to alleviate the cost and staffing problems associated with AUTODIN's TCCs via extension of automation to the user, system upgrades by replacement systems, and implementations at sites not currently automated. Further, there are three other important structural changes from the baseline. First is the addition of AUTODIN-DDN Interfaces; second is improved directory services; and finally, X.400 individual messaging is initiated.

4.2.1 Components. The Phase I components are the baseline components (Section 3, paragraphs 3.1.1 and 3.2.1) plus transition components. As many Phase I replacement and transition components as possible will use platforms (hardware and/or operating system) which are evolvable to components needed for Phases II and III. Some individual messaging components will begin the transition to X.400.

a. AUTODIN Switching Centers (ASCs). These are the 15 ASCs of the baseline (see 3.1.1 a). There will be software and hardware changes during this phase for continued viability and operations and maintenance (O&M) cost reduction, and to enable deployment of evolvable platforms.

b. Automated Message Processing Exchanges (AMPEs). These are the AMMEs, LDMXs, AFAMPEs, etc., of the baseline (see 3.1.1 b). Specific

emphasis will be placed on phasing out the AMME systems during Phase I to resolve high O&M cost and obsolescence problems.

c. Telecommunications Centers (TCCs). These are the TCCs of the baseline (3.1.1 c). A number of the baseline TCC systems will be replaced primarily because the existing TCCs (e.g., DCT 9000, 418 III) are not economically maintainable but also to deploy evolvable platforms, increase automation and extend messaging service to the users to the maximum extent possible.

d. Data Processing Installations (DPIs). These are the DPIs of the baseline (3.1.1 d). Actions will be initiated during Phase I via ADI components to migrate data pattern traffic from AUTODIN to DDN.

e. Automated Message Handling Systems (AMHSs). These are the AMHSs of the baseline (3.1.1 e).

f. DMS Directory (DIR). Initial directory improvements include automation of the AUTODIN baseline's paper documents (3.1.1 f); the Message Address Directory (MAD) and the ACP 117 CAN-US SUPP-1. The DIR is a transitional capability which will ultimately be integrated with the current E-Mail Directory to provide an initial integrated DMS DIR capability. The mature X.500 based integrated DIR with SDNS protection is targeted for Phase II.

g. AUTODIN-DDN Interface (ADI). To facilitate initial integration of AUTODIN and E-Mail, gateways or bridges are required. Currently four versions of ADI are being considered.

(1) Narrative Message ADI. This ADI provides AUTODIN and E-Mail subscribers the capability to intercommunicate (initially at the unclassified level).

(2) Data Pattern ADI. This ADI facilitates the migration of AUTODIN's data pattern traffic to the DDN.

(3) AUTODIN Trunking ADI. This ADI provides ASC-to-ASC interswitch trunking via the DDN.

(4) AUTODIN Subscriber Access ADI. This ADI allows AUTODIN subscribers to obtain ASC access via the DDN.

h. Electronic Mail (E-Mail) Hosts. These are the E-Mail hosts of the baseline (3.2.1 a). However, during Phase I, a translation capability between X.400 and SMTP individual messages (mail bridge) will be deployed, followed by deployment of X.400 based Message Transfer Agents (MTAs) and User Agents (UAs) for individual messaging. These initial deployments begin the migration to X.400 messaging that will be expanded during Phase II.

i. DoD Internet. This is not a DMS component per se, but is included for completeness. Major changes in the long-haul and baselevel transmission capabilities are not anticipated by the end of Phase I.

(1) Defense Data Network (DDN). The primary change occurring during the DMS Phase I time frame will be implementation of BLACKER host-to-host protection elements which will ultimately result in an integrated DISNET. By 1993, it is envisioned that the DDN will consist of the MILNET (unclassified) and DISNET (classified) segments connected by BLACKER protected gateways.

(2) Baselevel Transmission Facilities. By the end of Phase I, telephone modernization projects, implementing ISDN-based capabilities, are expected to be underway. Full-scale implementations of baselevel Installation Information Transfer Systems (IITS), are not anticipated until the Phase II time frame.

j. User Terminals. Both AUTODIN and E-Mail have a plethora of terminals used for sending and receiving messages. However, with Phase I automation of TCCs and extension of messaging service to the users, changes in the type and location of the AUTODIN terminals will occur. As X.400 UAs are deployed during Phase I, service derived by the users will not change appreciably even though the terminals will begin the evolution from baseline components to X.400 User Components (UCs).

4.2.2 Connections. The interconnectivity is essentially that of the baseline except for the improvements at the baselevel and the ADIs which provide bridges between AUTODIN and DDN. Phase I DIR improvements also offer changes in writer-to-reader connectivity by improving interoperability and reducing the need for manual handling of messages. The distinct nature of AUTODIN and E-Mail remains at the end of Phase I, but interoperability, extension of message service to the users and flexibility for change have been introduced. Connectivity with the Allied, Commercial and Tactical communities continue to be provided by tailored interfaces but by the end of Phase I, it is envisioned that the Tactical community will be actively involved in the DMS evolution.

4.2.3 Concept of Operations. Phase I is a transitional phase beginning with AUTODIN and E-Mail as separate and stand-alone capabilities and ending with initial integration. Many of the basics, the "ABCs" of military messaging, are changing.

a. Some AUTODIN users will see significant improvements in service as the extension of automation eliminates the need to create a paper DD Form 173 which must be hand carried to a TCC for OTC processing. The clerk or secretary who types today's DD Form 173 will be capable of sending messages directly and electrically by the end of Phase I. The automated TCC will ensure that only fully formatted procedurally correct messages are sent to AUTODIN. The Army plans to reduce the size and subsequently phase out TCCs by shifting a significant volume of unclassified AUTODIN messages to DDN, initially as E-Mail, later as X.400 individual and organizational messages.

b. E-Mail users will initially experience little change as the E-Mail community moves from SMTP to X.400. While this change is largely the replacement of one protocol for another, it is a significant step toward the Target Architecture of 2008. Initial versions of X.400 based UAs and MTAs

will be processing individual messages. X.400 based organizational messaging will not be initiated until Phase II.

c. To facilitate initial integration of AUTODIN and E-Mail messaging services, the transitional ADI and DIR DMS components are required. At this point, two ADI efforts are underway: Army's AUTODIN Mail Server (AMS) to provide AUTODIN and E-Mail narrative message interoperability for GENSER unclassified messages; and DLA's Data Pattern ADI capability for migration of AUTODIN data pattern traffic to the DDN. Both of these capabilities will be implemented at the baselevel. By the end of Phase I, it is envisioned that these capabilities will be implemented regionally so all users can derive these interoperability benefits and the DMS will be postured for evolution to Phase II. Very closely related to the ADI efforts are the Phase I Directory (DIR) improvements. Major Phase I DIR objectives are: automation of the current AUTODIN Directories, expansion and standardization of current AUTODIN Plain Language Address-to-Routing Indicator (PLA-to RI) conversion services and initial integration of the AUTODIN and E-Mail Directories. ADI and DIR efforts will be highly interdependent and the messaging policy and procedural changes necessary cannot be underestimated. Nevertheless, by the end of Phase I, the objective is to have initial interoperability between AUTODIN and DDN subscribers and the availability of a centrally managed, regionally implemented, integrated Directory.

d. Phase I sees the first evolutionary steps in what amounts to a revolutionary change in the current concept of operations. Formats, media, procedures, protocols, hardware, software, etc. will be significantly different in the 2008 Target Architecture as compared to the 1988 Baseline Architecture. Messaging in 2008 will be performed primarily by the users as opposed to the 1988 situation where thousands of communicators over and above the personnel at the writer and reader level are involved in messaging.

4.2.4 Estimated Cost. Given that the current DMS Implementation Strategy consists of a large number of candidate actions, accurate cost estimates are not currently available. However, the cost of anticipated upgrades can be expected to yield operations and maintenance savings near-term; and termination of recurring costs yield continued savings in the outyears. These savings are expected to be larger than the investment within one or two years. These savings are attributed to reduction in maintenance costs resulting from replacement of obsolete systems and reduced personnel costs resulting from the decreased staffing.

4.2.5 Estimated Staffing. By reducing the amount of manual intervention required for current message processing and replacing or upgrading some of the high maintenance components of the baseline DMS, staff years of effort could be saved between 1988 and 1993 as a result of anticipated Phase I actions, which translates to savings by the end of Phase I.

4.2.6 Comparison to Requirements. Each requirement contained in DMS MROC 3-88 (also listed in in Paragraph 1.4.3) is listed below with a brief

explanation of changes made to the current baseline by the implementation of Phase I. Where there has been no change in the satisfaction of a requirement, this is so stated.

a. Connectivity/Interoperability. The connectivity and interoperability will be significantly improved as a result of the introduction of AUTODIN-DDN Interfaces (ADIs) and the associated DIR improvements. The ability for individual users to have ready access to any/all messaging services will be improved and initial rationalization of AUTODIN/DDN message traffic will be possible.

b. Guaranteed Delivery. The implementation of more sophisticated protocols will provide guaranteed delivery and notification to the sender. This will replace the existing protocols and manual procedures to guarantee delivery.

c. Timely Delivery. As the messaging interface is extended to the user level, significant improvement in writer-to-reader speed-of-service will be realized based on the reduction of manual handling.

d. Confidentiality/Security. No significant gains are anticipated during Phase I.

e. Sender Authentication. Sender authentication is not significantly improved. Real improvement from a security standpoint will be realized with SDNS electronic signature use during Phase II.

f. Integrity. As obsolete baselevel equipment and protocols such as DCS Modes II and V are replaced by newer equipment and standard protocols, end-to-end message integrity will improve.

g. Survivability. While the survivability of the AUTODIN Switching Centers is unchanged, the potential interconnection via ADIs to DDN would mitigate the impact of losing multiple ASCs. Surviving subscribers capable of interfacing an ASC via the DDN would have a probability of obtaining connectivity via DDN and the ADIs to surviving ASCs. ASCs could avoid isolation by using the DDN for trunking.

h. Availability/Reliability. The phase in of evolvable equipment and the phase out of obsolete equipment should result in availability and reliability improvements as well as reduced O&M costs.

i. Ease of Use. The improvements in terminal equipment available to the user and improved directory service should contribute to improved ease of use.

j. Identification of Recipients. The directory service improvements planned for Phase I should result in improvements in service to the users.

k. Preparation Support. The introduction of new terminal devices and improved directory service will result in improvements in this area. As the messaging interface is extended to the user, user friendly message

preparation support will obviate the need for trained communications personnel to send/receive messages.

l. Storage and Retrieval Support. No changes to the current baseline are planned by the end of Phase I. Introduction of the X.400-based Message Storage Agent (MSA) is not expected until Phase II.

m. Distribution Determination and Delivery. Extending service to users is an improvement since it begins the phase out of over-the-counter (OTC) service. Message distribution services must be improved in order to effect message distribution to the correct offices (UA's).

4.3 Phase I Actions Overview.

Listed below are candidate actions selected by DMSWG members to implement the proposed Phase I Architecture. The following paragraphs summarize the intent for each of the candidate actions which are categorized as policy, procedural and component. Additional system analysis and system engineering effort is required to determine the feasibility and/or relative merit of these candidate actions, and some of them will need to be reevaluated to ensure compliance with the DMS MROC requirements currently being validated. Consequently, it is important to view the following as actions "proposed" vice actions "required" to implement the Phase I Architecture.

4.3.1 Policy Actions. To achieve the Phase I Architecture, a number of policy actions are required.

a. Overall DMS Policy. Upon formal approval of the DMS by the DAB/C3I Systems Committee, the overall DMS Policy will be specified in a DoD Directive.

b. DMS Multicommand Required Operational Capability (MROC). The MROC will provide validated DMS writer-to-reader requirements. This joint action is underway and should be completed by the end of 1988.

c. JCS Policy Revisions. To accommodate the transition from AUTODIN and E-Mail to the DMS, several existing JCS documents must either be amended or replaced. In either case, new wording is required to cover transitional changes. Depending on the degree of specificity, this action may have to be iterated during the period of user transition from AUTODIN and E-Mail to the X.400 organizational and individual messaging (approximately 1989 through 2000). Paragraph 5.3.1b addresses specific JCS Policy issues that must be resolved during Phase I to enable the architectural changes planned for Phase II.

d. DMS Security Policy. Specific DMS security policy guidance, initially addressing the areas outlined in paragraph 2.7, will be developed and included in Appendix C of this document. As additional DMS security issues surface or security policy guidance changes, DMS security accreditation representatives will reflect such additions and/or changes in Appendix C for subsequent revisions of the document. Examples of additional

security policy issues that must be resolved during Phase I are the SDNS issues outlined in paragraph 5.3.1c.

e. DMS Component Development Policy. Thus far, three classes of projects have been identified; "Central", "Joint" and "User" unique. The "User" class will be processed using existing policy. "Joint" and "Central" classes of projects are new and unique to DMS; thus, new policy is required to define the classes and the process(es) for their identification, funding, development, test and deployment. An early DMS Panel initiative will be to establish the process by which existing and proposed DMS projects are evaluated for consistency with DMS goals and to determine how results will be shared across the Services and Agencies.

4.3.2 Procedural Actions. The DMS migration to X.400 based messaging will require numerous procedural actions.

a. DoD Message Release. Obtain Service and agency agreement on exactly what constitutes certification of release to support automation of message release.

b. AUTODIN/DDN Subscriber Message Exchange. This action addresses the procedures required for exchange of narrative messages between AUTODIN and DDN E-Mail subscribers (initially SMTP based E-Mail).

c. PLA-RI Conversion for Non-AMPE Subscribers. This action will develop the procedures necessary to make the capability of 4.3.3 b (3) available to all AUTODIN customers who are not currently provided a plain language address look-up and routing indicator assignment (with associated reformatting) service from a Service or Agency AMPE.

d. Over-the-Counter (OTC) Diskette Service. The current office automation equipment of choice is the personal computer, to include a word processing software package. Thus, floppy disks are a medium that is widespread. Standard procedures are required for OTC diskette operations. This action will develop the necessary DoD-wide procedures for OTC handling of messages via diskettes.

e. DoD Use of X.400. With the advent of X.400 messaging, new procedures are required. This action will develop the necessary DoD-wide procedures for both organizational and individual messaging via X.400. A new Common Message Format (CMF) will be developed and documented in an Allied Communications Publication (ACP XXX).

f. Revised Naming/Addressing Conventions. In the transitional DMS (prior to full X.400 implementation), naming and addressing conventions for naming and addressing destinations in the DDN from AUTODIN and destinations in AUTODIN from the DDN are required. This action develops those conventions. In preparation for Phase II X.400 messaging and X.500 directories, definition and use of an X.500 naming structure should be accomplished during Phase I.

g. GENSER TS and SCI Delivery Points. This action is to develop the necessary procedures for combining GENSER Top Secret with DSSCS traffic. The resulting modified R/Y organizational and installation delivery points would be responsible for receipt, generation, control and distribution of GENSER TS and DSSCS traffic.

h. DSSCS/GENSER Component Development, Life Cycle Support (LCS). This action will develop procedures for the development and life cycle support of components fielded in both R and Y communities.

i. AUTODIN/DDN Data Pattern Exchange. This action will develop the procedures for the utilization of both AUTODIN and DDN for data pattern traffic. This is a necessary companion to the Data Pattern ADI action of 4.3.3 a (2).

j. Writer-To-Reader Organizational Message Accountability. This action will develop an expanded set of DCS AUTODIN Category III certification test procedures. The expanded test procedures will ensure organizational message accountability from writer-to-reader.

k. OUA, UA and MTA R&D Test Procedures. This action will develop procedures for performing research and development testing of X.400 based Organizational User Agent, User Agent and Message Transfer Agent DMS applications with Secure Data Network System (SDNS) protection.

4.3.3 Component Actions. To achieve the Phase I Architecture, several new components are required. The following component actions are proposed for completion during Phase I.

a. AUTODIN-DDN Interface (ADI). A major component is a bridge or gateway between the baseline backbones. Four ADIs have been proposed, each with a unique purpose. Additional systems analysis/system engineering effort is needed to determine if all are required or conversely, if these four are sufficient. For example, it is possible that regional vice baselevel implementations of the Narrative and Data Pattern ADIs would benefit substantially more users than the efforts currently underway.

(1) Narrative Message ADI. An existing Army project, AUTODIN Mail Server (AMS), provides a software package resident on the standard Army E-Mail Host that accepts either AUTODIN narrative or DDN SMTP (later X.400) formatted messages, converts the messages to the opposite format, and forwards the messages into the opposite system. The AMS performs all necessary format and addressing conversions.

(2) Data Pattern ADI. An existing Defense Logistics Agency (DLA) project will home its Defense Automatic Addressing System (DAAS) hosts to the DDN and allow its small users homed to AUTODIN to continue to receive service from the DAAS. This project is an initial step taken to enable the transfer of data pattern traffic from AUTODIN to DDN.

(3) ADI for AUTODIN Trunking. This project will analyze, develop, test and deploy an ADI which allows the DDN to provide some of

AUTODIN's interswitch trunking.

(4) ADI for AUTODIN Subscriber Access. This project will analyze, develop, test and deploy an ADI which allows the DDN to provide AUTODIN subscriber access to ASCs.

b. Directory Improvements (DIR). The DIR projects are a necessary companion to the ADI projects. Additional system analysis/system engineering is needed to determine optimum approaches to directory improvements.

(1) Automated Message Address Directory Service. This project will analyze, develop, test and deploy an automated alternative to today's paper Message Address Directory (MAD).

(2) Automated PLA-RI Translation Service. This project will analyze, develop, test and deploy an automated alternative to today's paper ACP 117.

(3) Expansion of Automated PLA-RI Conversion Service. This project will analyze, develop, test and deploy PLA-RI translation services (and message reformatting) for messages entered at a TCC connected to an ASC. This effort will result in a standardized and upgraded capability to provide the PLA-RI functions currently performed by AMPEs.

(4) Automated DDN/AUTODIN Name/Address Translation Service. This project will provide a centrally maintained X.500 Directory Service at the network/regional level to satisfy the DMS "Identification of Recipients" requirement. As a follow-on to the previous task, this task is to integrate the DDN Directory and the expanded (centrally maintained) DMS regional directory in preparation for a Phase II SDNS-compatible X.500 fully integrated DMS Directory Server.

c. X.400 Individual Messaging. The projects in this category represent the initial steps in the conversion from 1988 messaging to the target 2008 messaging. These projects only impact individual messaging.

(1) SMTP - X.400 Bridge for Individual Messaging. This project will develop, test and deploy a translation capability between SMTP and X.400 messages. This is a prerequisite to deployment of X.400 MTAs and UAs.

(2) Deploy X.400 MTAs and UAs. Upon the fielding of the SMTP-X.400 Bridge, this task will acquire, test and deploy X.400 Message Transfer Agents and User Agents.

d. Service/agency TCC Automation/Extension of Automation to Users. These projects are intended to alleviate a serious baselevel problem of staffing intensive TCCs, some of which use systems (e.g. DCT 9000) which are obsolete and virtually unsupportable.

(1) Army TCC Automation. This project initially automates the distribution of unclassified narrative traffic to the user using E-Mail

technology and migrates data pattern traffic to the DDN. The need for an end-to-end security capability is acknowledged to satisfy classified messaging requirements.

(2) Navy TCC Automation. This project will replace existing Remote Information Exchange Terminals (RIXTs) with state-of-the-art COTS NDI terminals which are capable of evolving into DMS components, and will transition TCC services to user commands via the PCMT and OAS components.

(3) Air Force TCC Automation. The lead project in this effort is the Formal Message Handling Service (FMHS) 2000 which will replace existing Air Force terminals (Standard Remote Terminals, AFAMPEs) with a single modular system. Subordinate near-term projects involve replacement of the DCT-9000 and Lundy-Farrington OCRs. The Host AUTODIN Message Processing System (HAMPS) program electrically connects the AF Data Processing Centers (DPC'S) to AUTODIN through an AUTODIN Interface Device (AID) or the backside of an AFAMPE.

(4) DLA TCC Automation. This project will replace existing AUTODIN interface systems with AFAMPE-like systems. This is primarily a cost avoidance effort. DLA plans for the new systems to be upgraded to DMS components in the future.

(5) DIA TCC Automation. This project will eliminate hardcopy distribution, reduce staffing and ensure timely delivery to all recipients.

(6) NSA TCC Automation. The NSA has several projects to upgrade NSA and Service Cryptologic Element headquarters and field activities' TCCs with state-of-the-art hardware and software as part of the Telecommunications Improvement Program (TIP) of the Agency's Global Telecommunications Service Architecture.

(7) Other TCC Automation. This is an umbrella effort to work with non-DoD AUTODIN subscribers to ensure that all subscribers are compatible and interoperable with the DMS.

e. TCC Automation Support Components.

(1) DSSCS Workstation. This project is to develop, test and deploy a stand-alone R/Y terminal capable of supporting DMS objectives. This project is based on the DIA sponsored Message Preparation and Dissemination Terminal.

(2) SARAH-Admin Enhanced Connectivity. This project is intended to facilitate the extension of automation for message preparation to the user and prepare for the elimination of the manual floppy disk transfer between the two versions of SARAH, thereby significantly improving speed of service and reducing staffing.

(3) AID with Selective Splitting (AID-SS). This project will develop, test and deploy an AUTODIN Interface Device (AID) with embedded

COMSEC and a splitting capability based on security level, RI, precedence and language media format.

(4) Personal Computer Message Terminal (PCMT) and Office Automation System (OAS) Components. These components will be located at user commands and will serve as generic/standard message entry/delivery components to allow transitioning services from TCCs to user commands/work stations.

f. Establish Testbeds. A major constraint on the DMS is funding. To ensure that the DoD gets the maximum value for its funding, the Services and agencies are to establish testbeds which will be used to operationally test DMS components prior to full-scale acquisition/deployment.

(1) R&D Testbed. A DCA lead joint R&D testbed capability is required to determine basic feasibility of DMS components planned for advanced DMS phases.

(2) Central Support Beta and OT&E Testbed. A DCA managed Central Support Testbed to perform Beta and OT&E testing will be established at the East Coast Telecommunications Center (ECTC) at Ft. Detrick, Maryland. This effort is an expansion of the current AUTODIN testing function which will use the on-line ASC/DDN capabilities.

(3) Army Beta and OT&E Testbeds. Army plans to establish testbeds at Ft. Ritchie, Maryland and Ft. Huachuca, Arizona. Both locations appear to be well suited for these test functions. Additional Beta testbeds are planned for Redstone Arsenel, AL; Ft Irwin, CA; and Ft Drum, NY.

(4) Navy Beta and OT&E Testbed. Navy plans to establish a testbed at Naval Communications Unit, Cheltenham, Maryland. This location is well suited for these test functions.

(5) Air Force Beta and OT&E Testbed. Air Force plans to establish a testbed at Mather AFB, California as an additional function of the existing Standard Command, Control, Communications and Computers (SC4) Model Base Program.

(6) DLA Beta and OT&E Testbed. DLA plans to establish a testbed at Gentile AFS, Ohio.

(7) DIA Beta and OT&E Testbed. DIA has no current plan to establish a Beta testbed. OT&E will be performed at contractor sites.

(8) NSA Beta and OT&E Testbed. NSA plans to use test facilities provided by support contract for the Telecommunications Improvement Program (TIP). The location of the NSA test facility has not been determined.

g. AUTODIN Switching Center (ASC) Evolution. DCA is responsible for actions required to maintain ASC viability. Many of the actions are normal maintenance/life cycle support, others will be taken to reduce costs.

Section 5

Phase II Implementation

5.0 Introduction.

Figure 5-1 illustrates the DMS Architecture at the end of Phase II (end FY 2000). The phase-in of new DMS X.400/X.500 based components with security protection provided by the Secure Data Network System (SDNS) during Phase II will begin the evolutionary phase-out of the baseline AUTODIN and E-Mail capabilities. At the regional level, the AUTODIN Switching Centers (ASCs) and Service/Agency Automated Message Processing Exchanges (AMPEs) will evolve to X.400 Message Transfer Agents (MTAs) and the directory improvements initiated in Phase I will be completed, providing a centrally managed X.500 integrated directory capability consisting of Directory System Agent (DSA) and Directory User Agent (DUA) implementations as shown in Figure 5-1. Architecturally, the ASC and E-Mail Directory components which were global components (GC) during the baseline and Phase I, are evolving to regional components (RC) with MTA and DSA functionality by the end of Phase II. The evolution to X.400 messaging is also occurring at the baselevel with the deployment of new installation components (IC), organizational components (OC) and user components (UC). Large bases may implement X.400 MTAs and X.500 DSA functions (which are normally implemented at the regional level) as ICs to provide these services at the installation level when required. Telecommunications Center (TCC) automation efforts initiated during Phase I continue during Phase II and evolve to X.400 based User Agent (UA), Organizational User Agent (OUA), Message Storage Agent (MSA), and Directory User Agent (DUA) functions which are deployed at the baselevel as organizational components (OC) and user components (UC). Initial implementations of Installation Information Transfer Systems (IITS) at the baselevel during Phase II will improve baselevel transmission capabilities and thereby facilitate this migration to X.400/X.500 based organizational and individual messaging with SDNS protection.

5.1 Phase II Objectives.

5.1.1 Consolidate Individual and Organizational Message Systems. During Phase I, actions have been taken to interface the baseline messaging systems, provide increased interoperability, reduce operations and maintenance costs, and begin the extension of the messaging interface to the users. The availability of X.400/X.500/SDNS DMS components during Phase II makes the provision of secure user-to-user individual and organizational messaging service possible. The speed at which these components are deployed during Phase II will depend not only on funding availability, but in large part on the aggressive continuation of the policy and procedural actions initiated during Phase I. As new OSI protocols, the Common Message Format, and new procedures are phased in, AUTODIN and DoD standard protocols, formats and procedures must be phased out.

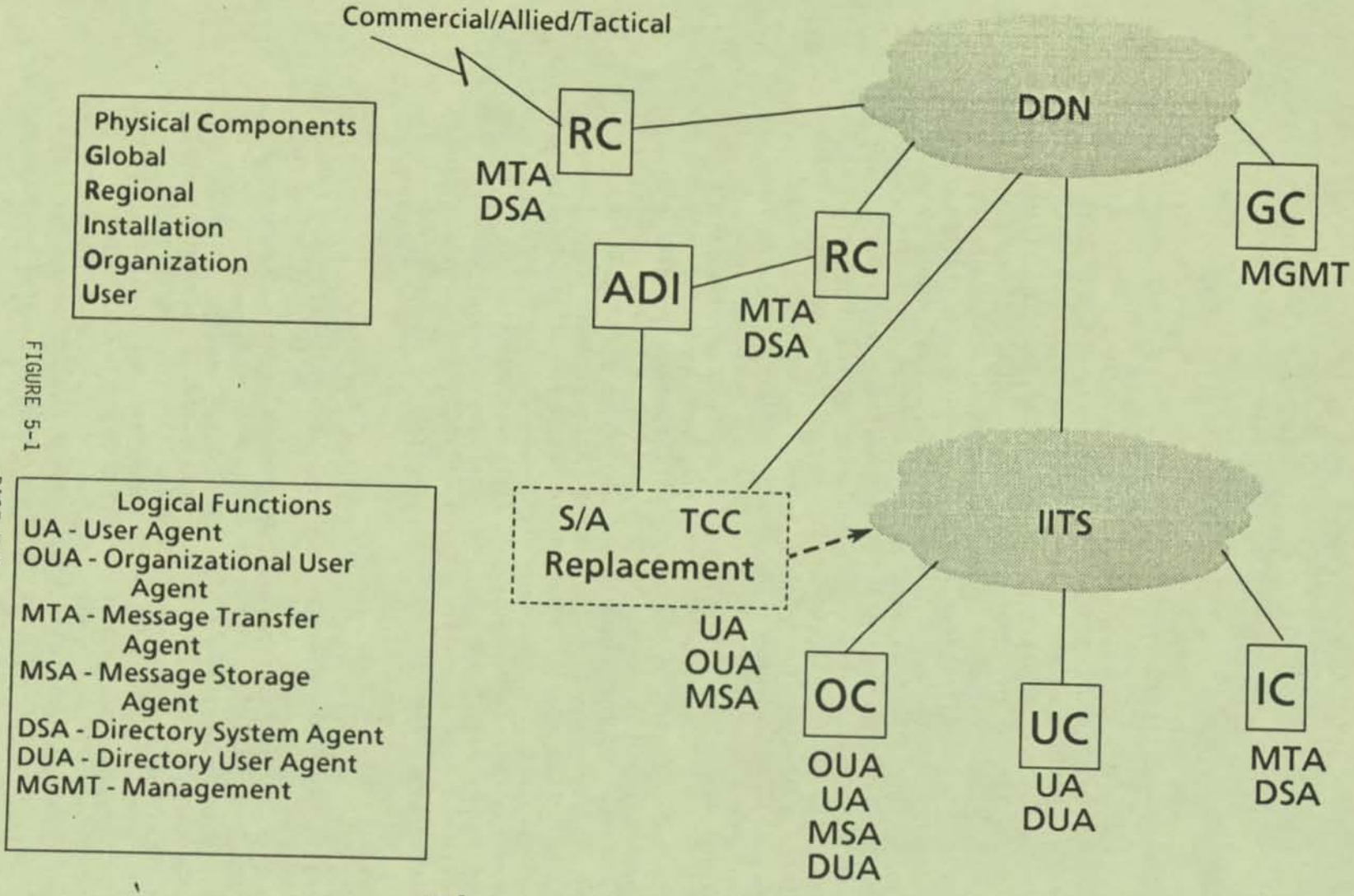


FIGURE 5-1

PAGE 5-2

Phase II Architecture 2000

5.1.2 Expand Writer-to-Reader Connectivity and Support. With deployment of new DMS components during this phase, extension of the messaging interface to the user will be complete. A user should have the ability to originate and receive both organizational and individual messages from the same terminal or workstation. While implementations of baselevel Installation Information Transfer Systems (IITS) are not DMS components, this improvement in the baselevel transmission capability, which allows transparent user access to all baselevel assets as well as access to long haul networks, will facilitate the effective interconnection of DMS components and provide the increased bandwidth that will be required for efficient X.400/X.500/SDNS messaging.

5.1.3 Provide Improved Writer-to-Reader Security. Assuming that BLACKER Host-to-Host protection is implemented during Phase I, the major security enhancement during Phase II will be deployment of Secure Data Network System (SDNS) security mechanisms designed to protect communications between "peer entities". SDNS is being designed specifically to provide security services within the Open Systems Interconnection (OSI) architecture which is a DMS objective. For the DMS, the primary "peer entities" to be protected are the User Agents (UAs and OUAs) and the protection is provided via end-to-end (i.e., User Agent-to-User Agent) encryption of each message's heading and text. Information exchanges between directory elements (e.g., DSAs, DUAs) will also require such protection. SDNS, which includes new and innovative cryptographic keying technology, provides six principal security services, all but one of which can be used by the DMS's X.400 MHS. All six services are outlined below.

a. Data Confidentiality. This security service protects data against unauthorized disclosure.

b. Traffic Flow Confidentiality. This is a special type of data confidentiality which protects the identities of communicating parties and the amount of communication between them. This service is not available for use by the X.400 DMS. To the extent that traffic flow protection is required, it must be met via other means (Also see 5.3.1 c.(2)).

c. Data Integrity. This service protects against unauthorized modification, insertion and deletion.

d. Authentication. This service verifies the identity of a communicating peer entity and the source of data.

e. Access Control. This service allows only authorized communication.

f. Non-repudiation With Proof of Origin. This service provides the recipient or disinterested third party proof of the origin of data and prevents the originator from denying that he sent the data or its contents.

5.2 Phase II Architecture.

5.2.1 Components. Phase II is also a transition phase. By the end of this phase (end FY 2000), the DMS consists of X.400/X.500 messaging components

and remaining baseline or Phase I transition components that are being phased out. The DMS has adopted the CCITT Recommendation X.400 Message Handling System (MHS) as the model for integrating DoD's messaging requirements into a single system. Initially there were concerns that the 1984 Recommendation did not meet military requirements and a NATO military extension was drafted. The 1988 Recommendation has incorporated many of the military requirements missing from the 1984 version. The MHS for the DMS will use an X.400 which fully meets the needs of the DoD and is interoperable with our strategic users, allies, and the tactical and commercial communities. To the extent that others have not evolved to X.400 MHS compatibility, they will be handled as exceptions on a case by case basis.

a. Global Components (GC). By the end of Phase II, it is expected that the AUTODIN Switching Centers will have evolved to regional Message Transfer Agents (MTAs) and the integrated X.500 Directory System Agent (DSA) function will be implemented regionally. Consequently, network management (MGMT) is the only function remaining that would require a GC(s). The primary MGMT functions performed at the global level will be directory management/maintenance, cryptographic key management, network status and performance monitoring, and network configuration control. A primary objective is to maximize automation of the MGMT functions to obtain maximum effectiveness and to ensure minimal expenditure of resources for this function. For example, a highly automated MHS addressing function that includes automatic delivery to alternate addresses in the event of primary addressee failures, could significantly improve speed of service while reducing the system control resources necessary to manage the alternate delivery function required for organizational messaging.

b. Regional Components (RC) and Installation Components (IC). Functions implemented as RCs and ICs during Phase II are the X.400 MTA and the X.500 DSA. Implementation of these functions on components is flexible. MTA and DSA functionality can be implemented in the same system or separately, depending on specific requirements to be satisfied. By the end of Phase II, it is envisioned that there will be a continuing need for the transitional ADI component deployed during Phase I at the regional and installation levels to provide AUTODIN/X.400 interoperability. The need for this ADI will remain until all baselevel TCCs have phased out and all allied, tactical, and commercial interoperability objectives have been met by other means.

(1) Message Transfer Agent (MTA). During this phase the Message Transfer System (MTS), the virtual store and forward messaging backbone, will be constituted with the fielding of RCs and ICs having the MTA functionality. The X.400 message consists of an envelope and its contents; the MTAs neither modify nor examine the content except for code conversion. With SDNS protection, the message content will be encrypted while being transferred within the MTS and since services have been moved out to the users, minimal staffing and minimal security protection and clearances should be required for DMS MTAs.

(2) Directory. Within the MHS, the MTAs must have, as a minimum, the originator/recipient (O/R) address to effect delivery of a message or notification. The function defined by the X.500 series of recommendations is the source of the O/R addresses. UAs, OUAs, and MTAs can, through use of a Directory User Agent (DUA) application, provide the DSA with the directory name of the intended recipient, and (subject to access control) obtain from the DSA, the recipient's O/R address. The UA may then supply both the directory name and the O/R address to the MTS. Another UA may supply just the recipient's directory name to the MTS. The MTS would then itself ask the DSA for the recipient's O/R address and add it to the envelope. The X.500 DSA function also plays a role in provision of SDNS protection through storage of public cryptographic key information for MHS users. Physical implementation of the DSA and DUA functions is flexible. It is envisioned that the DSA function will be implemented in regional and installation components and be collocated with the MTA function. The X.500 directory provides the following basic categories of service:

(a) User-Friendly Naming. The originator or recipient of a message can be identified by means of his user-friendly directory name, rather than his machine oriented O/R address. At any time, the MHS can obtain the O/R names/addresses of the individual recipients by providing the recipients' directory names to the directory.

(b) Distribution Lists (DLs). A group whose membership is stored in the directory can be used as a DL. The originator simply supplies the name of the list. At the DL's expansion point(s), the MHS can obtain the directory names (and then the O/R addresses) of the individual recipients by consulting the directory.

(c) Recipient UA Capabilities. The MHS capabilities of a recipient (or originator) can be stored in his directory entry. At any time, the MHS can obtain (and then act upon) those capabilities by consulting the directory.

(d) Authentication. Before two MHS functional entities (two MTAs or a UA and an MTA) communicate with one another, each establishes the identity of the other.

c. Organizational Components (OC). DMS OCs implemented during phase II will include those functions necessary for users to exchange organizational messages. As depicted in Figure 5-1, these functions include the Organizational User Agent (OUA), the User Agent (UA), the Message Storage Agent (MSA), and the Directory User Agent (DUA). These functions are also based on the X.400 Message Handling System model, with the OUA containing the most unique DMS functionality.

(1) Organizational User Agent (OUA). An X.400 User Agent (UA) is an application process that interacts with the Message Transfer System (MTS) or a Message Storage Agent (MSA) (defined below) to exchange messages on behalf of a single user. The MTS (i.e., cooperating MTAs) delivers the messages submitted by an originating UA, to one or more recipient UAs. The 1988 X.400 Recommendation states that "Functions performed solely by the UA

and not standardized as part of the message handling elements of service are called local functions." While appearing to the MHS as an X.400 UA, satisfaction of the unique DoD requirements associated with organizational messages requires the OUA to perform a series of these "local functions". The primary local functions unique to the OUA are: 1) approval of organizational messages prepared locally or by other subordinate UAs in the organization prior to transmission (i.e.," message release"); 2) automated distribution determination and delivery of received organizational messages to subordinate UAs in the organization; and 3) delivery of messages with high precedence or high classification received at any time day or night by any means available. It is important to note that not all OUAs will perform all of these functions. There will be numerous OUAs within a given organization that do not operate on a continuous (24 hours per day, 7 days per week) basis and are authorized to perform only the "message release" function. Selected OUAs (which may or may not operate on a continuous basis) will be designated to perform the distribution determination and delivery function but based on local requirements and hours of operation, they must also be capable of performing all OUA functions. OUAs resident in Command Posts or Duty Officer locations operated on a continuous basis, will perform as a minimum, the high precedence and high classification delivery function after normal duty hours but must also be capable of performing all OUA functions if required. Organizational messages may also be composed as well as "released" from an OUA. The OUA must also be capable of returning a message that cannot be released to the originating UA or forwarding the message to another OUA for release (e.g., for messages that must be released at a higher organizational level). "Release" of a message by an OUA will result in the addition of an SDNS signature block to the message which generates a cryptographic key for the signature block in addition to the key for the message. OUA functionality will typically be implemented on an intelligent terminal or workstation and all resident message data will normally be clear text. For each organization, at least one OUA will be operated on a continuous basis and be backed up (for alternate delivery purposes) by another continuously operated OUA. To enhance message addressing via the MHS, it is envisioned that each OUA's DUA will implement a limited cache of the DMS Directory containing the names and O/R Addresses commonly used by the organization. Maintenance of the cache would be accomplished interactively via the MHS between the OUA's DUA and the DSA without operator involvement. Since the O/R Addresses associated with collective names (AIGs, CADs, or other Distribution Lists) change frequently, their inclusion in the cache is not considered feasible. Consequently, transmission of each organizational message containing a collective or Distribution List (DL) name will require interaction between the OUA's DUA and the DSA for addition of the DL's O/R addresses to the X.400 envelope.

(2) User Agent (UA). From an organizational message exchange perspective, the UA is the application typically implemented on an intelligent terminal or workstation and operated by a user to create, edit, transmit and receive organizational messages. As previously indicated, a primary DMS objective is to allow a user to perform multiple applications from a single terminal or workstation. Consistent with this objective, the UA functionality will typically not be implemented on an organizational

component and is described here only to complete the discussion of organizational message exchange. Other office automation applications will typically be implemented on the same workstation, to include applications for preparation, transmission and reception of individual messages (see User Component below). For organizational messages, the user must be capable of, as a minimum: 1) composing a new message; 2) transmitting a composed draft message to other staff members (local or distant) for coordination via office automation techniques or via the MHS; 3) transmitting a coordinated draft message to the OUA via office automation techniques or via the MHS for message release and transmission; 4) receiving draft messages via office automation techniques or the MHS from the message drafter for staff coordination; 5) forwarding a draft message with comments via office automation techniques or via the MHS to the message drafter, another UA or an OUA; 6) receiving organizational messages from an OUA for user consumption, disposition, or as a comeback copy of a previously drafted message that was transmitted to an OUA for message release/transmission. Only this last capability results in an organizational message being resident in a UA because the message is not considered organizational until it has been approved for release by a competent authority. All draft organizational message transactions are considered "individual" messages from the DMS perspective. The feasibility of a DUA implementing a cache of commonly used organizational addresses on a UA is a matter for further study. It may be appropriate to only cache organizational "names" at the UA and allow the OUA that releases an organizational message to add the O/R addresses to the X.400 envelope prior to transmission.

(3) Message Storage Agent (MSA). The MSA is a general purpose capability of the X.400 MHS that acts as an intermediary between the UA (or OUA) and the MTA. The MSA is a functional entity whose primary purpose is to store and permit retrieval of delivered messages. The MSA also allows for submission from, and alerting to the UA. It is important to note that in the X.400 MHS model, the MSA is optional and is always implemented in series between a UA and an MTA. When subscribing to an MSA, all messages destined for the UA are delivered to the MSA only. The UA, if on-line, can receive alerts when certain messages (e.g., high precedence) are received by the MSA. Messages delivered to an MSA are considered delivered from the MTS perspective. When a UA transmits messages through an MSA, the MSA is transparent and operates in real-time. Like the UA, the MSA can be used for applications other than organizational message exchange. Both UAs and MSAs can be implemented on a wide variety of equipment, including intelligent terminals or workstations. For organizational messaging, the MSA could complement an OUA implemented on a terminal/workstation by providing a resident storage mechanism to take delivery of messages, provide short-term storage (normally provided by the MTS) and alerts for high precedence messages, and provide long-term storage of delivered messages for administrative, message accountability or analysis purposes. The MSA, in conjunction with resident or non-resident UA or OUA functionality, also appears to be a candidate for implementation of the functions performed by the current automated message handling systems (AMHSs). For most envisioned applications of the MSA functionality, message data resident on the MSA will be clear text. Current SDNS plans to encrypt message text from UA-to-UA, and the MSA placement currently specified in the X.400 Recommendation (i.e.,

in series between the MTA and UA) would appear to prohibit clear text message storage in the MSA. This is a matter for further study. No decisions have been made regarding the use of the MSA in the DMS. Clearly, message storage and retrieval are required functions; however, they need not be allocated to the X.400 MSA.

d. User Component (UC). The primary function implemented as a UC is the User Agent (UA). The UA function is an application process that interacts with the MTS on behalf of a single user. The UA has been described above from the organizational message perspective and the same UA can be used to send/receive individual messages. For the exchange of individual messages, an OUA is not involved, except as indicated above when the individual messages being exchanged are draft organizational messages and the OUA is the addressee. Since organizational requirements such as message release and distribution determination/delivery are not required, the UA interacts directly with the MTS to exchange individual messages with other UAs in a manner more closely fitting the X.400 MHS model. DUA implementation of a cache of commonly used individual addressees in the UA is envisioned with direct interaction with the DSA taking place as required to effect UA-to-UA message exchange via the MTS. As with organizational messages, the DUA cache would include the names of collective addresses or Distribution Lists but not the associated O/R Addresses. The MSA also has optional application for individual messaging in that it could provide individual short-term or long-term message storage service for multiple UAs. With this option, the MTS would not be required to store messages for periods of time while UAs are inoperable and UAs would be provided enhanced versions of the services currently provided by electronic mail and automated message handling system hosts.

e. DoD Internet. During Phase II, migration of the DoD Internet to an ISDN-based long-haul and baselevel transmission capability will begin. While the continuing upgrade and integration of the baselevel and network level transmission capabilities are independent of the DMS implementation, deployment of DMS X.400/X.500/SDNS components beginning in Phase II will rely heavily on these improved transmission capabilities for effective operation.

(1) Defense Data Network (DDN). With the phase-out of the AUTODIN Switching Centers during Phase II, the DDN will become the single DoD long-haul backbone for the DMS. While efforts to phase-out the baseline DDN in favor of an integrated ISDN-based Defense Communications System (DCS) backbone are expected to be underway, by the end of Phase II it is envisioned that the DDN will remain, either as an integrated network or as a continuation of the MILNET (unclassified) and DISNET (classified) segments. In the event the two interconnected DDN segments still exist, it is assumed that BLACKER or an equivalent capability will be widely implemented to allow DMS to view the DDN as a logically integrated long-haul backbone.

(2) Baselevel Installation Information Transfer Systems (IITS). As X.400/X.500/SDNS DMS components are implemented at the baselevel during Phase II, improved baselevel transmission connectivity will be needed to support the higher bandwidth required by these components. By the end of

Phase II, it is envisioned that baselevel telephone modernization projects will be well underway with the installation of ISDN-based IITS providing the increased transmission connectivity needed by the DMS as well as all other baselevel telecommunications assets.

f. Telecommunications Centers (TCCs). During Phase I, obsolete TCC equipment was replaced, TCC functionality was automated, and the messaging interface was extended to the user to the maximum extent possible. TCC equipment replacements and automation efforts emphasized the use of evolvable equipment, standard transportable operating systems, and implementation of international standard protocols to the maximum extent possible. If these objectives have been met, the TCC automation components implemented during Phase I can become the base for implementation of the Phase II X.400/X.500/SDNS components at the baselevel. By the end of Phase II, it is envisioned that many (if not most) of the TCCs will have been phased out in favor of X.400 organizational and user components.

g. Data Processing Installations (DPIs). By the end of Phase II, most, if not all, interactive data exchanges should be accomplished via the DoD Internet.

h. Automated Message Handling Systems (AMHSs). By the end of Phase II, many of the current AMHSs should have migrated to X.400 components (e.g., MSA with accompanying UA/OUA) to provide this functionality.

5.2.2 Connections. The connectivity of DMS components as of the end of Phase II is depicted in Figure 5-1. By the year 2000, the AUTODIN Switching Centers (ASCs) should have migrated to regional components (RC) implementing the X.400 MTA functionality with SDNS protection. The transitional DIR components implemented regionally during Phase I, should have migrated to regional components (RC) implementing X.500/SDNS DSA functionality. Some of the transitional ADI components implemented regionally during Phase I will remain until all baselevel TCCs have been phased out and the Allied, Tactical and Commercial Communities are able to directly interface the DMS regional and installation components implementing MTA and DSA functionality. The DDN continues to serve as the long-haul data switching backbone and the only remaining global components (GC) implement the DMS MGMT functions described above. At the baselevel, TCC phaseout continues as organizational and user components implement the X.400 UA, OUA, DUA, and optional MSA functions which are interconnected by new IITS capabilities. Depending on the Service or agency TCC automation project implemented during Phase I, a TCC that has not phased out by the end of Phase II may: interface directly with the DDN using a baselevel ADI transition component deployed during Phase I; interface with the regionally implemented ADI transition component; or both. To avoid prolonged use of these transition components, expedited phase-out of TCCs and satisfaction of Allied, Tactical, and Commercial interoperability requirements will be emphasized.

5.2.3 Concept of Operations. All messages exchanged via the DMS will be categorized as either "organizational" or "individual" and a message recipient must be able to clearly identify the category of each message. A number of policy and procedural issues must be resolved regarding this

categorization but for purposes of this concept of operations, a message originated as "individual" will not be addressed or delivered to an organizational address and a message originated as "organizational" will not be addressed or delivered to an individual address. Following are potential scenarios envisioned for the exchange of organizational and individual messages by the end of Phase II:

a. Organizational Message Exchange. Assuming that the user is logged onto his UA (e.g., workstation) and desires to draft an organizational message, he will indicate this choice to his UA. The UA will prompt the user for the information required for preparation of the organizational message in the Common Message Format and provide help menus as required for completion of the draft message. Information required from the user for message preparation should include only the basics such as: originating organizational name (FROM:); action organizational names (TO:); information organizational names (INFO: or CC:); message precedence; message classification (to include Caveats, Codewords, etc., if appropriate); message passing/handling instructions, if appropriate; and the message text (subject of the message is considered part of the message text for this description). The user must know the names of the intended addressees. If necessary, the user can obtain organizational name information from the DUA cache implemented on his IC/OC or initiate a directory query to the X.500 DSA implemented at the regional level. If the completed draft organizational message requires staffing/coordination prior to transmission to the appropriate OUA for release, additional information to support the coordination process (e.g., a supporting memorandum for record) may be appended to the draft. The staffing/coordination process will be accomplished electrically using office automation capabilities for coordination with local staff members or via the MHS for coordination with distant staff members. Messages exchanged between the drafter, local and distant staff members associated with the coordination of the draft organizational message (to include copies of the draft, comments to the draft, etc.) are considered "individual" messages from the DMS perspective. When the staffing/coordination process is complete, the draft organizational message is transmitted to the appropriate OUA for review and release. The release authority reviews the message on his OUA and takes one of the following actions: 1) modifies the message prior to release; 2) returns the message to the drafter for rework; 3) forwards the message to another OUA for release; or, 4) releases the message for transmission. Until the message has been released for transmission at an OUA, the message remains a draft and is considered an individual message. If the draft organizational message or any of the individual messages generated during the staffing/coordination process contain sensitive or classified information, this information will be afforded the appropriate protection. With SDNS protection, the text of these messages will have been encrypted from UA-to-UA or UA-to-OUA. When the message has been released, it is now an organizational message and strict message accountability information is recorded from the point of release to ultimate delivery to all addressees. Again assuming SDNS protection, the OUA encrypts the text of the message, adds an SDNS signature block, and transmits it to an MTA, thereby entering it into the MTS. Message accountability information is recorded by the originating OUA and by the MTS. The MTS, interacting with the DSA as

necessary for addressing and keying purposes, transfers the message to the destination OUA(s). Upon receipt by a destination OUA, the message text is decrypted and the message is processed for distribution determination and delivery purposes. The message text is again encrypted by the OUA and transmitted to each of the recipient UAs. It is important to note that for organizational messages, the message is delivered by the destination OUA to the organizational elements addressed by the originator and, based on distribution determination processing, to additional subordinate organizational elements (e.g., divisions, branches, offices) determined appropriate by the recipient organization. Message accountability information regarding this message is recorded by the destination OUA beginning with receipt from the MTS and ending with delivery to the last UA. Upon receipt of the organizational message by each UA, the message text is decrypted and made available to the destination user who may, through office automation capabilities, read, print, store, or otherwise manipulate the message. Message accountability information recording outlined in this scenario is the minimum required for organizational messages and refers to the recording of message transactions only (i.e., it does not refer to recording of complete messages). The capability for all DMS components to maintain this recorded information for a period of time (e.g., 30 days) to support problem analysis, statistics collection and tracer actions is required. With regard to requirements for storing complete copies of organizational messages, the following applies: within the MTS, complete messages are stored only until delivery has been effected to all OUAs. Long term storage (e.g., 30 days or more) of organizational messages at the OUA to support retrievals, retransmissions, tracers, and other applications, will be typical. As indicated in the component descriptions, the X.400 Message Storage Agent (MSA) functionality has potential application in this scenario depending upon its placement with regard to SDNS protection.

b. Individual Message Exchange. Assuming the user is logged onto his UA (and this can be the same UA used for organizational messaging), and desires to prepare and transmit an individual message, he will indicate this choice to his UA. The UA will prompt the user for the information required for preparation of the individual message in the Common Message Format and provide help menus as required for completion of the message. Information required from the user for individual message preparation should include only the basics such as: originating user's directory name (FROM:); action users' directory names (TO:); information users' directory names (INFO: or CC:); message classification; subject and text. (While a precedence requirement has not currently been stated for individual messages, such a requirement is a distinct possibility during the Phase II time frame as well as other improvements (e.g., improved message accountability) over the current E-mail method of providing individual messaging.) The user must know the directory names of the intended users. If necessary, the user can obtain user directory name information from the DUA cache implemented on his his IC/OC or initiate a directory query to the X.500 DSA implemented at the regional level. For individual messages, the user is the releaser and simply indicates to his UA when the message is to be transmitted. Assuming SDNS protection, the UA encrypts the text of the message, adds the O/R addresses (from the DUA cache) to the X.400 envelope, and transmits it to an MTA. Individual messages do not include an SDNS signature block. The MTS,

interacting with the DSA as necessary for addressing and keying purposes, transfers the message to the destination UAs. Upon receipt by a destination UA, the message text is decrypted and made available to the destination user who may, through office automation capabilities, read, print, store, or otherwise manipulate the message. Given that UAs are typically not operational on a continuous basis, the question concerning where individual messages destined for inoperable UAs will be stored is germane. For organizational messages, the OUA (with or without MSA functionality) has this responsibility. One candidate would be the MTS providing temporary storage of individual messages awaiting delivery to inoperable UAs. The X.400 MSA functionality (either collocated with the UA or implemented as a separate storage service for multiple UAs) would be an ideal candidate to provide this temporary storage capability as well as long-term storage of delivered individual messages for subsequent review and manipulation by the user. While the MSA seems to be the better candidate since it places the management of temporary message storage (e.g., queues or mailboxes) closer to the user and also provides the long-term storage capability, the use of the MSA functionality as currently defined in the X.400 Recommendation with SDNS protection is a problem requiring resolution.

5.2.4 Cost. Specific cost estimates for Phase II are not currently possible but economic benefits are anticipated in two major areas. First, DMS component acquisitions that are based on international standards versus DoD standards and maximize the use of NDI, commodity contracts, and products endorsed by the CCEP will be significantly more cost effective than the traditional DoD development acquisitions. Second, through deployment of Phase II DMS components, the messaging interface will be extended to the user at many more DoD locations, thereby allowing the additional communications staff reductions outlined in the next paragraph.

5.2.5 Staffing. The Phase II migration from discrete organizational and individual message systems to an integrated DMS will result in the reduction of staff dedicated to communications functions. UAs will be operated by users. OUAs performing only the message release function will be staffed by users having message release authority. OUAs performing the distribution determination and delivery functions can be operated by existing organizational administrative support personnel rather than dedicated TCC operators. OUAs performing functions requiring continuous operation can be located in Command Center or Duty Officer locations that are already staffed on a continuous basis. The optional MSA function can be collocated with other components and is not expected to require significant staffing. DMS components implementing the MTS and Directory functions are expected to require minimal staffing. The global MGMT function will require staffing to perform system control, data base management/maintenance, and key management functions but maximum automation of these functions will minimize the level of staffing required.

5.2.6 Comparison to Requirements.

a. Connectivity/Interoperability. Components and logical functions based on the X.400 MHS model implemented during Phase II provide significant improvements in flexibility and interoperability between users. The

ultimate DMS objective of providing connectivity from writer-to-reader is becoming a reality by the end of Phase II. Although there are a number of serious integration and security policy issues associated with Allied interoperability, during Phase II specific emphasis will be placed on resolving these problems and achieving full interoperability with our Allies.

b. Guaranteed Delivery. Significant improvement in satisfaction of this requirement will be realized with deployment of X.400 based DMS components during Phase II. The most notable improvement in this area will be for individual messaging as users derive the benefits from consolidation of the organizational and individual message systems. The MTS will maintain message accountability during all message transfers from UA/OUA-to-UA/OUA. Automatic notification to an originating UA that a recipient user has read the message can also be provided. Where guaranteed delivery is most critical (e.g., for organizational messages), additional measures such as duplicate data files, redundant data storage devices, etc., will be implemented by OUAs and/or MSAs to preclude the loss of messages during system failures.

c. Timely Delivery. With the extension of the messaging interface to the user during Phase II, there will be significant improvement in the satisfaction of this requirement. The most notable improvement in this area will be for organizational messaging since the manual handling of paper media will be phasing out. Deployment of X.400 based DMS components at the baselevel (UA, OUA, MSA) will allow the DMS to honor the users' desires with regard to timely delivery. An urgent organizational message can be delivered immediately to a user by the OUA or be expeditiously reviewed and passed to appropriate personnel for action in the event that the user's UA is inoperable. For individual messages, the MSA's alerting capability can be used to alert a user to receipt of an urgent or high interest individual message. For routine organizational or individual messages, the users will be capable of specifying timely delivery requirements (i.e., how often the UA will alert the user to message receipt and make received messages available for consumption) based on varying message criteria (e.g., precedence, subject matter, etc.).

d. Confidentiality/Security. All messages will be afforded protection appropriate to the sensitivity or classification of the information. During Phase II, the primary improvement in this area will be the deployment of DMS components providing SDNS protection. Applicability of SDNS to specific user communities is a matter for further study as is the interoperability between SDNS protected users and users who are either not yet SDNS protected or never will be. While a number of security policy issues remain to be resolved, in general, confidentiality and security will be provided throughout the DMS by limiting recipients to those cleared for the information through the use of the security measures in place, new security measures provided by SDNS, and multilevel security (MLS) protection as required. Security procedures appropriate for the level of classification will be required for message preparation, transmission, receipt, and consumption by users. Trusted Computing Base (TCB) technology will be used as required depending upon the application and the security environment.

Some of the security protections will still be provided by procedures and personnel security, but with the extension of the messaging interface to the user level, these procedures and personnel security clearances will apply to message writers and readers. A major objective will be to minimize the security clearance levels required throughout the DMS.

e. Sender Authentication. Deployment of X.400/X.500/SDNS components during Phase II will offer significant improvements in satisfaction of this requirement. While the X.400/X.500 method of messaging in and of itself provides improvements in sender authentication, those users protected by SDNS will have available the additional features of cryptographic electronic signature authentication and non-repudiation with proof of origin. Use of these features will be dependent upon the type of message and the user's specific requirements.

f. Integrity. Improvements being implemented in the DoD Internet during this phase, coupled with deployment of new DMS components, will collectively result in improved message integrity. Migration to newer protocols using cyclic redundancy checks vice the simple parity checks offered by some of the DoD standard protocols (such as DCS Mode I) in use during the baseline and Phase I time frames, will provide improved error detection and correction capabilities.

g. Survivability. Survivability of DMS components will increase during this phase as the AUTODIN Switching Centers are phased out and highly distributed and richly connected regional and installation components with MTA/DSA functionality are phased in. Further, with improvements to the DoD Internet being implemented during this time frame, both local and regional connectivity of DMS components will begin to improve.

h. Availability/Reliability. New or upgraded DMS components are expected to have little downtime and to be supported by inexpensive, highly reliable power and environmental support facilities. Those components requiring high availability (e.g., MTAs, DSAs, OUAs) will be either redundant or backed-up.

i. Ease of Use. The emergence of a simplified, X.400 based Common Message Format (ACP-XXX) will allow users to interact directly with the DMS. Specialized communications skills will not be required. UA interaction with the MHS, to include the directory and key management functions, will be for the most part, transparent to the user.

j. Identification of Recipients. Directory service improvements initiated during Phase I will mature during Phase II with deployment of the fully integrated X.500 DSA/DUA capabilities.

k. Preparation Support. The UA will provide the prompting and message formatting necessary for the user to easily prepare a message with no special training. During Phase II, this function will be fully integrated into the office automation environment as UAs are deployed.

l. Storage and Retrieval Support. The optional X.400 Message Storage Agent (MSA) functionality will provide a highly flexible message storage capability that can be used for multiple applications. Full utilization of this capability with SDNS protection is an issue requiring resolution.

m. Distribution Determination and Delivery. This function, which applies primarily to organizational messages, will be an automated capability of the OUA. Distribution profiles, reflecting the organizational users' distribution requirements, will be implemented on the OUA and be maintained by the local organization. Message distribution will normally be accomplished electronically by transmission from the OUA to the organizational users' UAs, with abnormal conditions (high precedence, high classification, UA inoperable) being handled by the OUA through alternate delivery, or review and delivery by other means. The MSA role in this process is a matter for further study.

5.3 Phase II Actions.

Specific actions will be taken during Phase II to deploy X.400/X.500 DMS components with SDNS protection. The successful completion of policy, procedural and component actions taken during Phase I is a prerequisite to accomplishment of the Phase II actions.

5.3.1 Policy Actions.

a. Overall DMS Policy. ASD/C3I will continue DMS oversight established during Phase I and maintain the overall DMS policy. Maintenance of the DMS Component Development Policy established during Phase I will continue during Phase II to ensure that DMS objectives are met. ASD/C3I will interface with the Defense Acquisition Board for resolution of major DMS acquisition issues.

b. JCS Policy. The Joint Staff will continue to update/formulate policy affecting joint issues and validate DMS requirements. Consolidation of the individual and organizational message systems of the baseline into an integrated DMS requires modification of multiple JCS Memorandums of Policy. The MOP modification process began during Phase I and will continue during Phase II. By the end of Phase II, the AUTODIN Switching Centers should be phased out, thereby obviating the need for JCS MOP 165. The need for an additional MOP to address the consolidated DMS must be investigated during Phase I and if needed, validated early in Phase II. It is envisioned that a DMS MOP (or modifications to existing MOPs) will be required to address operational direction and management control responsibility changes required as the result of the architectural changes occurring during the DMS implementation.

c. DMS Security Policy. The need for security policies associated with the deployment of SDNS surfaces early in Phase II. Consequently, the following issues must be worked during Phase I with their resolutions established as policy by early Phase II:

(1) SDNS Applicability. User communities that will use SDNS protection must be identified and prioritized. This will require determination of the message categories (organizational, individual) and message sensitivity/classification levels (all DoD unclassified, only "sensitive" DoD unclassified, all unclassified, all classified) requiring SDNS protection. Further, given that full interoperability with Allies is a Phase II objective, technical solutions to the policy constraint regarding the non-release of the SDNS key distribution mechanism must be sought (see paragraph 5.3.3c, Allied Interoperability).

(2) Lack of SDNS Traffic Flow Control Confidentiality. Consistent with the DMS Phase II objective of minimizing the security protection and personnel clearance levels required for regional or installation level DMS components implementing MTA functionality, the classification of information contained in the X.400 envelope (which will reside in the MTA as clear text) is a concern from a traffic flow confidentiality perspective. Consequently, in conjunction with Phase I procedural actions, such as formulation of the X.400 Common Message Format (CMF) where the mapping of existing formats to the X.400 envelope will be defined, the X.400 envelope information content must be reviewed carefully and its classification determined. The resulting security policy will have a significant bearing on the CMF formulation by specifying which information can be mapped to the X.400 envelope and which information must remain in the SDNS encrypted message content (heading and text). This policy will also have a significant bearing on the functionality of the MTS during Phase II since it will determine what clear text information is available for an MTA to perform functions other than pure message transfer (such as temporary storage).

(3) Directory Security Requirements. Minimizing security protection and personnel security clearance requirements for regional/installation level DMS components implementing the DSA functionality is also an objective. As directory contents and interactions are specified during Phase I, security classification and protection requirements must be defined as part of the security policy. With Phase II implementation of the fully integrated X.500 Directory System, this policy must be reevaluated, particularly in light of the Directory System's role in SDNS keying.

(4) Multilevel Security (MLS) Certification Requirements for Accreditation of DMS Components with SDNS Protection. For those DMS components implementing SDNS protection but processing messages in clear text (UA and OUA), accreditation policy must be developed regarding MLS certification requirements for these components in various security environments.

(5) SDNS Protected Message Storage Agent (MSA). As already indicated, the current description of the X.400 MSA as an application in series between an MTA and UA would result in all message text resident on the MSA being encrypted when SDNS protection is applicable. Such a situation severely limits the functionality of the MSA from a DMS perspective. Resolution of this problem, allowing messages resident on the

MSA to be clear text will require the coordinated efforts of personnel formulating the X.400 MHS Recommendation and personnel involved in the SDNS Program. The resulting security policy will have to address MLS certification requirements for accreditation of an MSA with clear text resident messages.

5.3.2 Procedural Actions. The MCEB will continue to lead development and implementation of procedures required for the DMS implementation. The significant number of procedural actions initiated during Phase I must be completed if the Phase II architecture is to be achieved. For example, the ACP XXX CMF must be available to support X.400/X.500 Phase II DMS component deployments. The following additional procedural actions will be required to support Phase II:

a. X.400 Precedence. Procedures will be required to support the use of precedence via the DMS as defined by the X.400 Recommendation. In the event that the X.400 precedence scheme differs from the current scheme, backward compatibility must be addressed from a messaging policy standpoint. ACP XXX modifications may also be required to support X.400.

b. SDNS Procedures. While SDNS protection will be largely transparent to the user, procedures will be required to address such areas as: use of the non-repudiation with proof of origin feature and handling of abnormal conditions.

c. DMS Test Procedures. Procedures developed during Phase I to implement the DMS test strategy will be refined as the DMS Implementation progresses to ensure optimum use of such strategies as BETA testing. R&D concepts and test procedures developed during Phase I will address (during Phase I) many of the Phase II policy, procedural and component problems outlined in this document to ensure their resolution prior to the Phase II Implementation period.

d. X.400/X.500 Messaging Procedures. Deployment of Phase II X.400/X.500 DMS regional, installation, organizational, and user components will require a significant number of new procedures to be developed. Development of these procedures will be an integral part of each DMS project or component development and the MCEB will be the forum for approval of joint procedures.

5.3.3 Component Actions. These actions will be the acquisition, testing, and deployment of the Phase II Global (MGMT), Regional/Installation (MTA/DSA) and Organizational/User (UA/OUA/MSA/DUA) components. These actions are directly related to and dependent upon the Phase II policy and procedural actions outlined above (most of which must be completed during Phase I). As the DMS progresses and these actions are definitized, Phase II component action documentation will be updated. Following are additional problems envisioned with the Phase II deployment of X.400/X.500 DMS components using SDNS protection that must be resolved early in the SDNS Program; i.e., during the DMS Phase I time frame.

a. SDNS Transition. Consistent with the "SDNS Applicability" security

policy action outlined above, SDNS must address interoperability between users who have implemented SDNS protection and those who have not (or never will). The use of gateways is an obvious choice but a number of associated security certification and accreditation issues require identification and resolution. Such issues must be worked during Phase I to ensure that SDNS protection can be effectively implemented during Phase II.

b. Collectively Addressed Messages with SDNS Protection. Submission and delivery of messages addressed to collective addresses (e.g., Address Indicator Groups, Collective Address Designators) appears to be well supported by the Distribution List (DL) and DL Expansion functions documented in the 1988 X.400 Recommendation. Submission and delivery of such messages assuming SDNS protection when the members of a DL can number 1,000 or more, raises questions concerning the SDNS keying technique to be used for this application. Further, during the SDNS implementation, the technique must address both submission and delivery of messages to DLs when not all parties involved (originator and DL members) are SDNS protected. This is another technical issue that must be resolved early in the SDNS Program.

c. Allied Interoperability. Consistent with the policy of not releasing the key-distribution mechanism used in SDNS to our Allies and the Phase II objective of Allied interoperability, a cooperative effort between NSA's Information Security Directorate and DCA must be established. This cooperative effort will examine the interoperability issues surrounding and propose solutions to allow communications between the US with SDNS key-distribution mechanisms and Allies with different key-distribution mechanisms.

Section 6

Phase III Implementation

6.0 Introduction.

Figure 6-1 illustrates the Target DMS Architecture, achieved at the end of Phase III (end FY 2008). This phase, based on 1988 knowledge and technology, appears to be somewhat anticlimactic; i.e., finish-up actions underway and improve on local and long haul transmission. However, given the pace of change in telecommunications technologies, by 2001 (the first year of Phase III), the DMS Target Architecture will undoubtedly be changed. The major thrust of the DMS is change (change in policies, procedures, formats, protocols, hardware, operating systems, applications software, etc.) toward standardization and interoperability. By the year 2000, the plans for Phase III will have iterated several times. The challenge for the DMS is adapting the DMS to take full advantage of these changes. The 1988 vision of Phase III is to complete the evolution of users to X.400 messaging and to take full advantage of advances in local and long haul communications by migrating to the Integrated Services Digital Network (ISDN). The DMS of 2008 will have powerful workstations at the user level using the X.400 MHS to send and receive both individual and organizational messages which are encrypted on a writer-to-reader basis.

6.1 Phase III Objectives.

6.1.1 Backbone Upgrade. During this phase, the long haul portion of the DoD Internet, the DDN, will be replaced by an ISDN-based Defense Communications System (DCS). The DCS by 2008 will be an integrated set of common-user services designed to provide custom tailored communications capabilities to users (voice, data, facsimile, video, etc.).

6.1.2 Installation Upgrade. At the baselevel, the 4kHz analog voice systems of the baseline will be replaced by large bandwidth Installation Information Transfer Systems (IITS). This phase will see the completion of modernization efforts initiated during Phase I. The IITS will be an ISDN-based capability fully interoperable with the ISDN-based DCS.

6.1.3 Project/Component Completion. During this phase, any action previously initiated will be completed. Some policy and procedural actions previously completed may need to be reviewed as the result of advances in technology.

6.2 Phase III (Target) Architecture.

6.2.1 Components. Initial fielding of X.400 messaging functions and X.500 directory functions with SDNS end-to-end encryption as DMS components were accomplished during Phase II. Use of ISDN-based communications initiated in

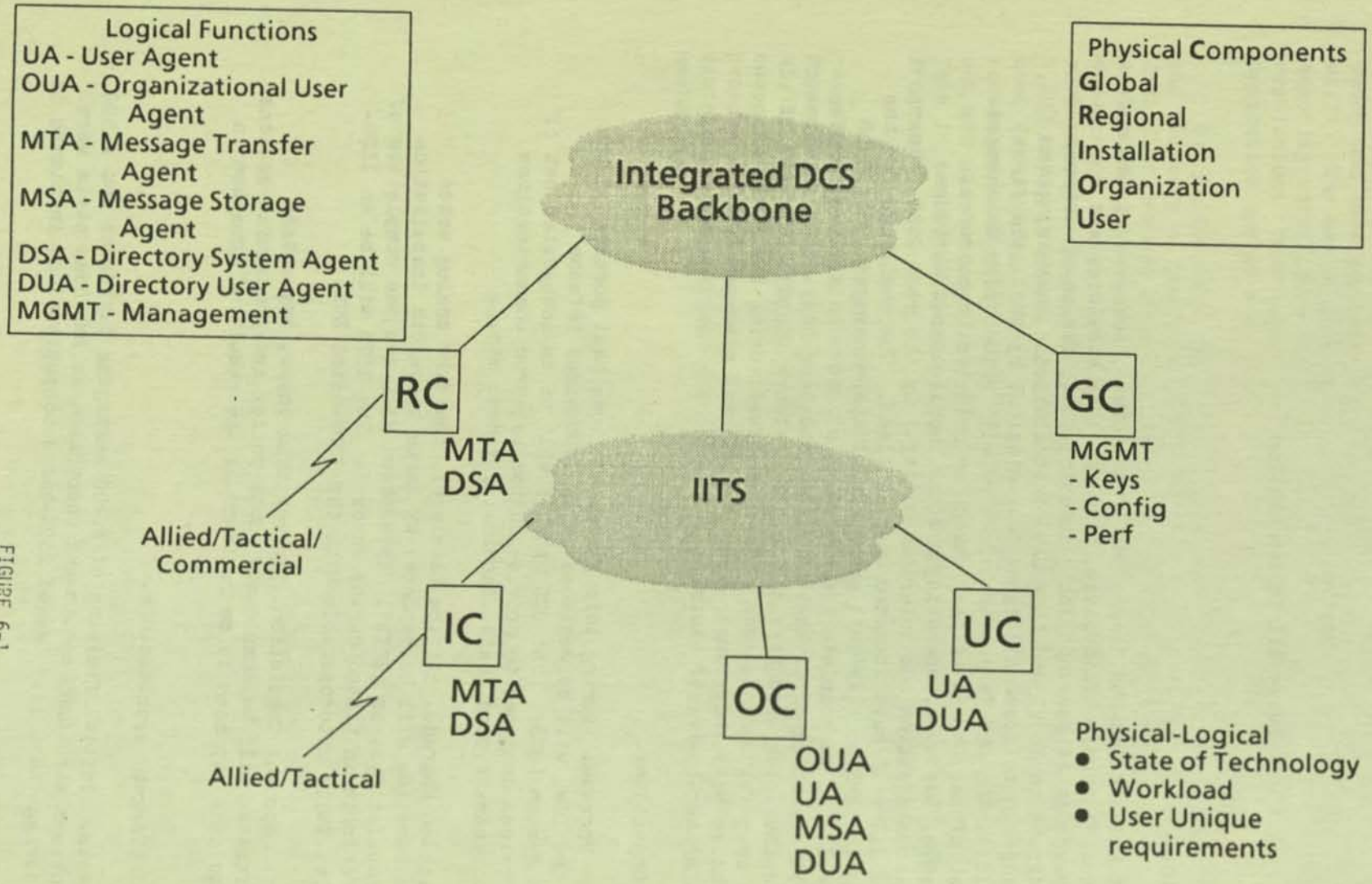


FIGURE 6-1
PAGE 6-2

Target Architecture 2008

Phase II, will be widely implemented in Phase III. No new DMS components are currently planned. However, advances in technology may result in new components for either new service(s) or further savings.

a. Global Component (GC). The GC is the MGMT of Phase II.

b. Regional Component (RC)/Installation Component (IC). The RCs/ICs are the MTA and DSA of Phase II.

c. Organizational Component (OC). The OCs are the OUA, UA, MSA, and DUA of Phase II.

d. User Component (UC). The UCs are the Phase II workstation UAs and DUAs of Phase II.

e. Integrated Defense Communications System (IDCS). The Target DMS will use an Integrated Services Digital Network (ISDN) based DCS for its backbone. The IDCS is not a DMS component per se, but is included for completeness. The IDCS backbone provides long haul interconnection for the DMS components.

f. Installation Information Transfer Service (IITS). This also is not a DMS component per se, but is included for completeness. The IITS provides the local interconnection of DMS components. Like the DCS, the IITS is an ISDN based facility ensuring excellent interoperability with the backbone.

6.2.2 Connections. The target architecture allows for total connectivity and interoperability from a network standpoint by using the ISDN standards and also by using a standard set of services as offered by the ISDN. These standards and services are to be provided and used at the local level as well as at the "higher" network level. This connectivity and interoperation is, of course, subject to the security and policy requirements of the DoD and the individual organizations.

6.2.3 Concept of Operations. The user will perceive little change during the course of Phase III (2001-2008), except for those users finally obtaining local service via IITS. The major thrust for Phase III will be achieving an ISDN-based IDCS. Other efforts are the deployment of IITS and the completion of other actions initiated prior to the start of Phase III. The concept of operations during Phase III is based on CCITT X.400 messaging. The Phase II concept of operations, Section 5, paragraph 5.2.3 captures the essentials. With the achievement of the Target DMS, all of the policy and procedural actions will be completed. Any operational difficulties surfaced in X.400 messaging will have been resolved. A typical writer-to-reader message flow by 2008 would have the user, originator of the message, log onto a workstation to prepare a message. The User Agent (UA) will prompt the user for the required information. If the user needs help in understanding the prompts, there will be help menus available for each step of message preparation. The user must obtain message recipient(s) addressing information either from the DUA cache or the X.500 DSA and supply it to the MTS via their UA. The message preparation capability and the DMS messaging interfaces will be integral parts of the office automation package

on the workstation. If the message must be staffed, it will be electronically staffed, again using office automation capabilities. When the message, if organizational, is ready to be released, the OUA performs this function and it is transmitted to the addresses on the message via the MTS. SDNS protection is transparent to the users and the message content is encrypted end to end. When the message is delivered to the recipient (by the OUA, if organizational), it is decrypted for presentation. The message is handled by the office automation facilities available to the recipient while being read, stored, or otherwise manipulated. Many abnormal conditions may arise that must be handled, therefore, much effort will be taken to assure that all user requirements are met in each situation.

6.2.4 Cost. Specific cost estimates for Phase III are not currently possible, but economic benefits are anticipated from the adoption of ISDN based communications and services. The operating and maintenance (O&M) costs associated directly with the DMS should be significantly reduced. Large numbers of professional communicators currently required in AUTODIN will no longer be required. All of the high maintenance items of the baseline will have been replaced by state of the art hardware featuring large scale integration and repair by replacement.

6.2.5 Staffing. The staffing reductions begun in earlier phases will be completed in this phase. Almost all residual communications functions will be performed by user personnel. With very few exceptions, the components will be located with the users versus the AUTODIN model of separate stand-alone communications facilities. In addition, the high degree of automation and the extension of automation to the user's workplace further minimize the need for personnel dedicated to communications and associated administrative handling of paper messages.

6.2.6 Comparison to Requirements. With the completion of Phase III, i.e., the achieving of the Target Architecture, all MROC requirements are fully satisfied.

a. Connectivity/Interoperability. The universal use of the ISDN standards make the DMS truly a single open system. Any user can communicate with any other user provided that the security and access aspects of the system have been met since all users will use the same standards.

b. Guaranteed Delivery. The source Message Transfer Agent (MTA) keeps outgoing messages until it has confirmation from all destination MTAs that all deliveries have completed normally. While the MTA can maintain journaling information to support problem analysis and billing, in general, messages will be stored only once at the source and destination. Consequently, there are times when a failure can cause the loss of a message, e.g., between backups and before transmission (source) or delivery (destination). In instances where this is not acceptable (such as at the OUA), extraordinary measures will be taken to preclude the loss of a message. These measures may include duplicate data files on different data devices. The message protocol also includes the provision for automatic sender notification when the receiver reads the message.

c. Timely Delivery. In the X.400 messaging world of 2008, the MTA will be primarily responsible for ensuring timely delivery. The MTAs (unlike the diverse E-Mail hosts of 1988) will be designed to work closely together to facilitate the rapid transfer of messages and to honor user desires with regard to timely delivery of messages. For organizational traffic, when the user's UA is unavailable, a full-period OUA can ensure that received traffic is expeditiously reviewed and passed to appropriate individuals when required, based on the urgency of the message.

d. Confidentiality/Security. Confidentiality is provided throughout the DMS by limiting recipients to those cleared for the information through the use of the security measures in place as a result of the SDNS which provides end-to-end encryption (E3), and multilevel security (MLS) protection, as required. There will be procedural measures appropriate for the level of classification that must be followed at the user level as the messages are prepared or read. Trusted computer systems will be used as appropriate depending upon the application and the environment. Terminals are classmarked with the security levels they are allowed to process. Messages from terminals are checked for valid security levels prior to acceptance and before delivery. Some of the security must still be provided by procedures and by personnel security even though much of the burden has been removed by the SDNS security architecture and by using trusted computing base technology.

e. Sender Authentication. Sender authentication will be provided by the features of the X.400 message protocol with its SDNS security architecture.

f. Integrity. Protocols provide excellent data or message integrity between the sending and receiving devices. Cyclic redundancy checks are provided and end-to-end checksums are used in the protocols. These protocols will be used not only in the backbone, but also on the IITS to preserve the data integrity at the local level as well.

g. Survivability. The DMS uses the DCS for the backbone carrier and international standard protocols that allow for use of commercial carriers as well as government networks. This allows a great deal of network reconstitution to add additional survivability. The potential bottlenecks such as directories will be duplicated within regions or areas based upon requirements.

h. Availability/Reliability. As a matter of policy, selected MTAs, MSAs and OUAs will be available 24 hours per day; backup in the form of redundancy or alternative facilities will ensure an absolute minimum of downtime. ISDN technology allows for dynamic reconfiguration of the network which greatly enhances the availability/reliability of the DMS.

i. Ease of Use. Users will be using their own office automation capabilities and are therefore assumed to be familiar with the procedures involved. Should the user need assistance in preparing or handling a message, automated help will be available for each step or procedure in use.

j. Identification of Recipients. The X.500 directory service, fully implemented during this phase, will ensure that users at all levels will be able to correctly identify to the DMS the intended recipient(s) for every message whether individual or organizational. The computing power of the workstations used for UAs and OUAs will allow for DUA caching of addresses most often used. Transparent to the user, the workstations should interact with the directory system (DSA/DUA) for correct addressing and dynamic updating of the cache. Sending collectively addressed messages requires a DSA call to ensure proper addressing but this should also be performed in a manner transparent to the user.

k. Preparation Support. The DMS users will have access via office automation workstations which will have appropriate message preparation capabilities and electrical DMS access via their IITS.

l. Storage and Retrieval Support. The Target Architecture includes Message Storage Agents (MSAs). The MSAs will provide the capability to hold messages on-line for some time period (e.g., 30 days) to allow for timely retrieval by the users at their workstations. MSAs can also provide message analysis and editing functions similar to the current Automated Message Handling System (AMHS).

m. Distribution Determination and Delivery. Actual message distribution determination will be accomplished by the OUA in accordance with the installation or organization policy. This is accomplished by use of a series of distribution profiles. Except in rare or emergency situations, all message deliveries will be accomplished electronically. Urgent messages will be delivered as determined unless there is no response at the destination workstation in which case, the message will be delivered to the staff duty officer for action in accordance with local policy.

6.3 Phase III Actions.

The IDCS backbone will become a totally implemented ISDN that provides an easy connection to the IITS that are also ISDN-based. There will be a full implementation of the IITS during this phase of the architecture.

6.3.1 Policy.

Policy issues will continue to be worked during this phase. Perhaps the most pressing policy issues will deal with the amount of freedom users at the local level will be given in message origination and how to control the capabilities that are inherent in the ISDN.

6.3.2 Procedures.

The universal messaging procedures will have been stabilized during Phase II. During this phase, the individual "fine tuning" of S/A procedures will be completed. This is viewed as an ongoing effort that will continue throughout Phase III.

6.3.3 Components.

The major efforts undertaken in Phase III will be related to the implementation of ISDN in the backbone and to the full implementation of the IITS at each installation and base in the DoD. No new DMS components are currently envisioned for this phase.

Section 7

DMS References

7.0 Introduction.

This section identifies the documents and standards directly applicable to the Defense Message System.

7.1 DMS Specific Documents.

USD(A) Memorandum, Program Guidance on the Defense Message System (DMS), 3 August 1988

MJCS-191-88, Multicommand Required Operational Capability for the Defense Message System MROC 3-88, 25 October 1988 (pending validation)

Charter, Defense Message System (DMS) Panel, Approved 22 August 1988.

Charter, Defense Message System (DMS) Implementation Group (DMSIG), Approved 22 August 1988.

DMS Test and Evaluation Master Plan (TEMP) (Draft), undated.

7.2 DMS Pertinent Standards.

CCITT Draft Recommendation F.400/X.400(ISO Working Document for DIS 8505), Message Handling: System and Service Overview, Version 3, August 1987.

CCITT Draft Recommendation X.500 (ISO Working Document for DIS 9594).

FIPS Pub 146, Government Open Systems Interconnection Profile (GOSIP)

7.3 Reference Documents.

Appendix A

DMS Acronyms

Acronym	Title
AC	Access Control
ACC	Access Control Center (for BLACKER)
ACP	Allied Communication Publication
ADI	AUTODIN-DDN Interface
ADP	Automatic Data Processing
AFAMPE	Air Force Automated Message Processing Exchange
AFCAC-251	Air Force Computer Acquisition Center Standard Multiuser Small Computer Requirements Contract
AID	AUTODIN Interface Device
AID-SS	AUTODIN Interface Device with Selective Splitting
AIG	Address Indicator Group
AIHS	Automated Information Handling System
AMF	Abbreviated Message Format
AMHS	Automated Message Handling System
AMIH	AUTODIN Mail Interface Host
AMME	Automated Multi-Media Exchange
AMPE	Automated Message Processing Exchange
AMS	AUTODIN Mail Server
ARPANET	Advanced Research Projects Agency Network
ASC	AUTODIN Switching Center
ASCII	American Standard Code for Information Interchange
AUTODIN	Automatic Digital Network
BFE	BLACKER Front End
CAD	Collective Address Designator
cc	Courtesy copy
CCEB	Combined Communications Electronic Board
CCEP	Commercial COMSEC Endorsement Program
CCITT	International Telegraph and Telephone Consultative Committee
CMF	Common Message Format
CMW	Compartmented Workstation
COMSEC	Communications Security
COTS	Commercial Off-the-Shelf Products
CSP	Communications Support Processor
CSRF	Common Source Routing Files
DAAS	Defense Automatic Addressing System
DAB	Defense Acquisition Board
DARPA	Defense Advanced Research Projects Agency
DCA	Defense Communications Agency
DCEC	Defense Communications Engineering Center

DCS	Defense Communications System
DCT	Digital Communications Terminal
DDN	Defense Data Network
DIA	Defense Intelligence Agency
DIR	Directory
DISNET	Defense Integrated Secure Network
DL	Distribution List
DLA	Defense Logistics Agency
DMS	Defense Message System
DMSWG	Defense Message System Working Group
DoD	Department of Defense
DPI	Data Processing Installation
DSA	Directory System Agent
DSSCS	Defense Special Security Communications System
DSTE	Digital Subscriber Terminal Equipment
DTG	Date Time Group
DUA	Directory User Agent
E3	End-to-End Encryption
EDI	Electronic Data Interchange
E-Mail	Electronic Mail
FMHS	Formal Message Handling Service
FMS	Formal Message Service / Formal Message Server
FRCT	Fixed Record Communications Terminal (USAF)
FTP	File Transfer Protocol
GC	Global Component
GENSER	General Service
GOSIP	Government Open Systems Interconnection Profile
GW	Gateway
HAMPS	Host AUTODIN Message Processing System (USAF)
HARPS	Hybrid AUTODIN Red Patch Service
HDLC	High-Level Data Link Control
IAS	Integrated AUTODIN System
IC	Installation Component
ICA	Integrated Communications Architecture
ID	Identifier/Identification
IITS	Installation Information Transfer System
IEEE	Institute for Electrical and Electronic Engineers
INFOSEC	Information Security
I/O	Input/Output
IP	Internet Protocol
ISDN	Integrated Services Digital Network
ISO	International Standards Organization
JANAP	Joint Army, Navy, Air Force Publication
JCS	Joint Chiefs of Staff
JDL	Joint Development Laboratory
JINTACCS	Joint Interoperability of Tactical C2 Systems

KDC	Key Distribution Center (for BLACKER)
KMGMT	Key Management
KMS	Key Management Service
LAN	Local Area Network
LCS	Life Cycle Support
LDMX	Local Digital Message Exchange
LEAD	Low-cost Encryption and Authentication Device
LMD	Lead Military Department
MAC	Message Authentication Code
MAD	Message Address Directory
MART	Modular AMME Remote Terminal
MBI	Mail Box Interface
MCEB	Military Communications Electronics Board
MEPS	Message Entry and Preparation Software
MGMT	Management
MH	Message Handling (X.400)
MHS	Message Handling System
MILNET	Military Network
MLS	Multi-level Secure
MOP	Memorandum of Policy (JCS)
MPDT	Message Preparation and Dissemination Terminal (CSP)
MROC	Multicommand Required Operational Capability
MSA	Message Storage Agent
MT	Message Transfer
MTA	Message Transfer Agent
MTS	Message Transfer System
MUT	Multiuse (Multiple Use) Terminal
NAMRADS	Naval Automated Message Reproduction and Delivery System
NBS	National Bureau of Standards (now NIST)
NDI	Non-Developmental Item
NIC	Network Information Center
NIST	National Institute for Standards and Technology (formerly NBS)
NMGMT	Network Management
NSA	National Security Agency
OAS	Office Automation System
OASD	Office of the Assistant Secretary of Defense
OC	Organizational Component
OCR	Optical Character Reader (Recognition)
O&M	Operations and Maintenance
OJCS	Office of Joint Chiefs of Staff
ONC	Offnet Connection
O/R	Originator/Recipient
OSD	Office of Secretary of Defense
OSI	Open Systems Interconnection
OSRI	Originating Station Routing Indicator
OSSN	Originating Station Serial Number
OTC	Over-the-Counter

OT&E	Operational Test and Evaluation
OUA	Organizational User Agent
PCMT	Personal Computer Message Terminal (Navy)
PLA	Plain Language Address
POSIX	Portable Operating System Interface (UNIX)
PSN	Packet Switching Node
RC	Regional Component
R&D	Research and Development
RFI	Request for Information
RI	Routing Indicator
RIXT	Remote Information Exchange Terminal
SARAH	Standard Automated Remote to AUTODIN Host
S/A	Service/agency
SBLC	Standard Base Level Computer (previously Phase IV) (USAF)
SC4	Standard Command, Control, Communications and Computers
SCI	Sensitive Compartmented Information
SCINET	Sensitive Compartmented Information Network
SDE	Submission and Delivery Entity
SDNS	Secure Data Network System
SMSCRC	Standard Multiuser Small Computer Requirements Contract (AFCAC-251)
SMTP	Simple Mail Transfer Protocol
SRT	Standard Remote Terminal
TCB	Trusted Computing Base
TCC	Telecommunications Center
TCP	Transmission Control Protocol
T&E	Test and Evaluation
TOF	Time of File
TTY	Teletypewriter
UA	User Agent
UC	User Components
USMCEB	United States Military Communications Electronics Board
UTC	Coordinated Universal Time
UWS	User Work Station
VDT	Video Display Terminal
WINCS	WWMCCS (Worldwide Military Command and Control System) Information Network Communications System
WS	Workstation

Appendix B

DMS Glossary

Access Control: Allows only authorized communication. Example: Only financial officers can have access to a company's financial plans. (Definition source - SDNS).

Authentication: Verifies the identity of a communicating peer entity and the source of data. Example: Owners of bank accounts require assurance that money will only be withdrawn by the owner. (Definition source - SDNS).

Ada: Name of DoD high order programming language described in ANSI/MIL-STD 1815A.

AFCAC 251: Air Force Computer Acquisition Center (AFCAC) commodity buy personal computer contract. The AFCAC-251 Project is also known as the Standard Multiuser Small Computer Requirements Contract (SMSCRC).

Beta Testing: The measurement of the favorable and unfavorable impacts to users in a baseline environment that results from the addition of a new component to that environment. Users of the planned component actively participate in the Beta test and provide feedback on operational and technical issues. Feedback may be incorporated as changes to a future Beta version based on feasibility and need for such change. Beta testing results are ultimately considered in deployment decisions.

BLACKER: A host-to-host protection (encryption) system used in conjunction with a set of PSNs to provide the basis for the DISNET. The components of the BLACKER are the BLACKER Front End (BFE), the Access Control Center (ACC), and the Key Distribution Center (KDC).

Body: The body of the message is the information the user wishes to communicate. In general, a body may consist of a number of different encoded information types such as voice, text, facsimile and graphics (Definition source - X.400 draft).

"Central" DMS Project: DMS policies; common procedures, formats and protocols; and centrally provided components which support all DMS users.

Commodity Buy: Large volume contract to provide hardware to a wide variety of users many of whom were not identified at the time of contract award.

Content: The piece of information that the originating UA wishes delivered to the recipient UA. For IPM UAs, the content consists of either an interpersonal-message or an IPM-status-report (Definition source - X.400 draft).

Data Confidentiality: Protects data against unauthorized disclosure. Protecting the details of an attempted corporate takeover is an example of the need for confidentiality. (Definition source - SDNS).

Data Integrity: Protects against unauthorized modification, insertion and deletion. Example: Electronic funds transfer between banks requires protection against modification of the information. (Definition source - SDNS).

Defense Data Network (DDN): The set of DoD packet switching networks including the classified DDN (DSNET 1, DSNET 2 and DSNET 3) and the unclassified DDN (MILNET, ARPANET, MINET).

Defense Message System (DMS): The DMS consists of all hardware, software, procedures, standards, facilities, and personnel used to exchange messages electronically between organizations and individuals in the Department of Defense. The DMS relies upon but does not include the DoD Internet.

Delivery: The interaction by which the Message Transfer Agent transfers to a recipient User Agent the content of a message plus the delivery envelope (Definition source - X.400 draft).

Descriptive Name: A name that denotes exactly one user in the MHS (Definition source - X.400 draft).

Directory (DIR): A function satisfying the DMS identification of recipients requirements (Definition source - DMSWG). The X.500 series of recommendations defines this as the Directory System (DS).

Directory System Agent (DSA): An element of the Directory System (DS) providing regional service. The DSA and Directory User Agent (DUA) form the DS.

Directory User Agent (DUA): An element of the Directory System (DS) providing local service to the user. The DUA and the Directory System Agent (DSA) form the DS.

DoD Internet: The long-haul data switching backbone networks (currently the DDN) and local post/camp/station electronic telecommunications distribution facilities/networks (LANs, IITS, BITS).

Envelope: A place in which the information to be used in the submission, delivery, and relaying of a message is contained (Definition source - X.400 draft).

Gillaroo: Commercial COMSEC Endorsement Program device for use primarily in personal computers.

Heading: The heading of a message is the control information that characterizes the message (Definition source - X.400 draft).

Individual Messages: This type of message includes routine communications between individual DoD personnel within administrative channels, both internal and external to the individual organizational element. Informational messages and those requiring only a basic transport service (the electronic analogue of the telephone call) will be treated as a part of this class. The driving requirements on the communications system for this class of messages are those of far-reaching, fine grained connectivity and ease of use. (Definition Source Draft - DMS MROC).

"Joint" DMS Project: DMS components which support activities at the base or local level and are intended for use by multiple services and agencies.

KERMIT: Communications protocol capable of supporting guaranteed delivery of binary data.

Mailbox: A computer file, queue or equivalent delivery point which can be accessed by the host's E-Mail delivery process and by the user for reading the mail. In many ways, mailboxes are analogous to US Postal Service mailboxes.

Mailbox Host: Computer system that supports E-Mail and has storage for messages.

Message: In the context of Message Handling Systems, the unit of information transferred by the MTS. It consists of an envelope and a content (Definition source - X.400 draft).

Message Handling System (MHS): The set of UAs plus the MTS (Definition source - X.400 draft).

Message Transfer Agent (MTA): The functional component that, together with the other MTAs, constitutes the MTS. The MTAs provide message transfer service elements by: (1) interacting with originating UAs via the submission dialogue, (2) relaying messages to other MTAs based upon recipient designations, and (3) interacting with recipient UAs via the delivery dialogue (Definition source - X.400 draft).

Message Transfer Layer (MTL): A layer in the Application Layer that provides MTS services elements. These services are provided by means of the services of the layer below plus the functionality of the entities in the layer, namely, the MTAEs and the SDEs (Definition source - X.400 draft).

Message Transfer Protocol (P1): The protocol which define the relaying of messages between MTA's and other interactions necessary to provide MTL services (Definition source - X.400 draft).

Message Transfer System (MTS): The collection of MTAs, which provide the Message Transfer Service elements (Definition source - X.400 draft).

Non-repudiation: Non-repudiation with proof of origin provides to the recipient proof of the origin of data and protects against any attempt by the originator to falsely deny sending the data or its contents. For example, non-repudiation with proof of origin can be used to prove to a judge that a person signed a contract. (Definition source - SDNS).

Offnet Connection (OFC): A function addressing the DMS Allied, tactical and commercial refile interfaces (Definition source - DMSWG).

Open Systems Interconnection (OSI): A term referring to the capability of interconnecting different systems (Definition source - X.400 draft).

Originator Recipient (O/R) Address: A descriptive name for a UA that contains certain characteristics which help the MTS to locate the UA's point of attachment. An O/R address is a type of O/R name (Definition source - X.400 draft).

Organizational Message: This type of message includes command and control traffic and messages exchanged between organizational elements. These messages require release by the sending organization and distribution determination by the receiving organization. Due to their official and sometimes critical nature, such messages impose operational requirements on the communications systems for such capabilities as non-routine precedence, guaranteed timely delivery, high availability and reliability, and a specified level of survivability (Definition Source - Draft DMS MROC).

Originating UA: A UA that submits to the MTS a message to be transferred (Definition source - X.400 draft).

Originator: A user, a human being or computer process, from whom the MHS accepts a message (Definition source - X.400 draft).

Rapid Prototyping: Method to accelerate the availability of a new system to field by configuring and testing components in a Beta Test site environment.

Recipient: A user, a human being or computer process, who receives a message from the MHS (Definition source - X.400 draft).

Recipient UA: A UA to which a message is delivered or that is specified for delivery (Definition source - X.400 draft).

Relaying: The interaction by which one Message Transfer Agent transfers to another the content of a message plus the relaying envelope (Definition source - X.400 draft).

Relaying Envelope: The envelope which contains the information related to the operation of the MTS plus the service elements requested by the originating UA (Definition source - X.400 draft).

SARAH: Standard Automated Remote to AUTODIN Host. AF developed software for personal computers to prepare and transmit DD173 and JANAP 128 formatted messages via AUTODIN.

Submission: The interaction by which an originating User Agent transfers to a Message Transfer Agent the contents of a message plus the submission envelope (Definition source - X.400 draft).

Submission and Delivery Entity (SDE): An entity that is located in the MTL, co-resident with a UA and not with an MTA, and responsible for controlling the submission and delivery interactions with a MTA (Definition source - X.400 draft).

Submission Envelope: The envelope which contains the information the MTS requires to provide the requested service elements (Definition source - X.400 draft).

Traffic Flow Confidentiality: A special type of data confidentiality; it protects the identities of the communicating parties and the amount of communication between them. Example: A marked increase in the communications between two companies could be an indication of a merger or joint product development project. (Definition source - SDNS).

User: A person or computer application or process who make use of MHS. A user is referred to as either an originator (when sending a message) or a recipient (when receiving one) (Definition source - X.400 draft).

User Agent (UA): Typically a set of computer processes (for example, an editor, a file system, a word processor) that are used to create, inspect, and manage the storage of messages. There is typically one user per UA. During message preparation, the originator communicates with his UA via an input/output (I/O) device (for example, a keyboard, display, printer, facsimile machine, and/or telephone). Also by means of these devices, the UA communicates to its user messages received from the MTS. To send and receive messages, the UA interacts with the MTS via the submission and delivery protocol (Definition source - X.400 draft).

User Agent Entity (UAE): An entity in the UAL of the Application Layer that controls the protocol associated with cooperating UAL services. It exchanges control information with the MTAE or SDE in the layer below. The control information is the information the MTL requires to create the appropriate envelope and thus provide the desired message transfer service elements (Definition source - X.400 draft).

User Agent Layer (UAL): The layer that contains the UAEs (Definition source - X.400 draft).

"User" DMS Project: DMS components which support a single Service or agency or portion thereof.

X.200: Reference model of open systems interconnection for CCITT applications.

X.400: Draft Recommendation X.400, Message Handling Systems: System Model-Service Elements, is one of a series of Recommendations and describes the system model and service elements of the MHS. This recommendation defines the MH Services that Administrations provide to enable subscribers to exchange messages in a store-and-forward basis. Two MH Services are provided. The Interpersonal Messaging (IPM) Service supports interpersonal communication, including communication with existing CCITT Telex and Telematic services. The Message Transfer (MT) Service supports general, application-independent message transfer (Definition source - X.400 draft).

X.500: Directory Server. Proposed standard for message address server.

Appendix C

Security Policy

C.0 Introduction.

This appendix will contain DMS Security Policy Guidance when developed by the DMS Security Policy Working Group (SPWG). See paragraphs 2.8 and 5.3.1c for examples of security policy issues that must be resolved during Phase I.

Appendix D

D.0 Introduction.

This appendix contains the list of organizations and offices receiving the DMS Target Architecture and Implementation Strategy. Department of Defense addressees are listed in paragraph D.1 and business and industry addressees are listed in paragraph D.2. Other addressees not covered in preceding paragraphs are listed in paragraph D.3, which primarily lists non-DoD organizations currently authorized to use the DMS for organizational messaging.

DISTRIBUTION	Copies

D.1 Department of Defense Distribution.

Office of the Assistant Secretary of Defense for Command, Control, Communications and Intelligence (Information Systems) The Pentagon, Room 3E187 Washington, DC 20301	5
Office of Joint Chiefs of Staff Attn: Code J6T Washington DC 20301	1

UNIFIED AND SPECIFIED COMMANDS

Commander-in-Chief U.S. Southern Command Attn: SCJ6-P APO Miami FL 34003-0226	1
Commander-in-Chief Strategic Air Command Attn: SC Offutt AFB NE 68113	1
Commander-in-Chief Central Command Attn: CCJ-B MacDill AFB FL 33608	1
Commander-in-Chief Europe Attn: C3S-TSP APO NY 09131	1
Commander-in-Chief U.S. Special Operations Command Attn: SOJ6-I MacDill AFB FL 33608-6001	1
Commander-in-Chief Atlantic Attn: J62B Norfolk VA 23511-5100	1
Commander-in-Chief Pacific Attn: C3STM11 Camp Smith HI 96861-5025	1

DISTRIBUTION	Copies
Commander-in-Chief Aerospace Defense Command Attn: KRQR Peterson AFB CO 80914	1

DISTRIBUTION	Copies
ARMY	
Headquarters Department of the Army Attn: SAIS-AD Washington DC 20310-0700	4
Department of the Army Attn: SAIS-PP Pentagon, 1D664 Washington, DC 20310-0107	5
Department of the Army Attn: SAIS-PS Pentagon, 1C710 Washington, DC 20310-0107	1
Department of the Army Attn: DAMP-FDC Pentagon, 2E537 Washington, DC 20310-0107	1
Chief U.S. Army C-E Services Office Attn: SFIS-FAC-M Room 918, Crystal Mall 4 Washington DC 20376-5009	1
USAOTEA ATTN: CSTE-CE 5600 Columbia Pike Falls Church, VA 22041	1
Commander U.S. Army Information Systems Command Attn: AS-PLN-AS, AS-LOG-LD, AS-ENGR Fort Huachuca AZ 85613-5000	4
Commander USAISEC Attn: ASB-TEP-B Fort Huachuca AZ 85613-5300	1
Commander USAISEC ATTN: ASB-SET-N (Mr. Laskowski) Fort Huachuca, AZ 86513-5300	1
PEO Networks Attn: AS-PEN-SWR (Mr. Petito) Squire Hall Ft. Monmouth, NJ 07703	1

DISTRIBUTION	Copies
Program Manager Defense Communications and Army Switched Systems Attn: ASM-SW-B Fort Monmouth NJ 07703-5501	1
Program Manager Army Information Systems Attn: AMCPM-COM-LG-SI-S Fort Monmouth NJ 07703-5501	1
Office of the Project Manager Multiservice Communications Systems Attn: AMCPM-MSCS (Barricelli) Ft. Monmouth, NJ 07703-5000	1
Commander U.S. Army Information Systems Engineering Support Activity Attn: ASBH-SDM-F, ASBH-OPA, ASBH-TES-D, ASBH-SES-D Fort Huachuca AZ 85613-5300	4
Commander USA Combined Arms Center Attn: ATZL-CAC-A Fort Leavenworth, KS 66027	2
U.S. Army PERSINSCOM Attn: ASNI-PP (Mr. Miller) 200 Stovall Street Alexandria, Va. 22332-1520	1
U.S. Army Intelligence and Security Command Code IATEL Arlington Hall Station Arlington Va. 22212	1
Commander USASC&FG Attn: ATZH-POE Fort Gordon, GA 30905	2
Commander USAISC Fort McPherson Attn: ASNA-MCP-PR Bldg 51 Fort McPherson, GA 30330-5000	1
Commander 7th Signal Command Attn: ASN-OP-PA Fort Ritchie MD 21719-5000	1

DISTRIBUTION	Copies
Commander 5th Signal Command Attn: ASE-OP-RN APO NY 09056	1
Commander 1st Signal Brigade Attn: ASK-OP-PI APO San Francisco CA 96301	1
USAISC-WESTCOM ATTN: AS-OP Ft Shafter, HI 96058	1
USAISC-Japan ATTN: ASJ-OP APO San Francisco 96343	1

DISTRIBUTION	Copies
NAVY	
Chief of Naval Operations Attn: Director, Naval Communications Division (OP 941C) Washington DC 20305-2000	1
Naval Security Group Attn: G13/G33 Washington D.C. 20390	2
Director Naval Telecommunications Automation Support Center c/o NAVCOMMUNIT Washington Attn: Code 44 Washington, DC 20397-5310	1
Commander-in-Chief U.S. Naval Forces Europe FPO NY NY 09510	1
Commander Space and Naval Warfare Systems Command National Center I Attn: 110-2L, PDW 110-1425, PDW 120 Washington DC 20363-5100	3
Commander Naval Intelligence Command Attn: NIC-00Q5 4600 Silver Hill Rd Washington DC 20389-5000	1
Commander Naval Telecommunications Command Attn: N51 4401 Massachusetts Avenue, NW Washington DC 20390-5290	1
Naval Research Laboratory Attn: Code 5540 4555 Overlook Avenue, SW Washington, DC 20375-5000	1
Commanding Officer Naval Electronic Systems Engineering Center Vallejo Attn: Code 320, Code 340 Bldg 509, Mare Island Vallejo CA 94592-5017	2

DISTRIBUTION	Copies
Commanding Officer Naval Electronic Systems Engineering Center Portsmouth Attn: Code 220 P.O. Box 55 Portsmouth VA 23705	1
Director Naval Telecommunications Systems Integration Center c/o NAVCOMMUNIT Attn: Code 02 Washington DC 20390-5340	1
Naval Data Automation Command Attn: Code 32 Building 166 Washington Navy Yard Washington DC 20374-1662	1
Naval Ocean Systems Center Attn: Code 852 San Diego, CA 92152-5000	1
Commander Operational Test and Evaluation Force Norfolk, VA 23511	1
Naval Commercial Communications Office 4401 Massachusetts Ave, NW Washington, DC 20390-5290	1

DISTRIBUTION	Copies
AIR FORCE	
Headquarters Department of the Air Force Attn: SCTT Washington DC 20330-5190	1
Headquarters Military Airlift Command Attn: SC Scott AFB, IL 62225-5001	1
Headquarters Air Force Communications Command Attn: XPQC Scott AFB IL 62225-6001	1
Headquarters Air Force Communications Command Attn: XPPB Scott AFB IL 62225-6001	1
Headquarters Air Force Communications Command Attn: DO Scott AFB, IL 62225-5001	1
Airlift Communications Division Attn: XP, DO Scott AFB IL 62225	1
HQ Electronic Security Command Attn: DC San Antonio TX 78243	1
Headquarters AFOTEC Attn: XPP Kirtland AFB, NM 87117-7001	1
1815 OTES ATTN: PEQM Wright-Patterson AFB, OH 45433	1
Headquarters Air Force Intelligence Agency Attn: IND Bowling AFB, DC 20332-5000	1

DISTRIBUTION	Copies
HQ ESC/ICP (AMHS PMO) ATTN: Mr. Henry Hajko/MAJ Goodner Hanscom AFB, MA 01731-5000	2
HQ ESD/AVB Hanscom AFB, MA 01731-5000	2
Standard Systems Center Attn: XP Bldg 888 Gunter AFB AL 36114-6343	1
Standard Systems Center Attn: SSMT Bldg 325 Gunter AFB AL 36114-6343	2
Headquarters 323 FTW Attn: SC4 Mather AFB, CA	1
HQ USWCOM Attn: C3S-TSP APO NY 09128	1
Command and Control Systems Office Attn: CC Tinker AFB, OK 73145-6343	1
Command and Control Systems Office Attn: XPP Tinker AFB, OK 73145-6343	1
HQ EID Attn: EP, EI, EPNB Tinker AFB OK 73145-6343	3
Headquarters Pacific Air Force Attn: SC Hickem AFB, HI 96853-5001	1
Headquarters U.S. Air Force Euprope Attn: SC APO New York 09012-5001	1

DISTRIBUTION	Copies
Headquarters Air Force Systems Command Attn: SC Andrews AFB, MD 20334-5000	1
Headquarters Air Force Logistics Command Attn: SC Wright-Patterson AFB, OH 45433-5001	1
Headquarters Air Force Space Command Attn: LK Peterson AFB, CO 80914-5001	1
HQ AFMPC Attn: DMPD Randolph AFB, TX 78150	1

DISTRIBUTION	Copies
US MARINE CORPS	
Headquarters US Marine Corps ATTN: Code CMC(CC) Washington DC 20380-0001	1
Headquarters US Marine Corps ATTN: Code CCP-17 Washington DC 20380-0001	1

DISTRIBUTION	Copies
DEFENSE COMMUNICATIONS AGENCY	
Director Joint Tactical Command Control and Communications Agency Attn: Code C3A-DWS, C3A-MS, RORC, C3A-SEET Fort Monmouth NJ 07703-5513	4
Director Joint Tactical Command Control and Communications Agency Attn: C3A-ADW-S 11440 Issac Newton Square, North Reston, VA 22090-5006	2
Defense Communications Agency Attn: Code A510 Washington, DC 20305	1
Defense Communications Agency Attn: Code A710 Washington, DC 20305	2
Defense Communications Agency Attn: Code B220 Washington DC 20305-2000	1
Defense Communications Agency Attn: Code B602 Washington DC 20305-2000	1
Defense Communications Agency Attn: Code B604 Washington DC 20305-2000	6
Defense Communications Agency Attn: Code B610 Washington DC 20305-2000	1
Defense Communications Agency Attn: Code B620 Washington DC 20305-2000	1
Defense Communications Agency Attn: Code B640 Washington DC 20305-2000	1
Defense Communications Agency Attn: Code B650 Washington DC 20305-2000	1

DISTRIBUTION	Copies
Defense Communications Agency Attn: Code B670 Washington DC 20305-2000	1
Defense Communications Agency Attn: Code B750 Washington DC 20305-2000	1
Defense Communications Agency Attn: Code H110 Washington DC 20305-2000	1
Defense Communications Agency Attn: Code H610 Washington DC 20305-2000	1
Defense Communications Agency Attn: Code H740 Washington DC 20305-2000	1
Defense Communications Agency Attn: Code N260 Washington DC 20305-2000	1
Defense Communications Engineering Center Attn: Code R100 1860 Wiehle Avenue Reston VA 22090-5500	1
Defense Communications Engineering Center Attn: Code R600 1860 Wiehle Avenue Reston VA 22090-5500	1
Defense Communications Engineering Center Attn: Code R620 1860 Wiehle Avenue Reston VA 22090-5500	1
Defense Communications Engineering Center Attn: Code R640 1860 Wiehle Avenue Reston VA 22090-5500	1
Defense Communications Agency European Area Attn: Code E500 APO NY 09131	1

DISTRIBUTION	Copies
Defense Communications Agency Pacific Area Attn: Code P650 Wheeler AFB HI 96854-5000	1
Defense Communications Agency Northwest Pacific Region APO San Francisco 96328-5000	1
Defense Communications Agency Southwest Pacific Region APO San Francisco 96274-5000	1
Defense Communications Agency Korea Field Office APO San Francisco 96301-0069	1
Defense Communications Agency Okinawa Field Office Box 959 FPO Seattle 98773	1
Defense Communications Agency Guam Field Office Box 141NAVCAMS WESTPAC FPO San Francisco 96630-1837	1
Defense Communications Agency Alaska Field Office Elmendorf AFB AK 99506-5000	1

DISTRIBUTION	Copies
NATIONAL SECURITY AGENCY	
Director National Security Agency Attn: Code T03 9800 Savage Road Fort George G. Meade MD 20755-6000	1
Director National Security Agency Attn: Code T124 9800 Savage Road Fort George G. Meade MD 20755-6000	1
Director National Security Agency Attn: Code T411 9800 Savage Road Fort George G. Meade MD 20755-6000	1
Director National Security Agency Attn: Code T414 9800 Savage Road Fort George G. Meade MD 20755-6000	1
Director National Security Agency Attn: Code C23 9800 Savage Road Fort George G. Meade MD 20755-6000	1
Director National Security Agency Attn: Code C207 9800 Savage Road Fort George G. Meade MD 20755-6000	1

DISTRIBUTION	Copies
DEFENSE INTELLIGENCE AGENCY	
Director Defense Intelligence Agency Attn: Codes DSE-2 3100 Clarendon Boulevard Washington, D. C. 22201-5324	2
Director Defense Intelligence Agency Attn: Code DSE-3 3100 Clarendon Boulevard Washington, D. C. 22201-5324	2
DEFENSE LOGISTICS AGENCY	
Headquarters, Defense Logistics Agency Attn: DLA-A, DLA-ZW, DLA-W, DLA-T, DLA-ZP Cameron Station Alexandria VA 22304-6100	5
Defense Automatic Addressing System Office Attn: DAAS-VC S. Chrisman Rd Tracy CA 95376-5000	1
Defense Electronic Supply Center Attn: DESC-W 1507 Wilmington Pike Dayton OH 45444-5000	1
Defense Logistics Service Center Attn: DLSC-ZT Battle Creek MI 49016	1
Defense Automatic Addressing System Office Attn: DAAS-V 1507 Wilmington Pike Dayton OH 45444-5000	1
Defense Logistics Agency Systems Automation Center Attn: DSAC-R P.O. Box P1605 Columbus OH 43216	1

DISTRIBUTION	Copies
DEFENSE MAPPING AGENCY	
DMA Telecommunications Services Center ATTN: Mr. Farrington 1840 Michael Farraday Drive Reston, VA 22090-5304	1
Defense Mapping Agency Deputy Director Information Systems Telecommunications Services Center 1840 Michael Farraday Drive Reston, VA 22090-5304	1
US MILITARY COMMUNICATIONS ELECTRONICS BOARD	
HQ USMCEB Room 1B707 Washington, DC 20301-5000	1

D.2 Industry Distribution.

ACS COMMUNICATIONS SYSTEMS, Inc 1
Attn: Paul G. Jones
480 Spring Park Place, Suite 900
Reston, VA 22090

Advanced Digital Systems, Inc. 1
Attn: Sharon C. Ballard
10052 Mesa Ridge Court
San Diego, CA 92121

Advanced Systems Development 1
Defense Systems Group
Attn: Donna S. Ireton
1701 N. Fort Myer Drive, Suite 1101
Arlington, VA 22209

Advanced Technology, Inc. 1
Attn: M. Trammell G-3.02
12001 Sunrise Valley Drive
Reston, VA 22091

Alta Telecom, Inc. 1
Attn: Carol Evans
Technology Park
680 Engineering Drive, Suite 120
Norcross, GA 30092

AMDAHL Corporation 1
Attn: Tom Kane
4801 Massachusetts Avenue, NW, Suite 600
Washington, D. C. 20016

American Management Systems, Inc 1
Attn: Tom Dean
1525 Wilson Blvd
Arlington, VA 22209

American Systems Corporation 1
Attn: Donna Charapich
14200 Park Meadow Drive
Chantilly, VA 22021

Analysis 1
1232 Glenbrook Road
Huntingdon Valley, PA 19006

A&R Associates, Inc. 1
Attn: R. D. McMichael
Box 479
Gwynedd Valley, PA 19437

DISTRIBUTION	Copies
ARDAK Corporation Attn: Dai Chuang Information Technology and Management 1493 Chain Bridge Road McLean, VA 22101	1
ARINC Research Corporation Attn: Rod Sato 2551 Riva Road Annapolis, MD 21401	1
Associated Enterprises, Inc. Attn: Cheryl Stevenson 120 Admiral Cochrane Drive Annapolis, MD 21401	1
Astronautics Corporation of America Attn: Joseph C. Racke P. O. Box 523 Milwaukee, WI 53201-0523	1
AT&T Federal Systems Attn: L. S. Page 204 Graham Hopedale Road Burlington, NC 27215	1
AT&T Federal Systems Attn: B. S. Booth P. O. Box 20046, Dept. 71GC027430 Greensboro, NC 27420	1
AT&T Attn: Dennis J. Dadant 9160 Guilford Road Columbia, MD 21046	1
Atlantic Research Corporation Attn: Sam Steed 5390 Cherokee Avenue Alexandria, VA 22312	1
Aura Tech, Inc. Attn: James Carr 5733 La Jolla Blvd, Suite 18 La Jolla, CA 92037	1

DISTRIBUTION	Copies
Authorization Systems, Inc. Attn: Edmond A. Allman Information Management Systems Suite 520 12300 Twinbrook Parkway Rockville, MD 20852	1
Aydin Monitor Systems Attn: Ann Malickson 502 Office Center Drive Fort Washington, PA 19034	1
BBN Communications Corporation Attn: Robert W. Streckfuss 8000 Westpark Drive, 6th Floor McLean, VA 22102	1
BETAC Corporation Attn: Carolyn K. Baker 1401 Wilson Boulevard Arlington, VA 22209	1
Boeing Aerospace Attn: Dan Schnackenberg M/S 87-06 P. O. Box 3999 Seattle, WA 98124	1
Booz-Allen and Hamilton, Inc. Attn: Marjorie E. Adams 4330 East West Highway Bethesda, MD 20814-4455	1
BYTEC Corporation Federal Systems Group Attn: Scott Armstrong/John R. O'Connor 1501 Lee Highway, Suite 204 Arlington, VA 22209	1
CEN Corporation Attn: John Wegl 8105 Langbrook Road Springfield, VA 22152-1226	1
Centel Communications Systems Attn: Regina L. Baer 601 Jefferson, Suite 1000 Houston, TX 77002	1

Centel Information Systems, Inc. 1
Attn: Deborah Cooper
5515 Security Lane, Suite 1100
Rockville, MD 20852

Centigram Corporation 1
Attn: Daniel E. Wessel
8401 Old Courthouse Road, #100
Tysons Corner, VA 22180-3807

Cincinnati Bell Information Systems, Inc. 1
Attn: Jed Jaffe
1100 Wayne Avenue
Silver Spring, MD 20910

COGNITRONICS Corporation 1
Attn: Clark Murphy
25 Cresent Street
Stamford, CT 06906

COMCON, Inc. 1
Attn: Jim Healy
Number 2 Commerce Drive
Morristown, NJ 08057

Command Corp. of W. Virginia 1
Attn: Curtis E. Brannon
116 E. Washington Street
Charles Town, WV 25414

Communication Machinery Corporation 1
Attn: A. J. Nicolosi
6303 Ivy Lane, Suite 400
Greenbelt, MD 20770

Communication Systems Technology, Inc. 1
Attn: Robert E. McKisson/Carol Fox
9740 Patuxent Woods Drive
Columbia, MD 21046

Communications & Power Engineering, Inc. 1
Attn: Borge Riis-Vestergaard
30343 Canwood Street, Suite 110
Agoura Hills, CA 91301-2018

Computer Data Systems, Inc. 1
Attn: S. Glen/Thomas H. Grim
One Curie Court
Rockville, MD 20850

DISTRIBUTION	Copies
Computer Sciences Corporation Attn: MaRee Guyton MC 212/Robert W. Steele 6565 Arlington Blvd. Falls Church, VA 22046	1
Concurrent Computer Corporation Attn: Rick Nasti 106 Apple Street Tinton Falls, NJ 07755	1
CONTEL ASC Government Networks Division Attn: Ed Firth 7916 Westpark Drive McLean, VA 22102	1
Conversational Voice Technology Attn: Laura Hinze 4205 Grove Avenue Gurnee, IL 60031	1
Cross Systems, Inc. Attn: Warner G. Ast 8601 Dunwoody Place, Building 100 Atlanta, GA 30350	1
CSM Consultants Attn: Mr. Charles S. Modricker 1123 Tollhouse Road Warminster, PA 18974	1
CTG, Inc. Attn: Brian T. Forbes/Steve Stofko 450 Main Ave East, Suite 208 Vienna, VA 22180	1
Cybercon Research Corporation Attn: Dr. Gene Hilborn 2555 Park Boulevard, Suite 8 Palo Alto, CA 94306-1919	1
C3, Inc. Attn: Robert A. Ballard/M. K. Gammill 460 Herndon Parkway Herndon, VA 22070-5201	1
Data General Attn: Lee Trumbore 7927 Jones Branch Road, Suite 500 McLean, VA 22102	1

Data Systems Analyst Attn: R.B. Clement 10400 Eaton Place, Suite 500 Fairfax, VA 22030	1
Denro, Inc. Attn: Kip Blair 9318 Gaither Road Gaithersburg, MD 20877	1
Digital Equipment Corporation Attn: Jim Scott MEL 4-13 8400 Corporate Drive Landover, MD 20785	1
EDS Attn: Diana Metzger 13600 EDS Drive Herndon, VA 22071	1
Eastern Computers, Inc. Attn: Maryellen Englehardt 564 Lynnhaven Parkway, Suite 101 Virginia Beach, VA 23452	1
Eaton Corporation Attn: Gordon Osborne 31717 La Tienda Drive West Lake Village, CA 91359	1
Electronic Data Systems Attn: Andy Szkotak 6430 Rockledge Dr. Bethesda, MD 20817	1
Electrospace Systems, Inc Attn: D. E. Heitzman 1601 North Plano Road Richardson, TX 75083-1359	1
EPS, Inc. Attn: Margaret D'Amore 70 Apple Street Tinton Falls, NJ 07724	1
E-Systems Attn: J.G. King Garland Division P.O. Box 660023 Dallas, Texas 75266-0023	1

DISTRIBUTION	Copies
Federal Information Technologies, Inc. Attn: Dale D. Rowley 450 Spring Park Place, Suite 900 Herndon, VA 22070	1
Fiber-Tel, Inc. Attn: Paul L. Rowe 1203 So. Houston Avenue Humble, TX 77338	1
Fluor Daniel Corporation Attn: Jim Hoffman 1627 K Street N.W. Washington, D.C. 20006	1
Ford Aerospace & Communications Corporation Attn: G. W. Lazaroff, MSPD 7100 Standard Drive Hanover, MD 21076	1
Ford Aerospace & Communications Corporation Attn: Barry D. Gay 10440 State Highway 83 Colorado Springs, CO 80908-3699	1
Ford Aerospace & Communications Corporation Western Development Laboratories Div. Attn: Bid Register Desk, M/S T-17 (James Joy) 3939 Fabian Way Palo Alto, CA 94303	1
General DataComm Systems, Inc. Attn: Karen B. Duanthan P.O. Box 1403 Oldsmar, FL 34677-1403	1
General Electric Company Automated Systems Department Attn: Mr. William T. Meyer 2700 Fry Boulevard, Suite B-3 Sierra Vista, AZ 85635	1
General Electric Company Attn: Charles Neelands 10803 Parkridge Blvd. Reston, VA 22091	1
General Electric Company Silicon Systems Technology Dept. Attn: Thomas S. Hosky 2750 Prosperity Avenue, Suite 200 Fairfax, VA 22031	1

DISTRIBUTION

	Copies
GEOSTAR Attn: Nick Cheston 1001 22nd Street, N.W Washington, D.C. 20037	1
Global Weather Dynamics, Inc. Attn: William A. Wolff 2400 Garden Road Monterey, CA 93940	1
Gray Communication Attn: George Ishee 1861 Wiehle Avenue, Suite 104 P. O. Box 3706 Reston, VA 22090	1
Grid Systems Attn: Risa Katz 8133 Leesburg Pike, Suite 600 Vienna, VA 22180	1
Grumman Data Systems Attn: James T. Peek 6862 Elm Street McLean, VA 22101	1
GTE Government Systems Corporation Attn: C. A. Barcynski 1777 N. Kent Street, Suite 500 Arlington, VA 22209	1
GTE Government Systems Corporation Government Systems Division Attn: A. Whitmore/Steve Longee 77 A Street Needham Heights, MA 02194	1
GTE Strategic Systems Divisions Attn: Gerald LeDuc P.O. Box 14009 Huntsville, Al. 35815	1
Harbor Research Group Attn: William M. Smith Golden Circle Business Development Center 2010 South Ankeny Blvd. Ankeny, IA 50021	1

Harris Corporation (GESD) 1
Attn: Richard D. Anders/Mark F. Wolf
P. O. Box 96000, M/S 6B-9411
Melbourne, FL 32902

Harris Data Services Corporation 1
Attn: Jeff DePasquale
3816 Elm Avenue
Montgomery, Alabama 36109

Heritage Engine Collection 1
6 Windward Drive
Severna Park, MD 21146

Hershey Business Products, Inc. 1
Attn: Neal R. Fischer
7360 Trade Street
San Diego, CA 92121

Honeywell Federal Systems 1
Attn: Jim Stewart M/S 1114
7900 Westpark Drive
McLean, VA 22102

Horizons Data Corporation 1
Attn: Charlie Strauss
503 Carlisle Drive
Herndon, VA 22070

Horizons Technology, Inc. 1
Attn: Donald H. Costello
Suite 201
10467 White Granite Drive
Oakton, VA 22124

Hughes Aircraft Company 1
Microelectronic Systems
Attn: J. B. Robertson
2601 Campus Drive
P. O. Box 19618
Irvine, CA 92715

IBM 1
Federal Systems Division
Attn: Bob Olivier
100 Lakeforest Blvd
Gaithersburg, MD 20877

DISTRIBUTION	Copies
IBM Federal Systems Division Attn: Carl Smothers 9500 Godwin Drive Manassas, VA	1
Information Networks Inc. Attn: Bob Norse/Bob Campbell 11426 Rockville Pike Suite 108 Rockville, MD 20852	1
Integrated Microcomputer Systems, Inc Attn: Andy Bilyk 2 Research Place Rockville, MD 20850	1
International Technology Corporation Attn: John D. Randall P.O. Box 6070 McLean, VA 22106	1
IRT Attn: Charles R. Corjay 1953 Gallows Road, Suite 200 Vienna, VA 22180	1
J. G. Van Dyke and Associates Attn: James Wood, II 5510 Cherokee Avenue, Suite 300 Alexandria, VA 22312	1
James P. Anderson, Co Attn: James P. Anderson P.O. Box 42 Fort Washington, PA 19034	1
KMS Fusion, Inc. Attn: W. J. Pollard P. O. Box 1567 3853 Research Park Drive Ann Arbor, MI 48106	1
Kaman Sciences Corporation Attn: John N. Elliott 1500 Garden of the Gods Road P. O. Box 7463 Colorado Springs, CO 80933	1
Lightnet Attn: Ralph Myers 600 East Jefferson Street Rockville, MD 20852-1150	1

Lockheed Electronics Company, Inc. 1
Attn: P. Jankouskas
1501 U.S. Highway 22, C.S. #1
Plainfield, NJ 07061-1501

Lockheed Missiles & Space Company, Inc. 1
Attn: Carol E. Kennedy
6800 Burleson Road
Austin, TX 78744

Lockheed Missiles and Space Company, Inc. 1
Attn: Keith Furney
6767 Old Madison Pike, Suite 180
Huntsville, AL 35806

Logicon RDA 1
Attn: J. B. Hendershot
2100 Washington Blvd
Arlington, VA 22204-5703

Martin Marietta Corporation 1
Attn: Scott Adler
6801 Rockledge Drive
Bethesda, MD 20817

McDonnell Douglas, Inc. 1
Attn: Ken Arnold/Teresa Ruiz
8201 Greensboro
McLean, VA 22102

Merdan Group Inc. 1
Attn: John Cronican
4617 Ruffner Street
P.O. Box 17098
San Diego, CA 92117

Microlog Corporation 1
Attn: John P. Mitchell
20270 Goldenrod Lane
Germantown, MD 20874

MJI Associates 1
Attn: Michael J. Ionta
13306 Tuckaway Drive
Fairfax, VA 22033

Motorola, GEG 1
Attn: Tom Grimes M/D H1114
8201 East McDowell Road
Scottsdale, AZ 85252

NCR Comten
Attn: Pete Rose
15235 Shady Grove Road
Rockville, MD 20850 1

Network Solutions
Attn: S.L. Christine
Defense Systems Department
8229 Boone Boulevard, 7th Floor
Vienna, VA 22180 1

Northern Telecom, Inc.
Attn: Paul D. Campbell
Federal Networks
12th Floor
8614 Westwood Center Drive
Vienna, VA 22180-2233 1

Paradigm Technologies Corp
2680 Monterey Road
Attn: Dan Van Ostrand
San Marino, CA 91108 1

Paradyne
Attn: John Duker
1577 Springhill Road #300
Vienna, VA 22180 1

Pilot Research Associates, Inc
Attn: Dudley Moorhous
8027 Leesburg Pike Suite 700
Vienna, VA 22180 1

RCA Corporation
Government Communications Systems Div.
Attn: CAGE 11447 (Robt V. Perkins)
Bldg. 2-4, Front & Cooper Streets
Camden, NJ 08102-2399 1

Reach Voice Mail Service, Inc.
Attn: Williams and Sutterfield
11520 Saint Charles Rock Road
Bridgeton, MO 63044 1

RJO
Attn: A. Michele Kebea
4550 Forbes Boulevard
Lantham, MD 20706 1

Rockwell International 1
Electronics Operations
Attn: Fay Blacketer
Bid Registry, 460-320
3200 East Renner Road
Richardson, TX 75081-6209

Rugged Digital Systems, Inc. 1
Attn: Kent Bartlett
665 Clyde Avenue
Mountain View, CA 94043

Science Management Corporation 1
Attn: Terry Goodman (CODE 1153)
8300 Professional Place
Landover, MD 20785

SFI Electronics, Inc. 1
Attn: Vicki Baker
400 Clanton Road, Suite A
Charlotte, NC 28217

Sidereal Corporation 1
Attn: Melvin R. Hall/T.G. Cassidy Jr
2011 Crystal Drive, Suite 210
Arlington, VA 22202

SIMPACT Associates, Inc. 1
Attn: Robert Curtis/D. Henry
11109 Sunset Hills Road
Reston, VA 22090

S. Kirvingusn, Inc. 1
Attn: Sam K. Irving
6613 Byrnes Drive
McLean, VA 22101

Snider Engineering Inc. 1
Attn: J. Snyder
8133 Leesburg Pike, Suite 250
Vienna, VA 22180

SofTech, Inc. 1
Attn: Donald W. Rice
3100 Presidential Drive M/S MD
Fairborn, OH 45324-2039

South Central Bell 1
Federal Government Marketing
Attn: Jim Futrell
3196 Highway 280S, Rm 318S-B
Birmingham. AL 35243

Squires Telecommunications Company 1
Attn: William J. Goodman
8401 Old Courthouse Road
Tysons Corner, VA 22180-3807

SRA Corporation 1
Attn: Joan van Steyn
2000 15th Street North
Arlington, VA 22201

Warren H. Suss 1
Attn: R. Schwartzbard
764 Old York Road
Jenkintown, PA 19046

SRS Technologies 1
Attn: Wayne Pennington
5113 Leesburg Pike, Suite #212
Falls Church, VA 22041

SSDS, Inc. 1
Attn: Shep Crow
8150 Leesburg Pike, Suite 1200
Vienna, VA 22180

Stanford Telecommunications, Inc. 1
Attn: Tony Pan/Larry Krebs
2421 Mission College Boulevard
Santa Clara, CA 95054

Sterling Software Inc 1
Attn: James C. Skaar/M.A.Theel
1404 Fort Crook Road South
Bellevue, NE 68005-2969

Sutter & Associates 1
Attn: W. E. Sutter
120 Donald Ross Drive
Pinehurst, NC 28334

SWL, Inc. 1
Attn: Jeffrey M. Hayden
Suite 700, Park Place
7926 Jones Branch Drive
McLean, VA 22102

Sybase Inc 1
Attn: Ben Martindale
Suite 709
11300 Rockville Pike
Rockville, MD 20852

Sysorex Information Systems, Inc. 1
Attn: Jim Murphy
5201 Leesburg Pike, Suite 700
Falls Church, VA 22041

Systems Integration & Research, Inc. 1
Attn: G. Torres/G.R. Reynolds
6201 Leesburg Pike, Suite 403
Falls Church, VA 22044

Tandem Computers, Inc. 1
U. S. Federal Operations
Attn: Martin Decre
12100 Sunrise Valley Drive
Reston, VA 22091-3407

Telecommunications Strategies, Inc. 1
Attn: Michael Vidnovic
80 Edgecumbe Drive
St. Paul, MN 55115

TELEDYNE Brown Engineering 1
300 Sparkman Drive
Attn: Vince Reed, Mail Stop 176
Huntsville, Alabama 35807

Telenet Communications Corporation 1
Attn: Robert E. Lipp M/S OP221A
Henry W. Schmauss
12490 Sunrise Valley Drive
Reston, VA 22096

Teleplex United Corporation 1
Attn: David B. Stefan
Sunrise Valley Drive, Suite 311
Reston, VA 22091

Tel Plus Communications, Inc. 1
Federal Systems Division
Attn: Karry B. Fornshill
2722 Merrilee Drive, Suite 300
Fairfax, VA 22031-4408

TENNMARK, Inc. 1
Attn: Donald Prince
475 Metroplex Drive, Suite 106
Nashville, TN 37211

Teqcom, Inc. 1
Attn: Jerry P. Keilsohn
326 N. Stonestreet Avenue
P. O. Box 1526
Rockville, MD 20850

The Computoll Group, LTD. 1
Government Division
Attn: Seth Loonan
171 Madison Avenue-Room 707
New York, NY 10016

The HiTech Engineering Company, Inc. 1
Attn: Edward B. Kolosvary
465 Spring Park Place
Herndon, VA 22070

The NTI Group 1
Attn: Thomas P. McReynolds
3265 Kifer Road
Santa Clara, CA 95051

Titan Systems, Inc. 1
Attn: James W. Coleton
1950 Old Gallows Road, Suite 500
Vienna, VA 22180-3933

T M Systems, Inc. 1
Attn: I. Shuldman
25 Allen Street
P.O. Box 9209
Bridgeport, CT 066091-9209

Tracor Applied Sciences, Inc 1
Analysis & Applied Research Div
Attn: Gary Moss
6500 Tracor Lane
Austin, TX 78725-2050

Tracor Applied Sciences, Inc 1
Analysis Programs Office
Attn: Judy Western
402 Cottonwood Drive
California, MD 20619

Tracor, Inc 1
Attn: Bill Steffan
503A Coliseum Blvd
Montgomery, AL 36109

Trusted Information System
PO Box 45
Glenwood, MD 21738
1

TRW
Integrated Data Systems
Attn: Raleigh E. Guynes
One Space Park R2/1094
Redondo Beach, CA 90278
1

TRW
Attn: Stacy Schultz
1050 Southwood Drive
San Luis Obispo, CA 93401
1

TYCHO Technology Inc.
Attn: Jim Meiggs
PO Box 1716
Bolder, CO 80306
1

Unisys Corporation
Attn: Robert L. Davis/L. Donnelly
7925 Jones Branch Drive
McLean, VA 22102
1

Unisys, Defense Systems
Attn: James E. Healy
P.O. Box 517
Paoli, PA 19301
1

Unisys Corporation
Attn: Keith Prentiss (APO-5th Floor)
8008 Westpark Drive
McLean, VA 22102
1

Verdix Corporation
Attn: Paul Moskowitz
Sullyfield Business Park
14130-A Sullyfield Circle
Chantilly, VA 22021
1

VMX
Attn: Courtney Peterson
Federal Markets Manager
110 Rose Orchard Way
San Jose, CA 95134
1

Wang Laboratories, Inc.
Federal Systems Division
Attn: Vincent D. Corace
7500 Old Georgetown Road
Bethesda, MD 20814
1

Wang Laboratories, Inc. 1
Attn: Ronald R. Trombley M/S 019-L10
Pamela Plitt M/S 019-L40
One Industrial Avenue
Lowell, MA 01851

Western Union 1
Attn: Tom MacLeod
1828 L St. N.W. Suite 1001
Washington, DC 20036

Whitestar Data Systems, Inc 1
Attn: Robert Skerstonas
25655 Springbrook Avenue
Building 8
Saugus, CA 91350-2562

W. P. L. Inc. 1
Attn: Warner Lombardi
P.O. Box 668
Hermosa Beach, CA 90254-0668

Xerox Special Information Systems 1
Attn: Dan R. Davis
1616 North Ft. Myer Drive 16th Floor
Arlington, VA 22209

Yeomans Networking Services 1
Attn: R. D. E. Yeomans
63 Oakridge Blvd.
Nepean, Ontario
Canada K2G2T7

Zenith/Inteq 1
Attn: David Garvis or Harry M. Bacheler, Jr.
13860 Redskin Drive
Herndon, VA 22071

D.3 Other Distribution.

CENTRAL INTELLIGENCE AGENCY

CIA 1
Attn: Code SAN-L (Ms. Curwen)
Washington, D.C. 20505

U.S. DEPARTMENT OF COMMERCE

National Institute of Standards and Technology 1
Institute for Computer Sciences and Technology
Attn: K. Mills, TECH/B217
Gaithersburg, MD 20899

MEDIA

Government Computer News 1
Attn: Neil Munroe
1620 Elton Road
Silver Springs, MD 20903

A Critical Analysis of the X.400 Model of Message Handling Systems

Marten van SINDEREN
and Evert DORREGEEST

Twente University, PO BOX 217, 7500 AE Enschede, The Netherlands, uucp: mcvax!utinul!sinderen

The CCITT X.400 model of store and forward Message Handling Systems (MHS) serves as a common basis for the definition of electronic mail services and protocols both within CCITT and ISO. This paper presents an analysis of this model and its related recommendations from two perspectives. First the concepts of service, protocol and interface are discussed together with their application to this model; second the positioning within ISO's reference model for Open Systems Interconnection (OSI) is commented on.

Keywords: X.400, Message handling systems, Open systems, Structuring concepts.

Marten J. van Sinderen received his M.S. degree in electrical engineering in 1982 from the Twente University, Enschede, The Netherlands. Since 1982, he has been a member of the Department of Computer Science of the Twente University, working on the functional design of distributed computer systems. His research interests include protocol specification, the use of formal description techniques, network interconnection, and higher level protocols. Van Sinderen is an active contributer to ISO/TC97/SC21/WG6 and WG5 on Open Systems Interconnection.

Evert Dorregeest studied at the Twente University in Enschede, The Netherlands, from 1982 to 1987, obtaining an M.S. degree in computer science. He is presently working in military service at the military computer centre in Apeldoorn, The Netherlands. His research interests include computer networks and electronic mail systems.

North-Holland
Computer Standards & Interfaces 7 (1988) 363–375

1. Introduction

The major impetus for the development of electronic mail systems has been provided by office automation applications. In office environments, electronic mail systems facilitate interpersonal message exchange, both from originator to single recipient and from originator to multiple recipients. Optimal usage in such an environment requires that an electronic mail system should be able to accept messages from a number of information sources (serving the originator) and support the delivery of messages to a variety of information sinks (serving the recipient). Messages are then not restricted to simple text but may contain various information types such as voice, facsimile and graphics. Also, submission and delivery of messages may either be interactive or spooled depending on the mixture of source and sinks.

A number of electronic mail systems have already been implemented. They have, however, often a limited application, being closed corporate systems (DECnet), part of a research network (EARN/BITNET, JANET), vendor-specific, or aimed at single system communities (EUNET/USENET) [4] discusses several such systems and their limitations). The comfort gained through an electronic mail system would be greatly enhanced when the system in not limited to the premises of an organization or constrained by specific implementations.

These user needs, as well as the potential market, are recognized by the CCITT, ISO and ECMA. They are currently making considerable efforts to define office document architectures, office document interchange formats [5], and services and protocols for message handling. These definitions are *abstract* in the sense that they do not rely on any specific coding or system implementation. In this paper we will analyse the message handling services and protocols as defined by CCITT in their X.400 recommendations for Message Handling Systems (MHS) [7]. MHS has gained broad acceptance among user communities and computer manufacturers, and is used as the basis

for ISO's Message Oriented Text Interchange System (MOTIS) [8].

The paper is organized as follows: Section 2 presents the basis architecture for MHS and summarizes the message transfer facilities which can be offered. Section 3 is a short tutorial on the concepts of service, protocol and interface as expedients for structuring communications systems. In Section 4, MHS is explained in more detail and the application of the structuring concepts is analyzed. The discussion is limited to communication aspects of MHS; for example, aspects of authentication, access restrictions and naming directories are not covered here. Section 5 analyses whether the proposed placement of MHS in the Open Systems Interconnection (OSI) reference model, namely on top of the OSI presentation service, yields an economical design. Section 6, finally, summarizes our findings from the previous two sections and presents some concluding remarks.

2. Summary of X.400

2.1 Layering

The X.400 architectural model has two layers (*Fig. 1*). The lower layer is the Message Transfer layer, which is made up of *Message Transfer Agent Entities* (MTAE) and *Submission and Delivery Entities* (SDE). The protocol which governs an MTAE (the communication between two MTAEs) is the message transfer protocol (P1). This protocol is concerned with the store-and-forward transfer of messages. That is, messages are sent from one end- or intermediate system MTAE to another end- or intermediate system MTAE. MTAEs provide storage of messages and can perform certain manipulative actions on them according to their included protocol control information. Forwarding a message may also imply sending it to a number of subsequent MTAEs, instead of one, in order to offer multi-recipient delivery. The protocol governing an SDE (the communication between an SDE and a MTAE) is the submission and delivery protocol (P3). P3 primarily provides a reliable exchange of messages and does not support particular end-to-end electronic mail functions; the messages exchanges are therefore "simple" messages, i.e. they contain the user-supplied information but not the additional protocol control information used, and generated by, P1. P3 is used to provide a distant application process with access to the message transfer functions.

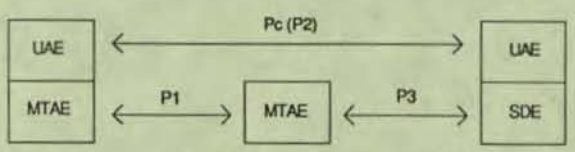


Fig. 1. Layered model of MHS.

The P1 and P3 protocol are both based on the OSI presentation service. Their coordinated operation provides the message transfer service which is available to the entities in the upper layer.

The upper layer is the User Agent layer, and consists of *User Agent Entities* (UAE). A range of protocols (Pc) can be defined at this level, each of them concerned with a particular syntax and semantics of data which is transparently transferred via the message transfer service. To date, only the interpersonal messaging protocol (P2) is defined. As the name suggests, this protocol supports the electronic equivalent of paper-based mail (memo) exchange between human participants.

2.2 Message Transfer Facilities

The message transfer service enables a UAE to submit messages destined to one or more recipient UAEs. If a message cannot be delivered, the originating UAE will normally be informed about this fact. The service is not connection-oriented: submission of data takes place without any previous interaction with the other side being required. The message transfer protocol can perform the following functions, among others, on request of an originating UAE:

1. notification of successful delivery of a message, or prevention of notification in case of non-delivery;
2. conversion of the encoded information type (see *Note*) on a message as specified by the UAE, or prevention of any conversion (otherwise, the message transfer protocol may optionally perform type conversions to enable delivery of a message);

   Note: An encoded information type is a particular encoding for instances of an abstract data type defined, or implied, by an application (e.g. codings used for

telex, teletex, videotex, facsimile, document interchange, etc.). The conversion mentioned thus concerns a conversion between codings of instances of possibly different, but "close", abstract data types (in case of different abstract data types loss of information may occur).

3. deferring delivery of a message until a specified date and time has elapsed;
4. returning the content of a submitted message to the originator in case it could not be delivered;
5. performing the transfer of a message in an urgent or non-urgent fashion;
6. disclosure of other recipients to each recipient UAE upon delivery of a multi-recipient message;
7. delivery of a message to an alternate recipient when the actual recipient UAE is not accessible;
8. probing the transfer and delivery of a (pseudo-) message as specified by the UAE.

In addition a recipient UAE can request:

9. holding messages destined to it, thus deferring their delivery, on certain specified criteria.

The primitives and some of their associated parameters, by which the above facilities can be requested, are discussed in Section 4, together with the supporting protocol structures and elements.

3. Architectural Concepts for Structuring a Communication System

Layering is one of the basic structuring techniques used in describing the communication functionality in distributed systems. It is applied in all modern network architectures to control their complexity and to achieve independency of logically unrelated functions. Also the MHS model makes use of this structuring technique.

Layering is based on the concepts of service, protocol and interface. Since we base our analysis of MHS on these concepts, we need a common understanding of them. The following descriptions are believed to be in line with the OSI reference model [9,10].

3.1 Service

Peer users of a distributed system communicate with each other by using their common intermediate – the distributed system – according to certain strict rules. This usage consists of different types of interactions between a user and the underlying system during which parameter values are established to which both the user and the system can refer. The elementary interactions (service primitives) possible between a user (service user) and the distributed system (service provider), their relevant parameters, and their relation to any other such interactions are defined by a *service*.

A service defines the external view of a system, as can be observed by its users. Actually, this *observational behaviour* is what really matters to the users: to define further interactions on top of the system they need not know the internal structuring and functional complexity of the underlying system. The definition and representation of service primitives should be consistent with this view; thus:

- a service primitive expresses useful interactions in the light of communication (i.e. interactions with only local repercussions should be omitted in a service definition). Note that spontaneous actions internal to the provider may also result in the execution of service primitives;
- the parameters of a primitive indicate what is relevant for both user and provider; information only relevant to the service users is transferred in a "transparent" data parameter.

The boundary between a service provider and a service user, where they can execute primitives is called a service access point (SAP). Since this boundary is a conceptual one and may be internal to a real world system, service primitives must be defined in such a way that their implementation is not constrained. This means that their definition is at a *high(est) level of abstraction*.

A more profound discussion of the service concept and its importance in the design of protocols can be found in [12].

3.2 Protocol

As mentioned above, a service does not define how some externally observable behaviour is achieved. This is defined by a protocol. A *protocol* defines the rules for exchanging and manipulating messages (protocol data units, PDUs), with an agreed format and coding for control information, between protocol entities; not to forget, it also relates the service primitives with the PDUs to make the external effects of its functioning clear.

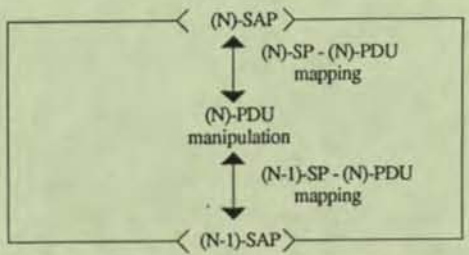


Fig. 2. Representation of a (N)-protocol entity (SP: service primitive; PDU: protocol data unit).

Service and protocol definitions can be applied *iteratively* to the design of distributed systems, as is illustrated by the OSI model. In a layered architecture an (N)-protocol is based on an (N-1)-service, and their composition provides a behaviour equal to that defined by an (N)-service. In this case, the protocol defines as well the relation between its PDUs and the service primitives of the underlying service.

Fig. 2 shows the representation of an (N)-protocol entity as an abstract machine performing mappings and manipulations according to the (N)-protocol. From the service discussion we know that an (N)-PDU is always represented in a data parameter of an (N-1)-service primitive, since its interpretation should be restricted to the (N or higher level)-protocol entities.

3.3 Interface

The local ordering of service primitives at a SAP and the interdependencies between, and restrictions on, their parameter values are described by an *abstract interface* (an abstract interface definition is therefore part of a service definition). An interpretation which is more often associated with the term interface is that of an *implementation description* of an abstract interface; we call this a *real interface*. In designing the real interface between a user and its service provider it may well turn out that the physical distance between the two causes such problems that further protocol engineering is required. The service and protocol concepts can then again be used for structuring purposes; in fact they can be *recursively* applied at different levels of abstraction. In this case, recursive application to an abstract interface yields a set of "interface" services and "interface" protocols.

4. X.400 Services and Protocols

We will now return to MHS. It is our objective to analyse the modeling of electronic mail functions in MHS and to investigate to what extent the X.400 recommendations are suitable prescriptions for "open systems interconnection". The latter means that we demand a general-purpose, *implementation-independent*, description, which leaves implementation freedom where possible and restricts implementations where necessary to allow interconnection and interworking of heterogeneous systems.

4.1 Message Transfer Layer (X.410, X.411)

Table 1 lists all primitives which have been defined for the message transfer service. The primitives are grouped on basis of their partake in certain activities. We can observe that some activities are *local*, i.e. they do not involve interactions which are *remote* to the initiator of the activity.

Non-local, or global, activities involve two or more users in different systems, and imply the coordinated behaviour of these users. The minimum coordination is defined by the service which is provided by the underlying distributed system. Local activity involves only one user (and the underlying system); there is no need for coordination, according to some service definition, with another user. In *Table 1* only "transfer" is considered as a global activity. The "transfer" primitives are therefore the relevant service primitives for the message transfer service, discussed in Section 4.1.1. Section 4.1.2 discusses the message transfer protocol, restricted to the support of the "transfer" interactivity.

"Local" and "global" are, of course, relative notions. We can take a closer look at a local interactivity and may find that this, too, involves several distinguishable entities (e.g. representing a workstation, channel and host) whose interactions can be described in terms of service and protocols, thus introducing a new level of locality. In Section 4.2.3 we will discuss the message transfer interface, where we consider the other activities mentioned in *Table 1*, but also reconsider the "transfer" activity.

Standardizing the local activities of *Table 1* is useful when a user agent and its message transfer agent fall under different implementation authori-

Table 1
Message
ind = in

Primitiv

transfer
SUBMIT
DELIVER
PROBE
NOTIFY

local log
(UAL)LO
(MTL)LO
LOGOFF

access m
(UAL)CH
PASSWO
(MTL)CH
PASSWO

transfer
REGISTE

(UAL)CO
(MTL)CO

local tra
CANCEL

ties a
recom
pleme
alone
an ad
definit
and d
tribute
to-end
the X
differe

SUBMIT
SUBMIT

NOTIFY

Fig. 3. T
one rec

Table 1
Message transfer service primitives in X.411 (req = request, ind = indication, rsp = response, cnf = confirmation).

Primitive	Types	Function
transfer:		
SUBMIT	req, cnf	submission of message
DELIVER	ind	delivery of message
PROBE	req, cnf	submission of probe
NOTIFY	ind	notification of (non) delivery of message or result of probe
local logon / logoff:		
(UAL)LOGON	req, cnf	user logon to system
(MTL)LOGON	ind, rsp	system logon to user
LOGOFF	req, cnf	logoff by user
access management:		
(UAL)CHANGE-PASSWORD	req, cnf	change of user's password
(MTL)CHANGE-PASSWORD	ind, rsp	change of system's password
transfer restrictions management:		
REGISTER	req, cnf	registration of user's receipt restrictions
(UAL)CONTROL	req, cnf	change of receipt restrictions
(MTL)CONTROL	ind, rsp	change of system's acceptance restrictions
local transfer annul:		
CANCEL	req, cnf	cancel request for submitted message

ties and are physically separated. In the X.400 recommendations it is recognized that a user-implemented UAE can be incorporated in a stand-alone workstation which must then interwork via an administration-supplied MTAE. This led to the definition of a separate protocol, the submission and delivery protocol. The definition of the distributed interface primitives and those of the end-to-end service are distinguished here, contrary to the X.411 recommendation, since they concern *different levels* of abstraction.

4.1.1 Message Transfer Service

The message transfer service enables the transfer of messages and probing the transfer of messages, as illustrated by the simplified time diagrams in *Fig. 3*.

Submission of a message is initiated by a SUBMIT request and is locally confirmed by a SUBMIT confirmation. Facilities (1) through (7), listed in Section 2.2, can be requested in the SUBMIT request by setting appropriate parameters. (Some of these facilities are essential – they must be provided when requested – while others are additional – they may be ignored by the system). Provided that the SUBMIT confirmation indicated "success", zero, one or more deliveries may occur by means of DELIVER indications. Depending on the requested facilities, the originating user agent may be informed of successful or unsuccessful deliveries by means of NOTIFY indications.

Probing whether a specified message can be delivered to one or more user agents, is requested in a PROBE request. Again, this request is locally confirmed. The result of this request will be reported back to the originating user agent in one or more NOTIFY indications.

A NOTIFY indication may report on several (would-be) deliveries of a single issued (pseudo-) message. This is only possible when the reports were generated by the same MTAE and the same type conversions were performed on each of the associated message copies.

Analysis: The following comments can be made w.r.t. the message transfer service description in X.411:

- the SUBMIT handshake is described with unnecessary detail; it can be represented as a *single* abstract interaction without degrading the service definition. This comment needs some further explanation.

  The SUBMIT confirmation seems to be intro-

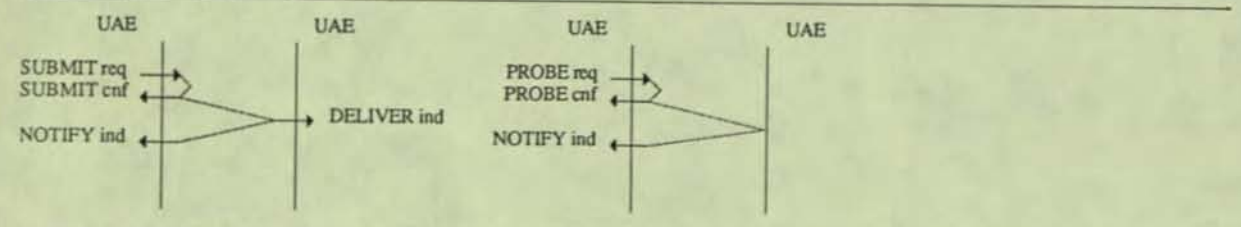


Fig. 3. Time sequence diagrams for transferring a message (with notification of delivery) and probing the transfer of a message. Only one recipient is shown.

duced for two reasons:

1. it takes into account the fact that implementations are subject to failures and represent finite capacities; therefore, a local confirmation of a submitted request can be used to provide certainty about the acceptance of the request;
2. it is used to define a flow of information which is from provider to user, as opposed to that in the corresponding request.

We recall, however, that a service primitive should be defined at the highest possible level of abstraction, not showing details which have only local relevance. Further, the direction associated with a primitive merely indicates the main flow of information [10]; parameter values associated with a primitive may be passed in either direction as appropriate for the primitive. A request for a service which is not acceptable for some local reason is considered as an unsuccessful interaction; such interactions should *not be visible* in the service. Once all parameter values have been established in a primitive execution, the primitive has completed successfully. After this, the provider may report on its inability of progressing the request or on the successful performance of the requested service. Both aspects are already modeled by the NOTIFY primitive.

- the PROBE handshake can be *omitted* completely in the service definition. The reason for this is that a PROBE request will never cause any interactions with a remote user agent, hence there is no need for coordination between users. On the other hand, interworking of MTAEs is required for fulfilling such a request. A protocol element defining this interworking can be considered as part of a management protocol; accessing its functions is a local matter.
- the *relation* between primitives (as in *Figure 3*) is poorly described in the service definition. Although this relation can easily be derived in this case, making it explicit in the service is generally useful to get a quick understanding of the externally visible effects of the service provider. For example, it would have shown which primitives have remote effects and which have not, and how the provider may influence the remote effects (loss of data, manipulation of parameters). For a full understanding of the relation between message transfer primitives we are now obliged to study both the message transfer protocol and the presentation service.

4.1.2 Message Transfer Protocol

An MTAE executing the message transfer protocol is modeled as consisting of three subentities: the message dispatcher, the association manager, and the reliable transfer server. The *message dispatcher* performs the relaying of messages, generation and forwarding of delivery reports, and information type conversion. The *association manager* controls the establisment and release of associations between MTAEs. The role of the *reliable transfer server* (RTS) is to provide and maintain the associations requested by the association manager, to release them when requested, and to perform the transferring of PDUs on basis of available associations.

The service primitives and PDUs which are used by these subentities are shown in *Table 2*. The association manager employs only the OPEN and CLOSE primitives for requesting a new or releasing an existing association, on basis of local management information; PDUs are not defined for these purposes. The message dispatcher employs two types of PDUs: the *user* MPDU, carrying a message submitted by a user agent for delivery, and the *service* MPDU which carries either a probe or a delivery report (MPDU stands for message PDU). MPDUs are mapped onto the user data parameter

Table 2
Service primitives and PDUs used by the association manager, message dispatcher and reliable transfer server.

Association manager and message dispatcher			Reliable transfer server
Primitive	PDU	Primitive	Primitive
		OPEN	CONNECT
SUBMIT	user MPDU	CLOSE	RELEASE
DELIVER		TRANSFER	DATA
PROBE	service MPDU	TURN-PLEASE	TOKEN-PLEASE
NOTIFY		TURN-GIVE	TOKEN-GIVE
		EXCEPTION	ACTIVITY-START
			ACTIVITY-INTERRUPT
			ACTIVITY-RESUME
			ACTIVITY-END
			ACTIVITY-DISCARD
			SYNCHRONIZE-MINOR
			U-EXCEPTION-REPORT
			P-EXCEPTION-REPORT
			U-ABORT
			P-ABORT

of TRANSFER primitives. The message dispatcher may further use TURN-PLEASE and TURN-GIVE primitives to manage the turn for sending MPDUs in case the available association(s) is (are) two-way-alternate. It receives an EXCEPTION indication primitive carrying a previously submitted MPDU when the transfer of that MPDU could not be performed in the specified *transfer time* (a parameter of the TRANSFER request). After receipt of an EXCEPTION indication, rerouting the associated message may be attempted, or a service MPDU with a negative delivery report is generated.

The RTS uses the OSI connection-oriented presentation service, and through this the session service [11], to reliably transfer the user data specified in TRANSFER requests. A user data parameter is called here an APDU (application PDU); this is not an explicitly defined PDU. No PDUs are defined for the RTS.

Each APDU transfer constitutes a single *session activity*. After the start of a session activity, the APDU can be transferred in one or more presentation SDUs, each one submitted through a DATA request. Multiple DATA requests per APDU can only be used when *checkpointing* was agreed during connection setup. An APDU is then sent in parts, where each part is separated from the other through the insertion of a checkpoint. All checkpoints must be confirmed by the recipient RTS entity; the maximum number of unacknowledged checkpoints which may be outstanding during a session activity is indicated by the *window size* negotiated at connection establishment time. This is shown in *Fig. 4*. In case problems occur during the transfer of an APDU, which can be locally detected or signalled through U/P-EXCEPTION-REPORT or U/P-ABORT primitives, the sending RTS entity will attempt to *recover* the transfer with several possible actions, starting from the last confirmed checkpoint. We will not elaborate on this (note that several corrections and additional explanations w.r.t. RTS, especially covering recovery, are described in [6]). If the transfer cannot be completed within the allocated transfer time, the activity is normally discarded (ACTIVITY-DISCARD) and an EXCEPTION indication to the message dispatcher is generated by the sending RTS entity.

Analysis: It is typical that the definition of the message transfer protocol (that is, P1) does not mention the message transfer primitives which we characterized as being local. This results in an inconsistency between the protocol and service definition. We can make the following further remarks:

- the content of a message, i.e. user data, is not always transferred *transparently* by the message transfer protocol. For example, the message dispatcher may perform information type conversion of the user-provided content of a message. The conversion is not restricted to changing the representation of the user data, but may also include the translation to another data type.
- the transfer time parameter in a TRANSFER request primitive has only *local significance* and therefore does not have to be represented. The transfer time is commonly agreed by the mes-

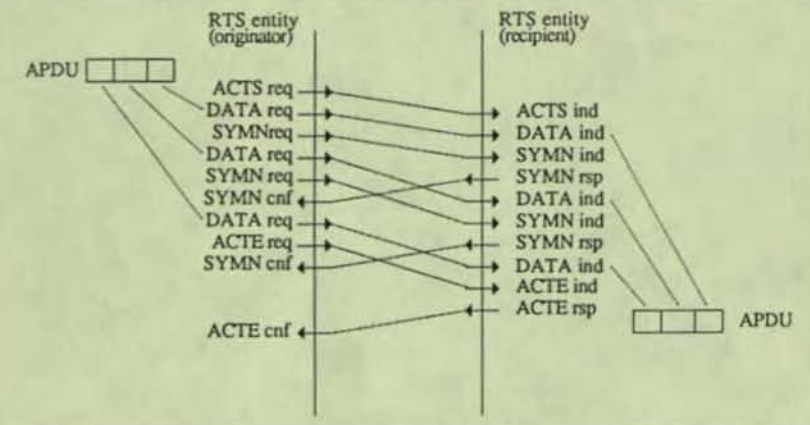


Fig. 4. Use of the presentation/session service for the transfer of an APDU in case checkpointing is used (here in 3 parts; checkpoint size is greater than zero and window size is at least two). (ACTS = ACTIVITY-START, ACTE = ACTIVITY-END, SYMN = SYNCHRONIZE-MINOR).

sage dispatcher and the local RTS entity at the sending side but is not visible at the receiving side.
- RTS defines a particular structure of the user data parameter of the presentation/session CONNECT primitives for transferring RTS-specific information, such as checkpoint size and window size. Since the OSI presentation service does not refer to this information, it seems that in this way an implicit RTS connect (-acknowledge) PDU is defined.
- the *correlation* between OPEN and CLOSE primitives is not described. CLOSE primitives carry no parameters: how then does the association manager indicate that it wants to delete an association with a particular MTAE? It is also not clear how the TRANSFER/TURN/EXCEPTION primitives are correlated with an association.

4.1.3 Message Transfer Interface

The possible distribution of a message transfer interface is represented in the X.400 recommendations as shown in *Fig. 5*. Two "concatenated" protocols, viz. the message transfer protocol (P1) and the submission and delivery protocol (P3), are used to provide the message transfer service. It should be noted that the P3 protocol is said to define the communication between an SDE and an MTAE, and not between two SDEs. The SDE functionality is thus "hidden" in such a MTAE. Another modeling of a distributed message transfer interface, consistent with the discussion in Section 4.1.1, is shown in *Fig. 6*.

The submission and delivery protocol is defined with the help of a general framework for interactive protocol definitions, referred to as *remote operations*. This framework defines four principal PDU data types, called OPDUs (for operation PDUs): Invoke, ReturnResult, ReturnError, and Reject. An Invoke OPDU specifies an operation; an entity sending an Invoke OPDU is said to

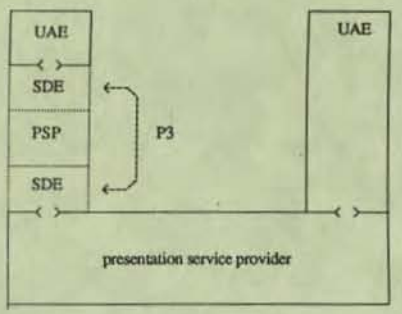


Fig. 6. Another view on "submission and delivery" (PSP: presentation service provider).

invoke a remote operation which must be performed by the recipient entity. Depending on the outcome of the operation, the recipient may return a:
- ReturnResult, reporting on the result of the operation when it was successful; or
- ReturnError, reporting on the error which occurred during the performance of the operation.

A Reject is sent on receipt of any of the Invoke, ReturnResult or ReturnError OPDUs when the OPDU was malformed and could not be processed for this reason.

For any specific protocol which makes use of the remote operations definition, hence also for the submission and delivery protocol, *particular operations* (and related results and errors) have to defined which are fit for that protocol. The submission and delivery protocol defines for all primitives listed in *Table 1*, except for the (UAL/MTL)LOGON and LOGOFF primitives, the associated operations. The so defined message transfer "interface" PDUs are transferred as user data on TRANSFER primitives of the RTS service, as described in Section 4.1.2. The (UAL/MTL)LOGON and LOGOFF primitives are directly mapped onto the RTS OPEN and CLOSE primitives.

Analysis: When we decompose an abstract in-

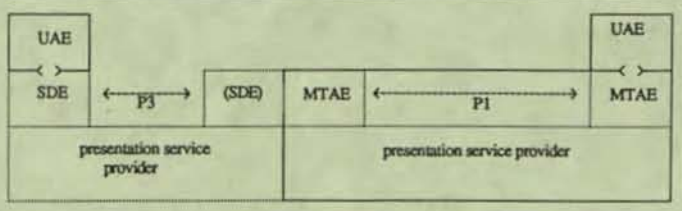


Fig. 5. "Submission and delivery" as modeled in MHS.

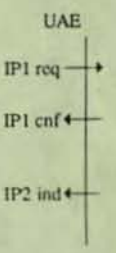


Fig. 7. Tir face of tw ing a sing IP2, respe

terface the tim service, primitiv shows based service vider-c tives. F a mess concluc
- since fines MTAI two the very that not req sion elem

(SUBMIT req

(SUBMI cnf

Fig. 8. betwee

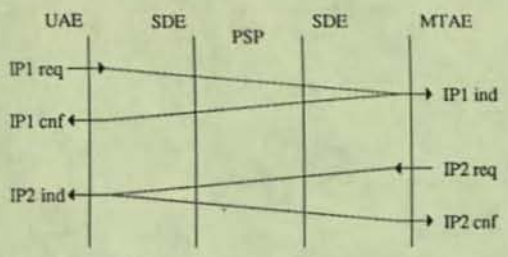


Fig. 7. Time sequences at a distributed message transfer interface of two (arbitrary) UAE-MTAE interactions, each one replacing a single service interaction (a request, IP1, and indication, IP2, respectively). (Internal mappings are not shown.)

terface (or SAP, represented by a vertical line in the time sequence diagrams of *Fig. 3* and *4*) of a service, we also have to decompose the service primitives which occur at that interface. *Fig. 7* shows a time diagram for such a decomposition, based on *Fig. 6*, and illustrates how a single service primitive can be represented as a "provider-confirmed" sequence of "interface" primitives. *Fig. 8* shows the specific case of submitting a message. On basis of these Figures we can conclude that:

- since the submission and delivery protocol defines the communication between an SDE and a MTAE (with embedded SDE), and not between two SDEs, the decomposition, or refinement, of the abstract message transfer interface is not very clear. It is for this reason, for example, that the (SUBMIT req) ind, shown in *Fig. 8*, is not explicitly specified, while the (SUBMIT req) req and the (SUBMIT req) cnf are. Similar omissions can be observed for the other interface elements. For the DELIVER and NOTIFY interface elements even two interface primitives, viz. the request and confirmation, are not described. The latter omission has important consequences as explained below.
- the DELIVER and NOTIFY interactions are not correctly described. Probably because there are no request and confirmation interface primitives specified, also the ReturnResult PDUs for the deliver and submit operations are not defined. Hence, in this case the acknowledgement of an operation is not only hidden at the invoker side, but completely omitted. This is in contradiction with *Fig. 7*.

The submission and delivery protocol relates to two sets of interactions. One is the set of interactions which are part of the service interactions described in the message transfer service, viz. SUBMIT, DELIVER and NOTIFY. The other concerns local activities, i.e. activities which involve no remote interactions (from the point of view of a message transfer service user) but only interaction between an UAE and its MTAE. This leads to the following comment:

- the submission and delivery protocol defines two sets of interactions which support different applications. These sets of interactions can be independently defined.

4.2 Interpersonal Messaging User Agent Layer (X.420)

Two PDU types are defined at this level: the intermessaging UAPDU and the status report UAPDU (UA for user agent). An intermessaging UAPDU consists of a heading and a body. The body contains one or more body parts, which can be looked

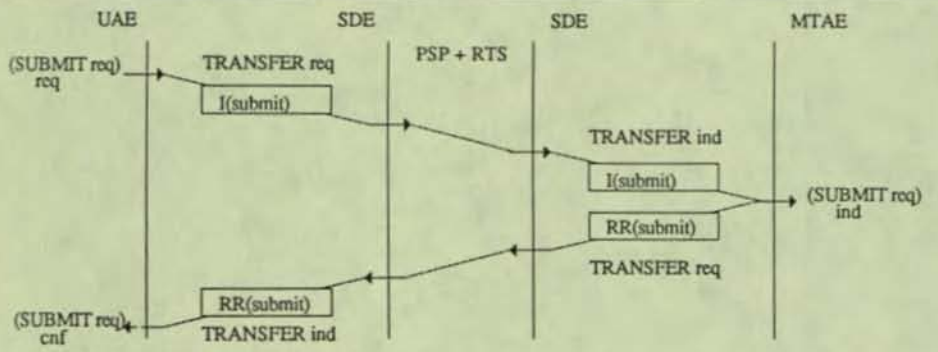


Fig. 8. Time sequence diagram for successfully submitting a message across a distributed message transfer interface (SUBMIT req, between brackets, indicates the original service primitive; I = invoke, RR = ReturnResult).

at as independent (sub)messages, with always an indication of the *body part type* (telex, teletex, voice, etc.). The heading always contains a *message identifier*, and optionally other interpersonnal messaging PCI. A status report UAPDU is used as an acknowledgement of the receipt or non-receipt of an intermessaging UAPDU; it therefore always carries the message identifier of the message to which it refers. Both PDUs are transferred by means of the SUBMIT/DELIVER service elements of the message transfer service. The interpersonal messaging protocol (P2) can provide the same facilities as listed in Section 2.2, on basis of the message transfer service, and some other facilities, including the following (a recipient interpersonal messaging service user is here shortly termed recipient):

- sending a message to one or more blind copy recipients, i.e. recipients which are not disclosed to the primary and secondary ("normal" copy) recipients specified in the request;
- notification of receipt or non-receipt (non-receipt means: receipt by the remote UAE, but not delivered to the intended recipient) of a message;
- delivery of messages which were auto-forwarded by the intermessaging protocol;
- conveyance of information as optional intermessaging UAPDU heading parameters, some of them on a per-message basis (the same information applies to all recipients in case of multi-recipient delivery), others on a per-recipient basis;
- transfer of a message consisting of several parts of possibly different types.

In addition, other, *management-like* functions are performed by UAEs which do not require the exchange of either of the above UAPDUs. Some of these functions concern the local access to the message transfer service and are not directly controlled by the interpersonal messaging service users. These functions are based on the use of the (UAL/MTL)LOGON, LOGOFF, REGISTER, (UAL/MTL)CHANGE-PASWORD, and (MTL)CONTROL. The other functions can be controlled by the interpersonal messaging service users; they are based on the use of the CANCEL, PROBE, and (UAL)CONTROL primitives.

Analysis: The following comments can be made:

- the interpersonal messaging *service* is poorly described. The service is not modeled by means of interrelated service primitives. Instead, the various service elements are outlined by indicating the effect of exchanging UAPDUs and the direct use of message transfer service (interface) primitives. The information which is exchanged in service interactions is not explicitly described, but must be derived from the UAPDU definitions or the message transfer service primitive definitions.
- the interpersonal messaging protocol describes the UAEs' engagement in both local and global activities. The same comments apply here as in Section 4.1.
- notification of successful delivery, provided by the message transfer service, is passed to the originating user of the interpersonal messaging service. This does not seem a very effective use of this service, as it only indicates a *probable* delivery to the peer user. Successful delivery can only be acknowledged by the receipt notification service element.
- some UAPDU heading parameters are not used by the interpersonal messaging protocol but have only relevance for the interpersonal messaging service users. This is the case with the optimal parameters which, if used, must be conveyed on a per-message basis: no interference of the interpersonal messaging protocol w.r.t. this information is required. It can therefore probably better be specified as a body part with an appropriate body part type.
- summarizing, it appears that the P2 protocol adds little value to the message transfer service. A part of the defined UAE operation concerns local management and does not require the cooperation with a peer entity; hence, such operation should not be described as part of the P2 protocol. Other definitions accrue from the need to distinguish between several user-relevant parameters, whose semantics must be correctly transferred (some of them only to a subset of the specified recipients) together with the actual message. Instead of mapping these parameters directly onto UAPDU parameters, a better design option seems to combine them in (recipient-bound) user data parameters with defined abstract syntaxes. In that case, the presentation service enables the correct interpretation of such data by the recipient peer user, while the data structure is not visible in the protocols supporting the users' interaction.

5. M

Th
of MI
and
catio
tion
prese
funct
not c
ity i
centr
Th
and
pend
initia
of th
class
(or t
Th
relia
enab
conn
ABOI
cate
since
class
prot
exce
crash
whe
the
Th
servi
with
turin
user
Ha
dant
form
of d
perf
With
of a
tain
tion
not
geo
that
mak
sync
case

5. Message Handling within OSI

This section is concerned with the integration of MHS in OSI, where the message transfer service and protocol together constitute another *application service element* [2], based on the presentation service. Our aim is to investigate whether the presentation service is well utilized, and whether functions of the presentation service provider are not duplicated. In this context the RTS functionality is most suspicious; we will therefore concentrate on this functional part of MHS.

The OSI transport service provides a *reliable* and cost-optimized data transport capability. Depending on the quality of service requested by an initiating transport service user and the reliability of the underlying network, a suitable protocol *class* is negotiated between two transport entities (or the transport connection is refused).

The recovery procedures of RTS enhance the reliability provided by the transport service by enabling survival of protocol malfunctioning and connection losses (reported by EXCEPTION and ABORT primitives, respectively). They also duplicate part of the transport protocol functionality, since RTS is based on the assumption that only classes 0 and 1 can be negotiated by the transport protocol. In an OSI environment, only recovery of exceptional cases (network partitions, application crashes) should be left to an application protocol, whereas "normal" recovery can be delegated to the transport service provider.

The OSI session service enriches the transport service with the capability of exchanging data without imposing *length restrictions* and of *structuring* the communication (dialogue) between the users of the service.

Hence, checkpointing appears to be a redundant RTS functionality. The session protocol performs segmenting and reassembly to offer transfer of data of any length (recovery of data segments is performed by the transport service provider). Without checkpointing, and with the introduction of an RTS data- acknowledge PDU to obtain certainty about the acceptance of a data unit, selection of the activity management functional unit is not required any more. This might be advantageous for some implementations, given the fact that none of the current OSI application protocols makes use of activity services. Also the minor synchronize functional unit is not required in that case.

The OSI presentation service provides independence from the local *data representation* (encoding) in different systems involved in a communication.

RTS makes minimal use of the presentation service. On the other hand, considerable efforts were made by ISO to allow the conveyance of X.400 data by the presentation protocol. The reason for this is that X.409, which is the notation used for the definition of the X.400 PDUs, slightly diverges from the abstract syntax notation used by ISO. A universal treatment of data should be made possible in the presentation layer. The information type conversion function of the message transfer protocol also gives rise to some criticism. From an OSI point of view, representation of user data should be a concern of the presentation layer, and conversion from one to another datatype should be considered as an information processing task pertinent to a level above that which provides transparent transfer of the associated data, that is, the message transfer layer.

The entities which make up the OSI application layer are subdivided into entity parts, called application service elements (ASE). Corresponding ASEs communicate according to a user-defined or standardized application protocol, where the latter may be either *application-specific* or *common* to most applications.

When MHS is to form a separate ASE in the application layer structure, it must also allow correct interworking in the presence of other ASEs. Interworking of "composite" application entities is still under study in ISO TC97/SC21. As a final remark, it can be noted that the use of naming directories is currently described as an integral part of MHS. ISO defines separate service elements which allow common access to such directories. If this work is completed, other ASEs will probably use the offered capability and include appropriate references to the relevant directory services.

6. Conclusions

Analysis of the X.400 recommendations gave rise to various points of criticism. Since the analysis was performed from two perspectives, two categories can be distinguished:

1. Misinterpretations of the architectural concepts

of service, protocol and interface. Among others, the following points are raised:

- Local and remote interactivities are mixed in the message transfer service definition.
- The service primitives used in describing the remote interactivities are not defined at the highest possible level of abstraction.
- P1 (message transfer protocol) is "concatenated" with P3 (submission and delivery protocol). In fact, P3 is a protocol which defines the interactions at the abstract interface between a UAE and a MTAE. Some of these interactions are a decomposition of the message transfer service primitives, which in turn define part of a remote interactivity. Others have no relation with message transfer service primitives since they have no corresponding remote effects.
- The decomposition of message transfer service primitives described by P3 is incomplete.
- The interpersonal messaging service is poorly defined. The protocol functionality which is added by P2 (interpersonal messaging protocol) is minimal.
- Transparent transfer of user data is not always performed by P1 and P2, contrary to what is claimed by the corresponding service or what could be expected from basic structuring principles.

It should be noted that these misinterpretations do not necessarily lead to wrong implementations. However, they blur the architecture and consequently impair the advantages of good structuring. For example, modelling errors may unnecessarily restrict implementations and may hamper correctness proofs; furthermore, they may lead to more complex implementations which are more difficult to test and to maintain.

2. Overdesign of the message transfer protocol as a consequence of disregarding lower layer functionality. In particular, the following observations are made:

- The RTS recovery procedures can be simplified given the service offered by the transport service provider.
- The RTS checkpointing function is redundant since the session service offers normal data transfer without length restrictions. The activity management and minor synchronize functional units are then no longer required for support of message handling.
- The existence of X.400 is visible in the presentation PDU definitions. Although suitable transfer syntaxes must be registrated for X.400 support, handling X.400 user data should not be different from any other user data.

Again, redundancy does not lead to wrong implementations. In this case, the architecture becomes unnecessary complex. It leads to implementation overhead and hence results in excess costs for subscribers to the service. For this reason it can better be avoided.

In addition to this basic criticism, a number of smaller defect have been discovered which were not discussed here. As has been shown in [3], such defects, including ambiguities, points of incompleteness and inconsistencies, can easily be discovered by using a formal description technique in defining the services and protocols. These techniques have the additional advantage of enlightening architectural aspects which remain vague in most informal texts.

It may be clear from the above that the positioning of MHS within the OSI reference model is problematic, in particular because OSI services and protocols are (should be) consistent with the concepts of service, etc. (which is not always the case, see e.g. [1]). In the light of the important application areas of message handling, the necessary adaptions should be agreed as soon as possible.

References

[1] I. Ajubi, M. v. Sinderen: "Design of a CCR Protocol Using a Formal Description Technique," submitted for inclusion in EUTECO '88 post-conference proceedings (North-Holland 1988).

[2] ISO: "Application Layer Structure," DP 9545, TC97/SC21 N1743 Revised, Oct. 1987.

[3] E. Dorregeest: "Analysis and Formal Specification of Electronic Mail," M. Thesis Report No. INF-87-3, Twente Univ., Enschede, The Netherlands, March 1987.

[4] T. Kalin (ed.): *Proc. of the European Telematic Conference (EUTECO), Workshop 1: Message Handling*, Varese, Italy, October 3–6, 1983 (North-Holland, 1983) 125–263, 631–640.

[5] W. Horak: "Office Document Architecture and Office Document Interchange Formats: Current Status of International Standardization," *IEEE Computer*, Oct. 1985, 50–60.

[6] CCITT: X.400-Series Implementor's Guide (Version 3)," COM VII-66-E (also: ISO/TC97/SC21 N1246), April 1986.

[7] CCITT: "Message Handling Systems," Recommendations X.400 ff., Red Book, Vol. 8, Fascicle 8.7, 1984.

[8] ISO: "Information Processing Systems – Text Communications – Functional Description of MOTIS," DIS 8505, TC97/SC18 N604, Feb. 1986.

[9] ISO: "Information Processing – Open Systems Interconnection – Basic Reference Model", IS7498, TC97, 1984.

[10] ISO: "Information Processing Systems – Open Systems Interconnection – Service Conventions," ISO TR8509, 1987.

[11] ISO: "Information Processing Systems – Open Systems Interconnection – Basic Connection Oriented Session Service Definition," ISO8326, 1987.

[12] C.A. Vissers, L. Logrippo: "The importance of the Service Concept in the Design of Data Communication Protocols," *IFIP WG6.1, 5th Int. Workshop on Prot. Spec., Ver. and Testing*, Toulouse-Moissac, France, June 10–13, 1985 (North-Holland, 1986) 3–17.

Volume 7, Number 4, 1988
ISSN: 0920-5489
CSTIEZ 7(4) 333-444 (1988)

COMPUTER STANDARDS & INTERFACES

LAST ISSUE
OF THIS VOLUME

The International Journal on the Develop
and Application of Standards for Compu
Data Communications and Interfaces

North-Holland

ISDN and the Move to Integrated Communications – An Introduction

Michael D. SZPAK

Nixdorf Entwicklungsgesellschaft für Kommunikationstechnik mbH, Wittestraße 30c, 1000 Berlin 27, Federal Republic of Germany

The article provides an overview of the CCITT I-Series of Recommendations on ISDN as part of the current trend towards integrated communications. Attention is primarily focussed on the user-network interface. Descriptions of the ISDN reference configuration, the basic and primary rate user access structures, and the D-channel signalling protocol are provided. The article closes with a short descussion of the as yet unsolved problems facing the introduction and wide-spread penetration of ISDN.

Keywords: ISDN, User–network interface, Primary access, Basic access.

Michael D. Szpak is a hardware specialist with Nixdorf Entwicklungsgesellschaft für Kommunikationstechnik (NEK) mbH, a daughter company of Nixdorf Computer AG. He received his B.E.E. degree from the Georgia Institute of Technology in 1981 and was an exchange student at the Technische Universität Berlin in 1981-2. In 1983 he was employed by Krone GmbH as a design engineer working on the BIGFON project. He received his M.S.E.E. degree from the University of Illinois in 1985. Since that time he has been working at NEK in the area of ISDN interfaces and with the EC sponsored RACE program as a member of the Customer Premises Network group in the RACE Definition Phase.

North-Holland
Computer Standards & Interfaces 7 (1988) 349–362

1. Introduction

Over the past decade, there has been a marked increase in the use of the telephone system for more than just voice transfer. Data applications have taken over a growing portion of the telephone network bandwidth.

Despite this trend, the telephone system has remained predominantly analog in its transmission methods, especially in the subscriber loop. This has required the use of modems or alternate (and more expensive) systems, i.e. dedicated networks, for long distance data communications. Furthermore, the implicit bandwidth limitations for analog transmission using modems and the installed wiring has restricted digital transmission to relatively low bit rates on the order of 2400–9600 bits/s.

These and other factors have contributed to the international trend toward ISDN – the Integrated Services Digital Network. This trend would not be possible without standards. The purpose of this article is to provide the reader with a general understanding of these standards together with other important factors affecting the move to integrated communications. It should be pointed out that the author, in striving to provide a general understanding, has found it necessary to omit many of the finer details of ISDN. Readers desiring a more detailed understanding of this complex subject should read the CCITT I-Series Recommendations.

2. What Is an ISDN?

ISDN is a broad concept including switching, network control facilities, interfaces to customer premises equipment, and a defined set of service features and functions. In the I-series Recommendations, the CCITT defines an ISDN as a network that provides end-to-end digital connectivity to support a wide range of services, including voice and non-voice services, to which users have

access via a limited set of standard multi-purpose user–network interfaces.

It should be noted that the CCITT generates Recommendations. As the name implies, recommendations are not binding and national administrations usually reserve the right to make changes in the recommendations for national use. The above definition leaves room for a rather large number of possible implementations and configurations of ISDNs according to specific national situations. Emphasis is placed, however, on the usage of "end-to-end digital connectivity," "a wide range of services," and "a limited set of standard multi-purpose user–network interfaces."

What do these three terms imply for a network? The first, "end-to-end digital connectivity," implies that any application that can represent its information in a digital form and within the limits of the ISDN interface capacity (see Section 5.2) can use the network as a transport medium. Thus modems are no longer required for data communication. Also, digital representation allows the application information transferred by the network to include voice, data, image, and text information without any distinction within the transfer channels. Such a network is service independent – one of the primary objectives of ISDN.

The second term, "a wide range of services," implies the ability of the network to do more than transparently transfer information. The provision of enhanced or value-added services beyond simple telephony is supported by efficient connection to specialized storage and processing centers belonging to either the ISDN network operator or other service/network providers. Examples of such services include electronic mail, facsimile, videotex, music and video distribution.

And lastly, "a limited set of standard multipurpose user-network interfaces," implies that one or two interface types, realized as so-called communications sockets, will be capable of supporting a large number of different types of equipment. This allows service independence at the user-network interface, as well as, terminal portability among different network access points and independent evolution of terminal and network equipment, technologies, and configurations – further objectives of ISDN.

A network may be viewed in any one of several ways. Among these are from the viewpoint of the services provided by the network and their corresponding network capabilities and from the viewpoint of the user connection to the network. The next sections give an introduction to ISDN as specified in the CCITT I-Series Recommendations with emphasis on the defined user-network interfaces and the user view of an ISDN.

3. The CCITT Approach to ISDN Standardization

CCITT has concentrated its standardization efforts for ISDN in three major areas. They are:

a. the standardization of services offered to customers so as to enable services to be internationally compatible (I.200 Series). The standardization of these services will allow the user access to identical services from any ISDN;
b. the standardization of user-network interfaces so as to enable terminal equipment to be portable (I.400 Series). Such interfaces, together with the appropriate terminal equipment, will support any of the services specified in point (a);
c. the standardization of network capabilities so as to enable user-network and network-network interworking in support of points (a) and (b) (I.300 Series).

The I.100 Series presents a description of ISDNs in terms of general principles and evolution. The following points are made:

- An ISDN supports a wide range of voice and non-voice applications.
- These applications include circuit-switched, packet-switched, and non-switched connections and their concatenations.
- The ISDN is an intelligent network providing processing power in support of service features, maintenance, and network management.
- Access to an ISDN will be specified using a layered protocol structure.
- ISDNs are expected to evolve from present day IDNs (Integrated Digital Networks) initially designed to support 64 kbit/s voice services but progressively incorporating additional functions and network features of other dedicated networks, e.g. circuit-switched or packet-switched data networks.
- The evolution will allow the introduction of new services with the same network structure and, at a later stage, switched connections at bit rates higher and lower than 64 kbit/s.

4. The I

The
duced i
and he
(CCITT
to avoi
layer ar
The
the net
control
U-plan
user ap
control

Fig. 1.

4. The Protocol Reference Model

The ISDN protocol reference model is introduced in the I.300 Series. This model is based on, and hence similar to, the OSI Reference Model (CCITT X.200). Layer numbers, not names, are used to avoid confusion between the functionality of a layer and the layer name.

The information flow from end to end through the network is partitioned into two planes: the control (*C*) plane and the user (*U*) plane. In the *U*-plane, user information is transferred from one user application process to another. In the *C*-plane, control information, information which is acted upon within the network for the purposes of network connection control, maintenance, or management, is transferred between protocol end points.

The protocol reference model employs the *U* and *C* planes in its introduction of the generic ISDN protocol block (*Fig. 1*). In the Figure, one may see that the control and user protocol stacks may contain different protocols and are handled separately. This protocol block model is valid for all forms of ISDN equipment throughout the network, although in some cases particular layers may be null. The management portion of the protocol block is responsible for local management aspects such as monitoring the activities of

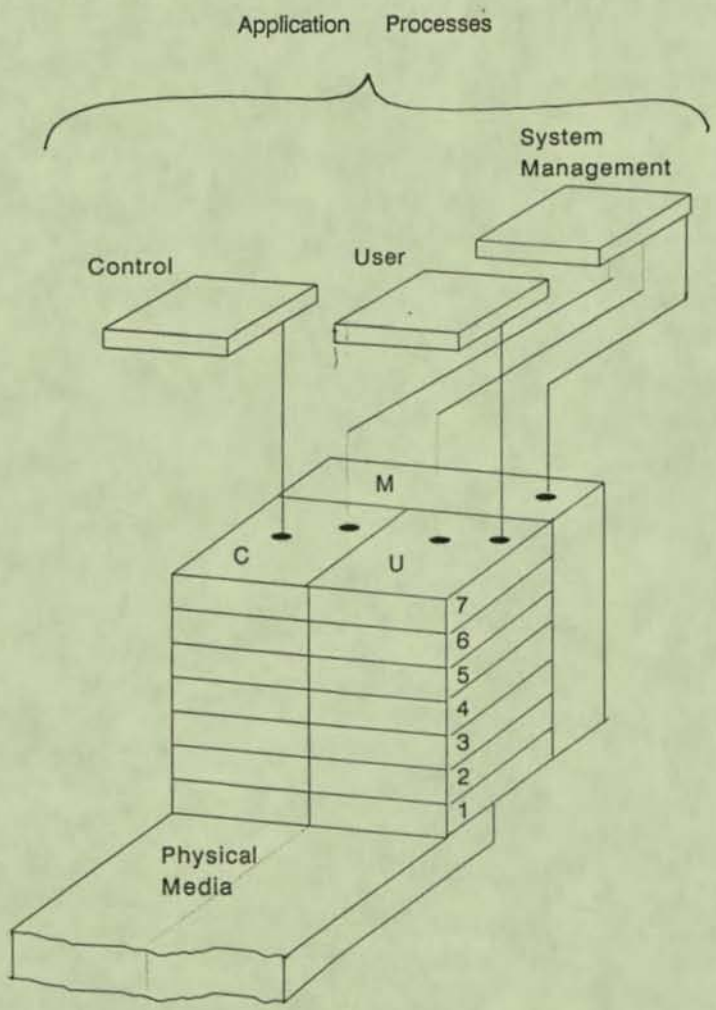


Fig. 1. Generic ISDN protocol block.

the user and control protocol stacks and providing an information exchange mechanism between the *U* and *C* processes.

At the bottom of the protocol stacks is the physical media used to transmit information. This may or may not be the same physical connection for the *U* plane and its controlling *C* plane. At the top of the protocol stacks are the interfaces to the various user, control, and management application processes which are outside of the protocol block. Not shown in *Fig. 1* are the peer protocols whose interactions take place in a layered fashion between different protocol blocks.

5. User–Network Interfaces

The I.400 Series describes a small number of user-network interfaces with the objective of providing maximal flexibility, terminal portability, and service integration in connection to an ISDN.

5.1. The ISDN Reference Configuration

Various physical user access arrangements are defined in terms of reference configurations consisting of functional groups separated by reference points. In different implementations, a reference point may or may not correspond to a physical interface, i.e. more than one functional group may be incorporated into a single piece of equipment. However, physical interfaces that do not correspond to reference points are not considered a topic for consideration by CCITT, e.g. interfaces internal to a PBX implementation of the NT2 functional group.

The general ISDN reference configuration is shown in *Fig. 2*. The physical interfaces defined in the I-Series apply at both reference points *S* and *T*. Other CCITT and non-CCITT interface specifications may be applied at reference point *R*. At the moment, there is no CCITT-defined reference point or physical interface at the transmission line. The telecommunications industry, however, generally refers to this point as the *U* reference point.

Between the reference points are the functional groups. Not all of the functions listed for each functional group need be present. In some physical implementations, an entire functional group may be absent in which case, reference points coincide. The functions of each of the functional groups are listed below.

The NT1 generally performs layer 1 functions, providing the proper physical and electromagnetic termination of the network.

NT1 – Network Termination 1:
- Line transmission termination
- Layer 1 maintenance functions and performance monitoring
- Timing
- Power transfer
- Layer 1 multiplexing
- Interface termination, including multidrop termination employing layer 1 contention resolution.

The NT2 generally performs functions at layers 1, 2, and 3. Examples of NT2 implementations include PBXs, LANs, terminal controllers, or any combination of these.

NT2 – Network Termination 2:
- Layers 2 and 3 protocol handling
- Layers 2 and 3 multiplexing

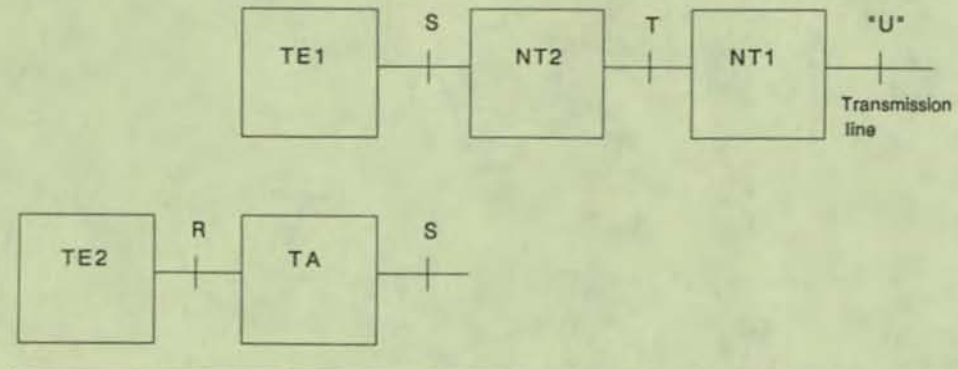


Fig. 2. ISDN reference configuration for user–network interfaces.

Fig. 3.

- Switching
- Concentration
- Maintenance functions
- Interface termination and other layer 1 functions.

The TE generally performs or supports the functions of layers 1 through 7, although not in every case. Examples of TE implementations include digital telephones, data terminals, and integrated workstations.

TE – Terminal equipment:
- Protocol handling
- Maintenance functions
- Interface functions
- Connection functions to other equipment.

There are two categories of terminal equipment:

TE1 – Terminal Equipment type 1: the TE1 interface complies with the ISDN user–network interface recommendations.

TE2 – Terminal Equipment type 2: the TE2 interface complies with a non-ISDN interface specification.

In an ISDN environment TE2 requires the functions of a TA to connect to the network.

TA – Terminal Adaptor: the TA provides the layer functions necessary to adapt the TE2 interface at the *R* reference point to one of the ISDN specified user–network interfaces at the *S* or *T* reference points.

TE1 and the combination of TE2 with TA may be considered functionally identical.

At reference points *S* and *T*, any one of the following systems may be connected:
- Customer terminals
- Customer systems, e.g. PBXs, LANs, or systems providing customer application services
- Private networks.

At reference point *R*, other standardized services, e.g. CCITT X and V Series of Recommendations, may be accessed according to the type of terminal adaptor provided. *Fig. 3* gives examples of some of the possible physical configurations.

A great number of implementations of the physical configurations are possible and several examples are given in *Fig. 4*. Perhaps the two most common realizations to be expected in the long term in a pure ISDN environment are:
- in the residential environment (*Figs. 3c* and *4c*):

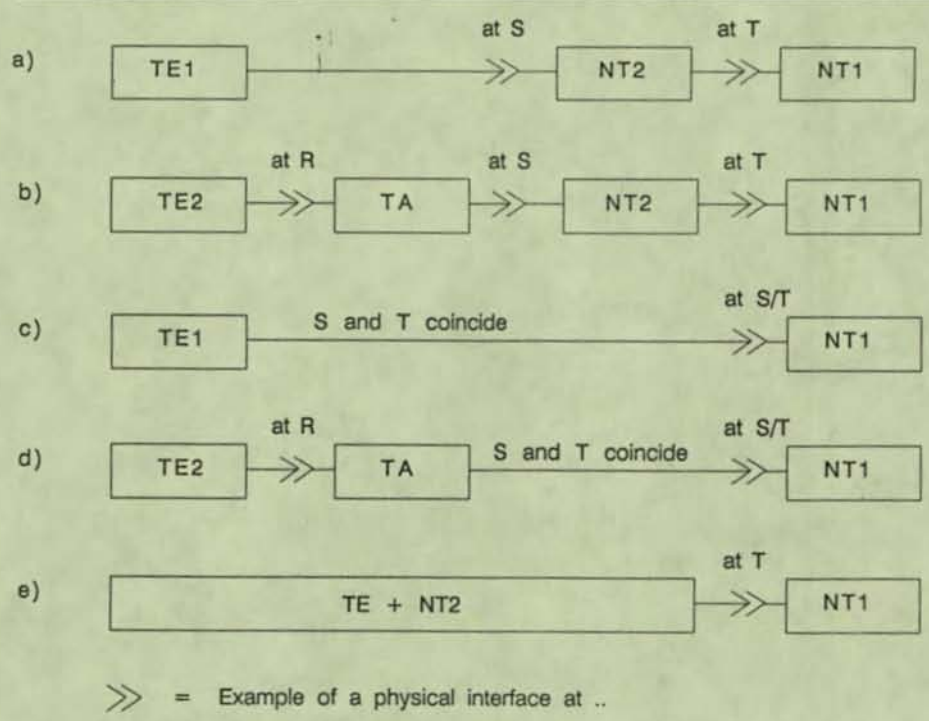


Fig. 3. Examples of physical configurations.

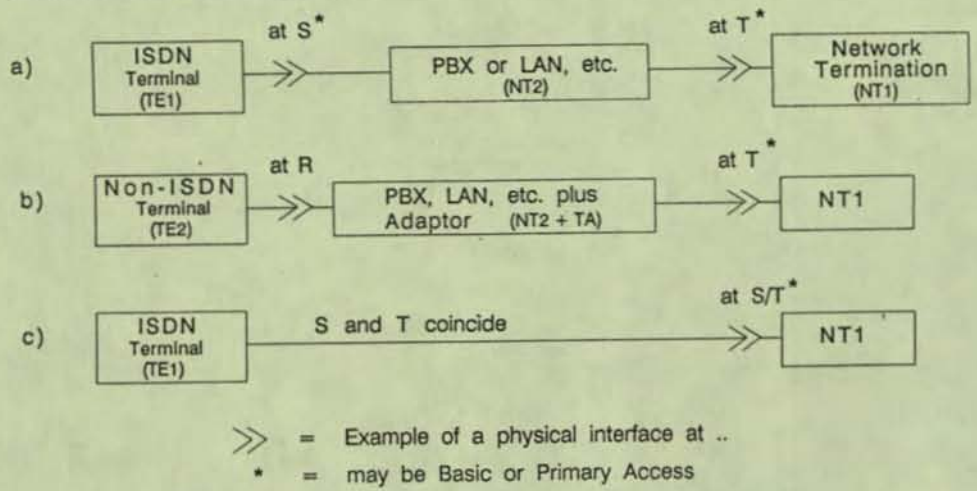


Fig. 4. Examples of NT1 and NT2 implementations.

- A digital telephone (TE1) is connected to the network through the NT1. In this case, the NT2 is functionally null and reference points *S* and *T* coincide;

● in the business environment, particularly large businesses (*Figs. 3a,b* and *4a,b*):
- Digital telephones, data terminals, etc. (TE1 or TE2 plus TA) are connected to a PBX or LAN (NT2) at the *S* reference point with the NT2 connected to the network through the NT1 at the *T* reference point.

At the *S* and *T* reference points there may be more than one physical user-network interface implemented.

5.2. Channel Types

The interface structure at a particular reference point is described in terms of channel types available at the physical interface coinciding with that reference point and other characteristics. The ISDN channel types are described below:

● *B channel*: 64 kbit/s
- Usage:
  - To carry a wide variety of transparent user information;
  - In the case of telephony, full transparency may not be possible due to encoding;
  - *B* channels may be circuit- or packet-switched, or transmitted on a semi-permanent connection;
  - If packet-switched, the *B* channel will carry protocols at layers 2 and 3 in accordance with the X.25 Recommendation and will only be transparent to the network above layer 3;
  - Bit streams at rates less than 64 kbit/s may be rate adapted to be carried on a *B* channel. Recommendations I.460 (general), I.461 (X.21 and X.21 bis), I.462 (packet mode terminals), and I.463 (V.Series terminals) provide details on this subject.

● *D channel*

The *D* channel bit rate varies depending on the interface structure with values of either 16 kbit/s or 64 kbit/s.
- Usage:
  - The *D* channel is primarily intended to carry signalling information for circuit switching;
  - The *D* channel may also be used to carry packet switching data or user-user signalling;
  - The *D* channel signalling protocol for layers 2 and 3 is specified in Recommendations I.440, I.441, I.450, and I.451. More detail concerning this signalling protocol is presented in Section 6.

● *E channel*: 64 kbit/s
- Usage:
  - The *E* channel is primarily intended to carry signalling information for circuit switching;
  - The *E* channel is only used in the alternative primary rate interface described below.

  * The *E* channel signalling protocol for layers 2 and 3 is specified in Recommendations I.450, I.451, and Q.710 (CCITT Signalling System No. 7). More detail concerning this signalling protocol is presented in Section 6.
- *H channels*
- *H*0: 384 kbit/s
- *H*11: 1536 kbit/s
- *H*12: 1920 kbit/s
- Usage:
  * The various *H* channels may carry a variety of user information on a dedicated or simultaneous basis;
  * Examples of user information are: fast facsimile, video, high speed data, or packet-switched information.

5.3. Physical Interfaces

The physical interfaces at reference points *S* and *T* must comply with one of the interface structures defined below. Not all channels listed in the interface structure need be supported by the network or the terminal, but whether supported or not, the defined frame structure must be present at the interface.

5.3.1. Basic Access

Interface Structure:

$$2B + D$$

The *D* channel in this case is 16 kbit/s. The two *B* channels may be used independently of one another. The interface may also support channels as $B + D$ or just *D*.

Other Characteristics:

The combined bit rates of the $2B + D$ channels result in 144 kbit/s. The frame structure of the basic access interface, however, requires 192 kbit/s to allow for DC-balancing of the transmission line and synchronization.

The frame structure for basic access is not symmetric but differs depending on the transmission direction. The frame length and repetition rate are nonetheless identical for both directions with values of 48 bits and 8 kHz, respectively.

The same basic rate interface supports two modes of operation at layer 1:

point-to-point;

point-to-multipoint.

In a point-to-point configuration, a single terminal is connected at the interface. In point-to-multipoint operation, up to 8 terminals may be connected in a passive bus configuration. The active terminals all share the 2 *B* channels and the *D* channel.

Point-to-multipoint operation may be configured in one of two ways: (1) as a short passive bus with terminals attached randomly along the bus or (2) as an extended passive bus with the terminals clustered relatively close to one another at a distance from the NT. The bus length is limited by the access control mechanism required for *D* channel access in the point-to-multipoint configuration. In case 1), the maximum bus length is 100–200 meters; in case (2), about 500 meters with the terminals clustered within the last 25 to 50 meters. The reach of the point-to-point configuration is limited by the cable attenuation and allows a distance of up to 1.0 km between the TE and NT or between the NT2 and NT1.

In the point-to-point configuration, a single signalling end point exists on both sides of the user interface. A terminal capable of handling multiple services may use both *B* channels, but the signalling for these channels is multiplexed at layer 2 and no contention resolution is required.

In the point-to-multipoint configuration, each of the active terminals supports a signalling end point. This requires an access control mechanism in the user-to-network direction for *D* channel access as well as an addressing mechanism in the network-to-user direction for terminal selection.

The access control mechanism makes use of an echoing function whereby the network echoes the incoming signalling bits from the multiple terminals. The terminals monitor these echoed bits to determine if they have achieved access to the *D* channel. Should a terminal receive an echoed bit in disagreement with the bit it last transmitted, it stops sending immediately. In this way, only one terminal maintains access to the *D* channel. Also, no information is lost through collision since the terminals stop sending at the first echoed bit in disagreement with their transmission. Most collisions will occur within the address field of the HDLC frame (see Section 6).

The channel access mechanism is coupled with a priority mechanism which allows terminals to be grouped into two classes with two priority levels in each class. The priority mechanism is based on counting the number of consecutive ones or inac-

tive bits in the *D*-channel before being allowed to send. In the higher class, the terminals count either 8 or 9 consecutive ones before being enabled to send, in the lower class either 10 or 11 ones are counted. After having achieved access to the channel through counting and the subsequent activation of the above access control mechanism, a sending terminal places itself into the lower of the two priority levels within its class until no further terminals attempt access at the higher level. At this time the terminal may increase its priority level within its given class. Signalling in the *D* channel is always in the higher of the two priority classes.

In the other direction, i.e. network-to-user, a TEI (terminal endpoint identifier) is employed as part of the layer 2 address to determine which of the terminals is the *D* channel end point. The TEI is assigned per hardware within the terminal or by the network through a TEI assignment procedure at layer 2. This procedure involves determining if the TEI is already assigned followed by a handshake between the NT and the TE.

No contention takes place in the *B* channels themselves since the signalling protocol determines which of the terminals have access to which of the *B* channels at any given time.

For incoming calls in a multipoint configuration, any terminal may accept the call by completing the layer 3 call setup signalling handshake with the network.

Despite the fact that there are two bidirectional *B*-channels in the basic access interface, terminals in the bus configuration cannot communicate with one another over the bus except via a connection through the network's switch.

Synchronization of the interface follows from the NT. That is, the TE synchronizes its frame to the incoming frame from the NT. There is a 2 bit period delay in the different directions to allow the *D* channel bits arriving at the network to be echoed.

The basic access interface further allows for activation/deactivation of the terminal and the NT1 equipment for low power consumption when no calls are in progress. The equipment is activated or deactivated depending on the type of signal at the interface.

In the basic access interface, a pair of wires is provided in each direction for transmission of the digital signal. The appropriate pair may additionally be used to provide a phantom power circuit from the NT to the TE on an optional basis. The power level is left for specification by the national administrations.

The option of power feeding to the TE in an emergency situation is also permitted. In the emergency situation, the polarity of the power at the interface is reversed and the TE may receive power of up to 400 mW over the interface. Other power feeding options are also mentioned in the I.430 Recommendation.

The line code used is an inverted AMI code. A binary one is transmitted as no line signal and a binary zero as alternating positive and negative pulses. Mark violations are employed to ensure that correct frame alignment is achieved within 13 bit periods.

One of the most attractive aspects of the Basic Access interface is that the interface is capable of using the dual twisted pairs already installed for the analog telephone system in the local loop and inside of buildings. This provides a tremendous savings for the introduction of ISDN since new cable need not be installed.

5.3.2. Primary Access

Interface Structure:

Primary rate:	$23B + D$ and $30B + D$
Alternative primary rate:	$23B + E$ and $30B + E$

The *D* channel in this case is 64 kbit/s as is the *E* channel. All the *B* channels may be used independently of one another.

Other Characteristics:

All primary rate interfaces having the following characteristics:

- They may be implemented at the *S* or *T* reference points;
- They support only point-to-point connections at layer 1, thus there is no need for an access control mechanism at this layer;
- The transmission frame is symmetrical for both directions of transmission with a frame repetition rate of 8 kHz;
- These interfaces are always in an active state, i.e. no activation/deactivation mechanism is provided;
- There is no provision for power feeding as in the basic rate interface;
- If at the *S* or *T* reference points, several primary

rate
of o
chan
chan
The
alternat
ling pr
channel
D chan
the *E* c
Signalli
The
the int
channe
face bi
The fo
structu

S

Note:

Fig. 5.

rate interfaces are implemented, the signalling of one interface may be carried in the *D* or *E* channel of another allowing the unused *D* or *E* channel to function as an additional *B* channel.

The difference between the primary rate and alternative primary rate interface lies in the signalling protocol specified below layer 3. For the *D* channel, the signalling protocol is identical to the *D* channel protocol of the basic rate interface. For the *E* channel, the signalling protocol is the CCITT Signalling System No. 7 protocol.

The specification of two different bit rates at the interface results in different numbers of *B* channels for the primary rate interface. One interface bit rate is 1544 kbit/s, the other 2048 kbit/s. The former supports the $23B + D$ or *E* channel structure, while the latter supports the $30B + D$ or *E* channel structure. The support of two bit rates for primary rate access has historical and evolutionary reasons in that in North America the present day IDNs use the 1544 kbit/s rate while in Europe, the 2048 kbit/s rate is implemented.

As to be expected with different primary bit rates, the frame structures, framing mechanisms, and synchronization methods are different as well.

5.3.2.1. The 2048 kbit/s Primary Rate Interface

The frame structure at this bit rate contains thirty-two 64 kbit/s channels which take up the entire bandwidth. Thirty of the 64 kbit/s channels are *B* channels, one channel is used for frame synchronization, and the remaining channel is used for the *D* or *E* channel.

The TE synchronizes its bit, byte (octet), and

SMF	Frame Number	Bits 1 to 8 of the frame							
		1	2	3	4	5	6	7	8
I	0	C_1	0	0	1	1	0	1	1
	1	0	1	A	S_n	S_n	S_n	S_n	S_n
	2	C_2	0	0	1	1	0	1	1
	3	0	1	A	S_n	S_n	S_n	S_n	S_n
	4	C_3	0	0	1	1	0	1	1
	5	1	1	A	S_n	S_n	S_n	S_n	S_n
	6	C_4	0	0	1	1	0	1	1
	7	0	1	A	S_n	S_n	S_n	S_n	S_n
II	8	C_1	0	0	1	1	0	1	1
	9	1	1	A	S_n	S_n	S_n	S_n	S_n
	10	C_2	0	0	1	1	0	1	1
	11	1	1	A	S_n	S_n	S_n	S_n	S_n
	12	C_3	0	0	1	1	0	1	1
	13	S_i	1	A	S_n	S_n	S_n	S_n	S_n
	14	C_4	0	0	1	1	0	1	1
	15	S_i	1	A	S_n	S_n	S_n	S_n	S_n

Note: Frame alignment frames contain the bit pattern 0011011.
The C bits of SMF II are the result of the CRC4 operation applied to SMF I.
The A bits are alarm bits for later definition.
The Sn bits are for national definition.
The Si bits are international bits; also for later definition.
The CRC synchronization bit pattern is 001011 in bits 1 of alternating frames.

Fig. 5. CRC4 multiframe structure in the 2048 kbit/s primary rate interface.

frame timing to the signal received from the NT and synchronizes its transmission accordingly. Frame synchronization is achieved via alternating bit patterns in channel 0 providing a multiframe structure of two frames. The first of the two frames contains the bit pattern for frame alignment. The second frame contains a forced bit to distinguish it from the frame alignment frame as well as an alarm bit whose exact function is yet to be defined and 5 bits reserved for national use and to be determined by the different administrations.

The first bit of both of these frames have been reserved for later definition. A suggested use for this bit, however, is for a CRC4 error detection procedure. It looks as though this suggested use may become mandatory during the ongoing CCITT study period. Such a procedure decreases the probability that false synchronization occurs through simulation of the frame alignment sequence in the data stream and increases the probability that bit errors are detected.

The CRC4 procedure produces a multiframe structure consisting of 16 frames (see *Fig. 5*). The multiframe is partitioned into two submultiframes (SMF) of eight frames each. The first bit of frame alignment frames within an SMF contain the four CRC4 bits calculated over all the bits of the foregoing SMF. The first bit of the non-frame alignment frames provide for synchronization of the CRC4 multiframe. This leaves the first bit of two frames free for future definition.

The *D* or *E* channel, if present at the interface, is transmitted in time slot (channel) 16 of the 2048 kbit/s primary rate interface. Time slots 1 to 15 and 17 to 31 are allocated to B channels or possibly to *H* channels. *H*0 (384 kbit/s) channels may be transmitted in groups of six time slots. The time slots used for the transmission of an *H*12 (1920 kbit/s) channel at this interface has not been specified.

The physical connector for the primary interface has not been specified, however, the characteristics of the physical transmission medium are specified in Recommendation G.703. This is a four wire interface and foresees a coaxial pair or a symmetrical pair for each direction.

The specified line code is the HDB3 (high density bipolar 3) code. It is a pseudo-ternary code, i.e. three states: +, −, and 0, using alternate mark inversion and special coding rules involving code violations for strings of four spaces.

The reach of the primary rate interface will depend on the type of cable used but will be in the range of 10 km.

5.3.2.2. The 1544 kbit/s Primary Rate Interface

The frame structure at the 1544 kbit/s rate contains twenty-four 64 kbit/s channels and one 8 kbit/s channel. Twenty-three of the 64 kbit/s channels are *B* channels and the remaining 64 kbit/s channel is used for the *D* or *E* channel. The total frame length is 193 bits, one bit more than required for the 24 channels. This additional bit constitutes the 8 kbit/s channel, is called the *F* bit and is the first bit in the frame structure. The function of the *F* bit is described below.

The TE synchronizes its bit, byte (octet), and frame timing to the signal received from the NT and synchronizes its transmission accordingly.

Frames are organized into a 24 frame multiframe structure whereby the *F* bits contain a 6 bit synchronization pattern as well as some additional information bits whose definition is for further study.

The *D* or *E* channel, if present at the interface, is transmitted in time slot (channel) 24 of the 1544 kbit/s primary rate interface. Time slots 1 to 23 are allocated to B channels or possibly to *H* channels. *H*0 channels may be transmitted in groups of six time slots. Time slots 1-24 may be used for the transmission of an *H*11 (1536 kbit/s) channel if the signalling for this channel is carried in another interface.

The physical connector for the primary interface has not been specified, however, the characteristics of the physical transmission medium are specified in Recommendation G.703. This is a four wire interface and foresees a symmetrical pair for each direction.

The suggested line code is B8ZS wherein patterns of 8 consecutive zeroes are replaced by a predefined pattern.

The reach of the primary rate interface is limited by the electrical characteristics of the transmitted and received pulses and the type of cable used but will be in the range of 10 km.

6. Signalling – the *D* and *E* Channel Protocols

Signalling is the process by which connections are controlled. It provides the means to establish,

maintain, and terminate network connections across an ISDN (or a concatenation of ISDNs) between communicating application entities at their respective user-network interfaces. This process includes allocation of resources such as negotiating the network service and choosing which channel to use in the connection.

IDNs until now have used bit-oriented signalling techniques (PCM channel associated signalling and *T*1 bit-robbing). ISDN signalling is message-oriented, transmitted in a packet-mode, and is out-of-band. Out-of-band means that the signalling is transmitted in its own channel and that this channel is, in effect, independent of the other channels at the interface as far as protocols and switching of the channel are concerned. Such a procedure decouples the signalling information from the user information allowing for:

* Transparent user channels (*B* channels);
* Service independence of the user channels;
* Greater flexibility and a broader range of signalling information (easy expansion of signalling protocol by adding new message types).

6.1. D Channel Signalling

D channel signalling is comprised of a duplex bit transparent *D* channel at layer 1 with further protocol specifications at layers 2 and 3.

Layer 2 is an HDLC type protocol referred to as LAPD. This is an extension of the well known LAPB protocol used in X.25 packet-switching systems. In addition to the LAPB protocol, LAPD contains the previously mentioned TEI assignment procedure and an extended address field, as well as, a single frame acknowledged transfer service. In the single frame mode, no new *I* frame is sent until acknowledgement has been received for the previously sent frame. Acknowledged information transfer is only applicable for point-to-point connections at layer 2.

Layer 3 has a message-oriented protocol that provides the connection control aspect of signalling. It negotiates the network bearer services, which *B* channel(s) to use, and performs compatibility testing for services between end terminals.

The layer 3 messages are intended for application in the control of circuit-switched, packet-switched, and user-user, i.e. PBX-PBX signalling connections. However, some additional work still needs to be done in this area.

The protocol layers and their respective definitions for the *B* and *D* channels are shown in *Fig. 6*. *Fig. 7* gives a simplified example of *D* channel signalling flow between the terminal and the network at each end of a circuit-switched connection.

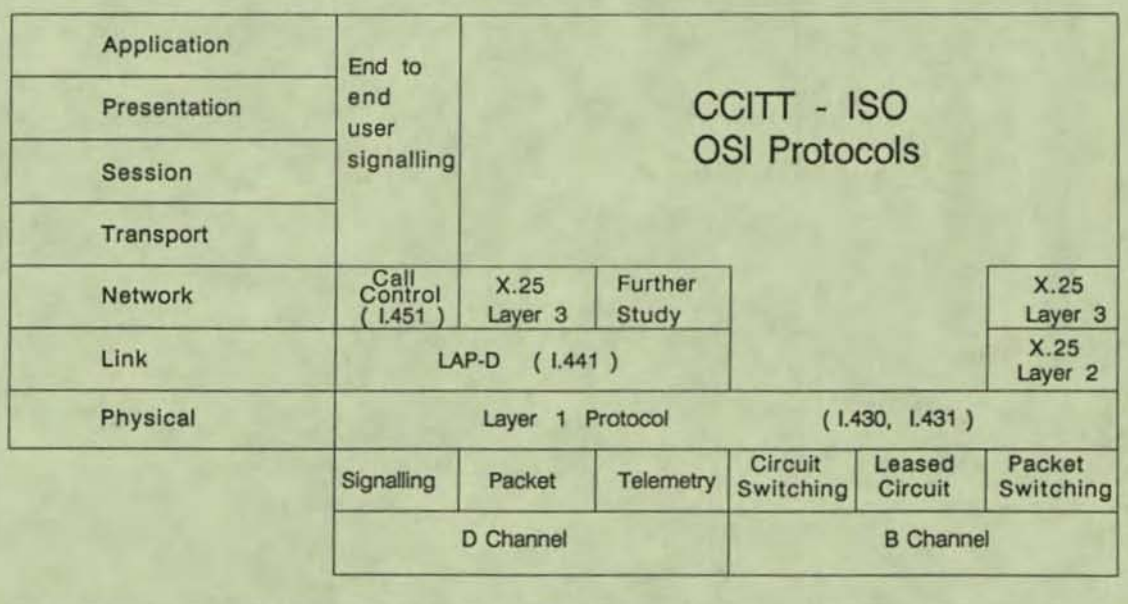
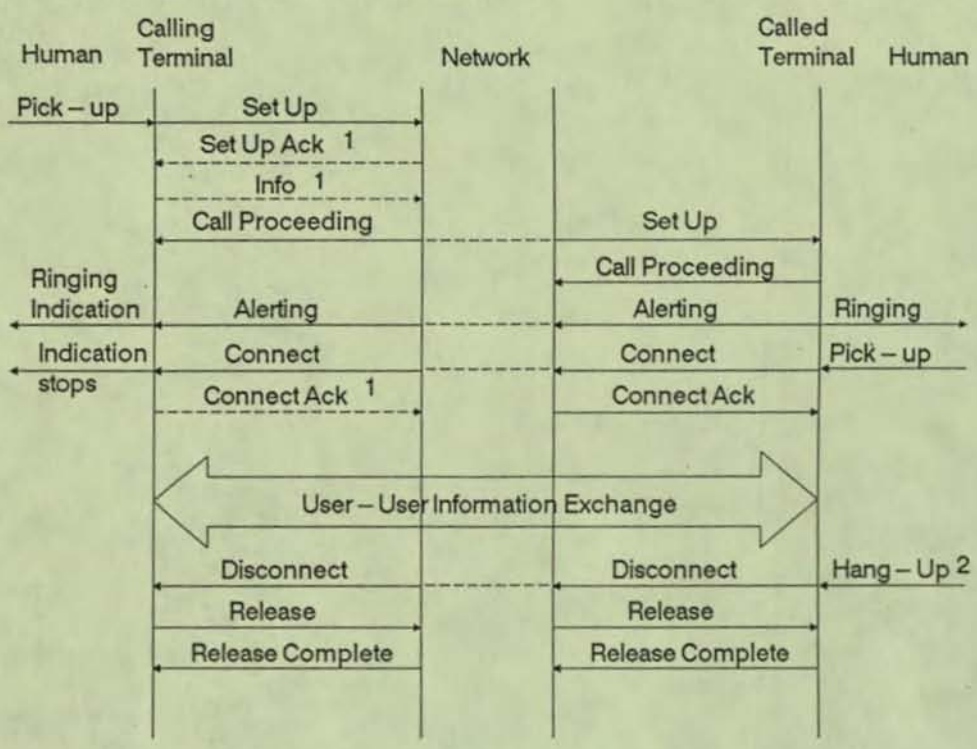


Fig. 6. ISDN layered protocol structure for user–network interfaces.



Note 1: These messages are optional depending on the implementation.
Note 2: The connect release sequence may be initiated by either party.

Fig. 7. Example of call control procedure at layer 3 for a simple circuit-switched call.

This would be a normal telephone connection with today's network. A point-to-point connection between terminal and network is assumed. The names show some of the different layer 3 message types.

6.2. E Channel Signalling

The *E* channel signalling protocol is also a layered protocol but its lower layers follow a different layering principle. It has the *D* channel layer 3 protocol fit onto the CCITT Signalling Systems No. 7 (SS7) lower layers.

SS7 was originally conceived for inter-exchange signalling and is one of the first examples of protocol layering. It was written shortly before the OSI Reference Model and is therefore not fully compatible with OSI. CCITT recommends that the *D* channel signalling protocols be used in preference to the *E* channel protocols.

7. Where Work Still Needs To Be Done

This section lists some of the areas where further work is needed in order to achieve a universal fully compatible telecommunications network. It may be unrealistic to expect that such a network could ever be achieved, however, ISDN is a good initial step in that direction.

X.200 (OSI Reference Model) was conceived primarily for data communications, whereas ISDN supports multiservice communications. Thus, there are some areas where the X.200 Recommendation does not suffice. These areas are enumerated within Recommendation I.320.

There are still inconsistencies in the *I*-Series of Recommendations. These are expected to be reconciled by the end of the 1985–1988 study period.

The areas of maintenance and management have only been lightly touched upon in the *I*-Series but are of major importance to proper network

operation. These subjects as well are expected to be covered in the 85–88 study period.

The CCITT leaves the definition of the border between customer premises and network open to national administrative jurisdiction. In North America this border is placed at the transmission line in the reference configuration. In Europe, this border is generally placed at the *T* reference point with the equipment providing the NT1 functions belonging to the network operator. This difference has resulted in minor squabbles as to the form this interface at the "*U*" reference point should take as well as different emphasis on the priority this interface should have in the standards efforts of CCITT. Decisions on this matter will also affect who can sell what equipment where, i.e. the interface for connection of customer premises equipment (CPE) to the network.

There is a consensus that the interface at *U* should be two wire, however, disagreement prevails as to the transmission mechanism to use. The ANSI T1 committee (they write the ISDN specifications for the U.S.) has chosen a time compression multiplexing or ping-pong mechanism where the transmission rate is twice that of the interface with bursts of information alternating direction. The european administrations are backing an echo-cancelling mechanism whereby the transmitted signal is filtered out of the received signal. There is also disagreement as to the line code to be employed at this interface. A quick decision by CCITT on these matters is urgent so as to enable semiconductor manufacturers to start designing chips for this interface and to help stop the growing rift between ISDN standards in North America and in Europe.

The present ISDN specifications are all based on 64 kbit/s channels and are generally referred to as narrowband ISDN. This places strict limitations on achievable bit rates making some services, e.g. high quality video, next to impossible. The next generation ISDN, broadband ISDN, is intended to handle higher bit rate services and is discussed below.

A final problem involves modelling of traffic patterns for ISDN. The mixing of services results in entirely new traffic patterns for which there is little or no precedence and for which the old models for voice traffic or data traffic alone no longer suffice. New models must be developed for dimensioning PBXs and exchanges.

8. What Is Happening Now?

A number of ISDN field trials are underway or have been planned for 1987–88. These generally involve a mixture of equipment provided by different vendors. In the U.S. these trials are being undertaken by the Regional Bell Operating Companies (RBOCs) while in Europe they are being performed by the national administrations or private network operators.

The introduction of ISDN for business usage will follow closely on the heels of these field trials as the same equipment starts being subscribed for commercial purposes. This should start happening during 1988.

9. What Is Happening Next?

The next generation of telecommunications will be broadband ISDN (BB-ISDN). CCITT has already started discussions on channel structures and transfer modes in this area. It is assumed that BB-ISDN will make heavy use of fiber optics.

New service types for use with BB-ISDN are also being discussed. Among these is the introduction of distribution services via the public network. Such services include high definition TV, high quality audio and video distribution, tele-newspaper, as well as new interactive series such as tele-library and tele-university, to name just a few.

There has also been a bit of excitement lately concerning a new transfer mode known as the asynchronous transfer mode or ATM. This mode is a mixture of packet- and circuit-switching with information transfer occurring in small fixed length packets over virtual connections.

10. Economics and Technology Support

10.1 When Will ISDN Be Available?

Decisions on the tariffing of ISDN services will have a strong effect on how quickly ISDN will penetrate the consumer market. Present suggestions in some countries follow the reasoning that the basic rate interface supplies two user channels and thus should be tariffed at twice the present rate for analog telephone connections. In more competitive regions, talk is of 1.5 times the present

rate. For businesses, either case will mean a savings, being in effect cheaper than present systems due to higher bit rates, no modems, and no requirements for special cabling. However, such tariffing will tend to slow residential penetration until new equipment and new services beyond telephony are perceived as desirable by residential consumers.

With regard to the PTTs, aspects such as capital for new equipment and write-off periods for old equipment, as well as politics and business strategy will affect how quickly ISDN and especially BB-ISDN is available. Due to the above factors, one may expect a period of several decades before ISDN shows a high penetration, however, first implementations are not far off.

10.2. Technology Support

Many semiconductor manufacturers are now offering chip families based on the 1985 I-Series publication. Basic rate access chips are being offered by AMD, AT&T, Intel, Mitel, Motorola, National Semiconductors, NEC and Siemens. Primary rate access chips have been announced for 1987-88 by Mitel and Siemens. In general, the chip sets split their functions between layers 1 and 2 with layer 3 being performed by software.

Terminology is sometimes used loosely with regard to functional descriptions of chips and the designer must be careful in determining just what each chip family does. For example, the basic access interface is often referred to as the *S* interface or the *S*-Bus interface. Such terminology is not completely accurate since CCITT calls the interface Basic Rate access.

Further research and technology support is necessary in the areas of data compression algorithms, multidata rate switching, and transmission at higher data rates as well as in new areas of network technology such as ATM.

References

[1] *CCITT Red Book*, Vol. III, Fascicle III.5, Integrated Services Digital Network (ISDN), Recommendations of the I Series, Geneva, 1985.

[2] *CCITT Red Book*, Vol. III, Fascicle III.3, Digital Networks – Transmission Systems and Multiplexing Equipment, Recommendations G.700-G.956, Geneva, 1985.

[3] CCITT Recommendation Q.710 Recommendation on the use of Signalling System No. 7 for PABX application.

[4] *Proceedings of the First Pan-European Conference on ISDN*, Nov. 1986: A. Blunschi, J. Halter, "User Advantages with the ISDN Basic Access"; P. Polushik, "U.S. ISDN Activities"; J. Van Remortel, "Private ISDN: Terminals, Terminal Adaptors and Services – A Necessary Complement of Public ISDN".

[5] H.G. Holzgrebe, "Das amerikanische ISDN-Konzept," *Fernmelde-Praxis*, June, 1987.

[6] P. Kemezis, "What price ISDN? First cost details bared," *Data Communications*, Aug. 1987.

[7] N. Mokhoff, "ISDN Gains Ground as Needed ICs Emerge," *Computer Design*, Nov. 1986.

[8] B. O'Brian, "ISDN: Users Think it's a Distant Prospect. Wrong," *Data Communications*, Dec. 1985.

[9] "ISDN Close-up," *Data Communications*, Dec. 1986.

Volume 7, Number 4, 1988
ISSN: 0920-5489
CSTIEZ 7(4) 333–444 (1988)

COMPUTER STANDARDS & INTERFACES

LAST ISSUE OF THIS VOLUME

The International Journal on the D
and Application of Standards for C
Data Communications and Interfaces

North-Holland