2822-88

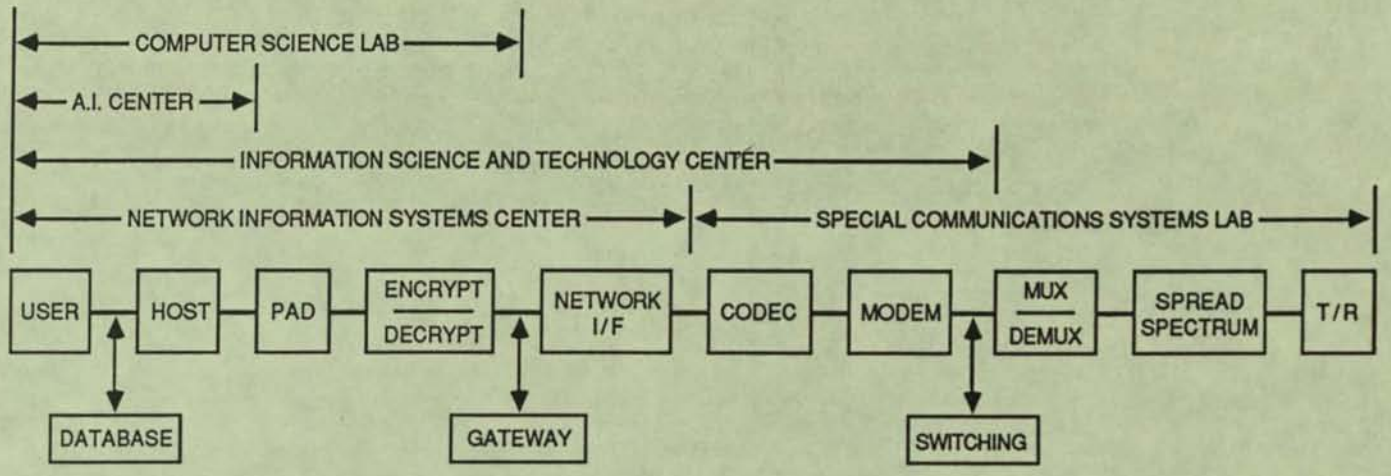
IN-PROGRESS REVIEW, April 7, 1988

Presented by: SRI International, Network Information Systems Center, 333 Ravenswood Ave., Menlo Park, CA 94025

Presented to: Defense Communications Agency Washington, DC 20305

REPORTS

SRI CAPABILITIES IN COMMUNICATION-INFORMATION-COMPUTER SCIENCE

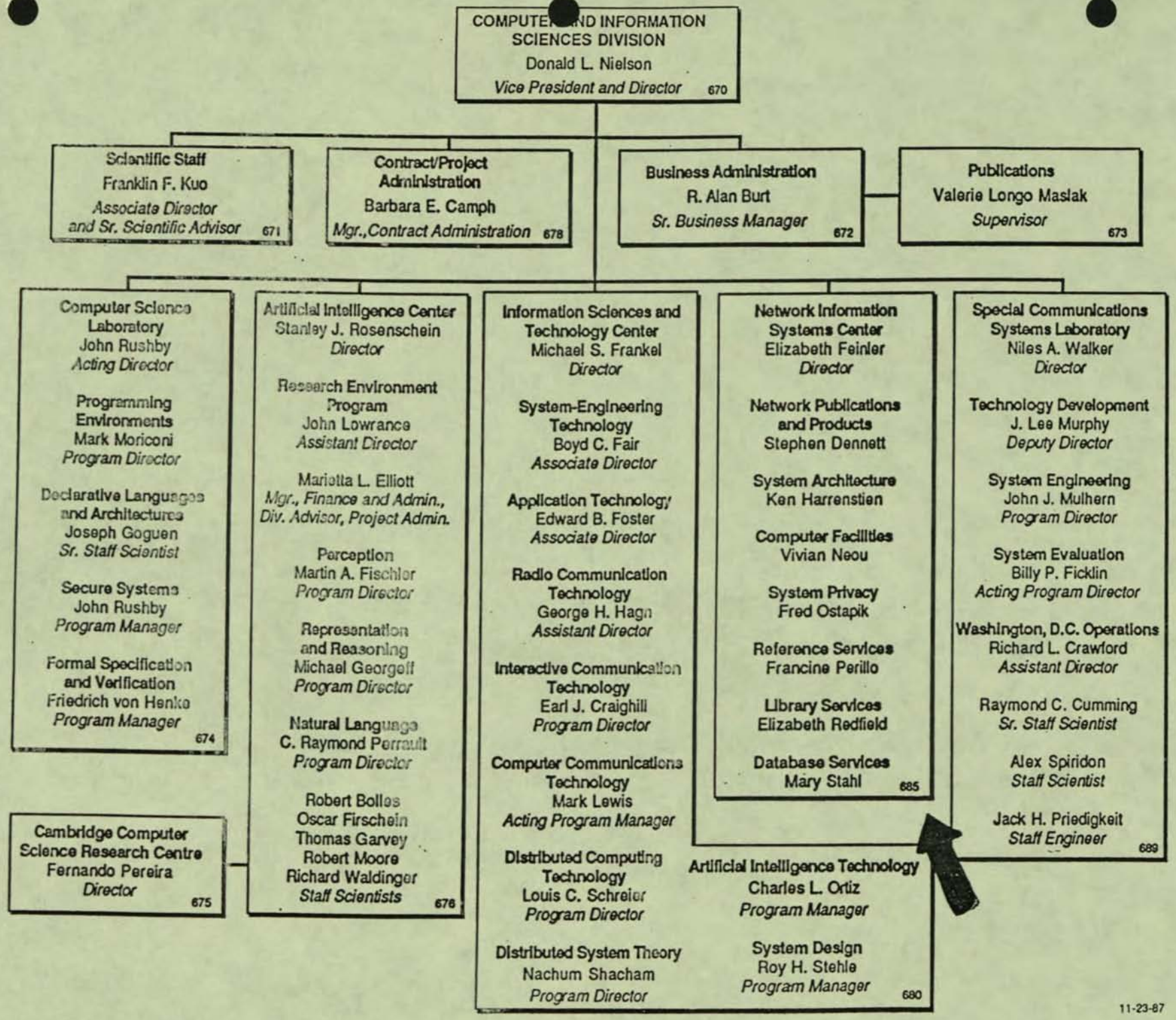


TOPICS TO BE COVERED

- DDN information infrastructure
- Augmenting users
- Naming and distributed domains
- Protocol transition and technology transfer
- Email for military users
- Information management tools

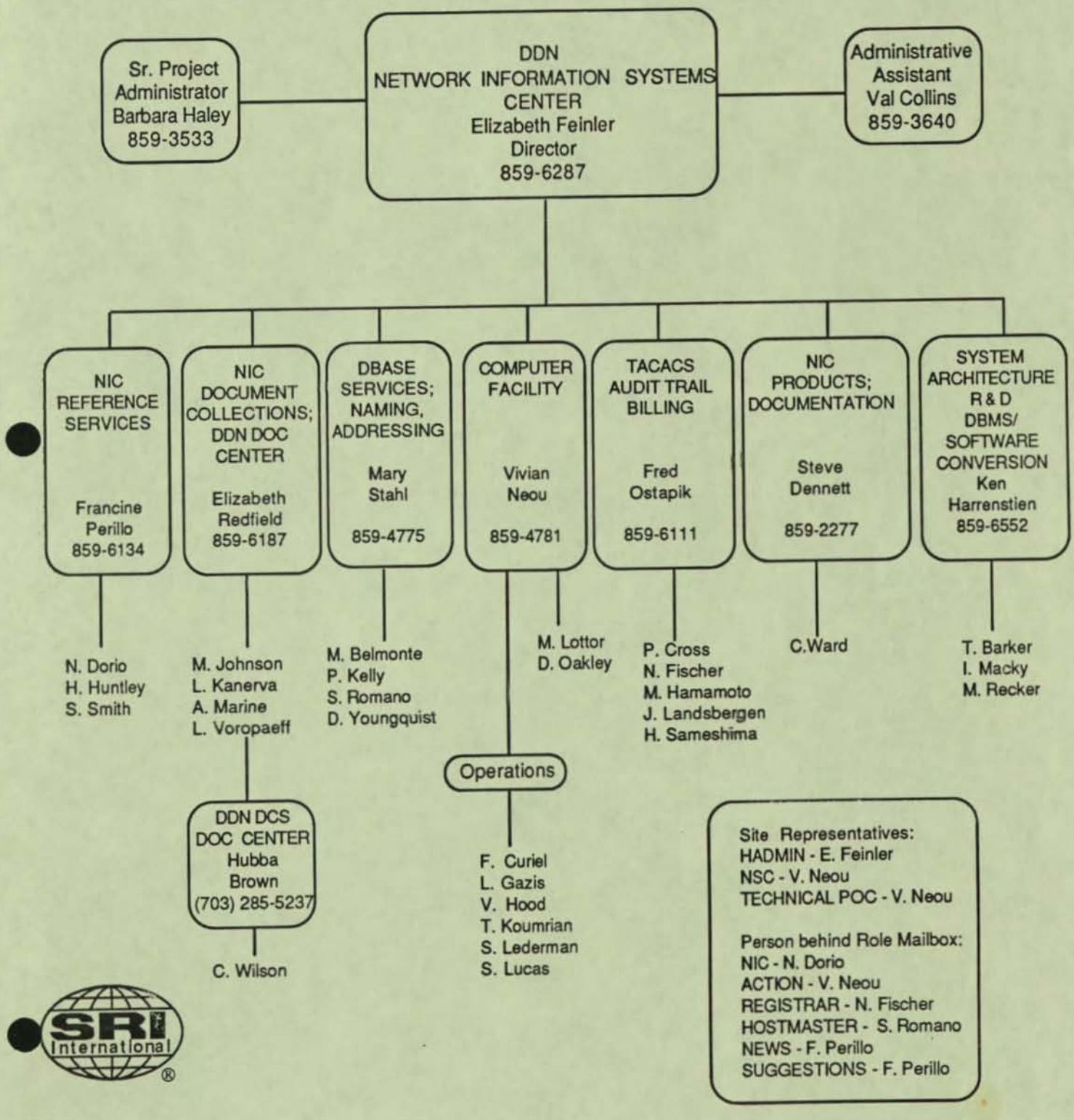
TOPICS NOT COVERED

- Information architectures
- User registration
- Protocol implementation and testing
- Audit trail and billing
- Network journal and repository
- Onsite government computer facility
- POC coordination and training
- Electronic "yellow and white" pages


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
Stanley J. Rosenschein
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
Michael Georgeff
Program Director
Natural Language
C. Raymond Perrault
Program Director
Robert Bolles
Oscar Firschein
Thomas Garvey
Robert Moore
Richard Waldinger
Staff Scientists 676
Cambridge Computer Science Research Centre
Fernando Pereira
Director 675
Information Sciences and Technology Center
Michael S. Frankel
Director
System-Engineering Technology
Boyd C. Fair
Associate Director
Application Technology
Edward B. Foster
Associate Director
Radio Communication Technology
George H. Hagn
Assistant Director
Interactive Communication Technology
Earl J. Craighill
Program Director
Computer Communications Technology
Mark Lewis
Acting Program Manager
Distributed Computing Technology
Louis C. Schreier
Program Director
Distributed System Theory
Nachum Shacham
Program Director
Artificial Intelligence Technology
Charles L. Ortiz
Program Manager
System Design
Roy H. Stehle
Program Manager 680
Network Information Systems Center
Elizabeth Feinler
Director
Network Publications and Products
Stephen Dennett
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
Jack H. Priedigkeit
Staff Engineer 689
11-23-87

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 - S. Romano
NEWS - F. Perillo
SUGGESTIONS - F. Perillo

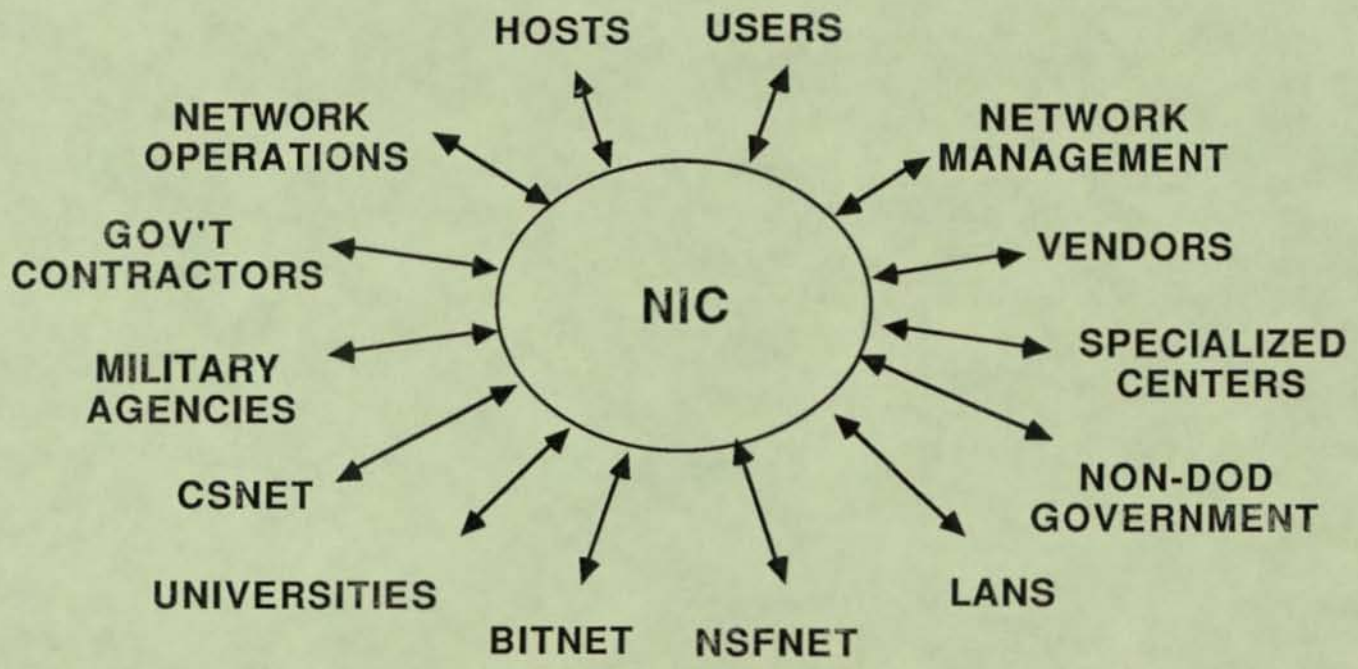
SRI International®

4/7/88

TOPICS TO BE COVERED

- DDN Information Infrastructure
- Augmenting Users and Subscribers
- OSI Naming and Distributed Domains
- Protocol Transition and Technology Transfer
- Email for Military Users
- Information Management Tools
- Audit Trail and Billing System

INTERCONNECTIVITY
AND INTEROPERABILITY



4/7/88

NEED MORE INTERCONNECTIVITY AND LIAISON AMONG MILITARY INFO CENTERS

DoD Internics

4/7/88

MORE DCA/NIC LIAISON NEEDED

- DCA Should Keep NIC Informed of
  - Policy
  - Publications
  - Procedures
  - Changes
  - Events
- Work as a Team
- Use NIC to Save Time for DCA

4/7/88

CURRENT PROBLEMS WITH DDN INFORMATION FLOW

- NIC/NMCs not kept informed
- Loops Badly
- Lacks Structure
- Much Overlap
- Duplication of Effort
- Many Gaps
- Conflicting Directives
- More Coordination Needed

RESULTS

- Technical Mistakes
- Competing Activities
- Wasted Funds
- Frustration
- Confusion
- Poor Use of Contractors
- "Bad Press" for DCA

4/7/88

SUGGESTED APPROACH

- An Internics Infrastructure
- Information Protocols
- A Military Advisory Committee
- A Network Distributed Archive System
- Clear Administrative Guidelines
- Replicated Services
- Delineation between Subscribers/End Users

4/7/88

TOPICS TO BE COVERED

- DDN Information Infrastructure
- Augmenting Users and Subscribers
- OSI Naming and Distributed Domains
- Protocol Transition and Technology Transfer
- Email for Military Users
- Information Management Tools
- Audit Trail and Billing System

USERS

- No One Knows Who They Are
- No One Knows How Many There Are
- No One Knows What They Are Trying To Do

4/7/88

USERS NEED

- An Introduction to the Network
- Ubiquitous, User-Friendly Services
- TAC Access and Registration
- Documentation
- Standard Protocol Interfaces
- Consistent Network Commands
- More Bandwidth
- Knowledge of Resources
- A Network Archive

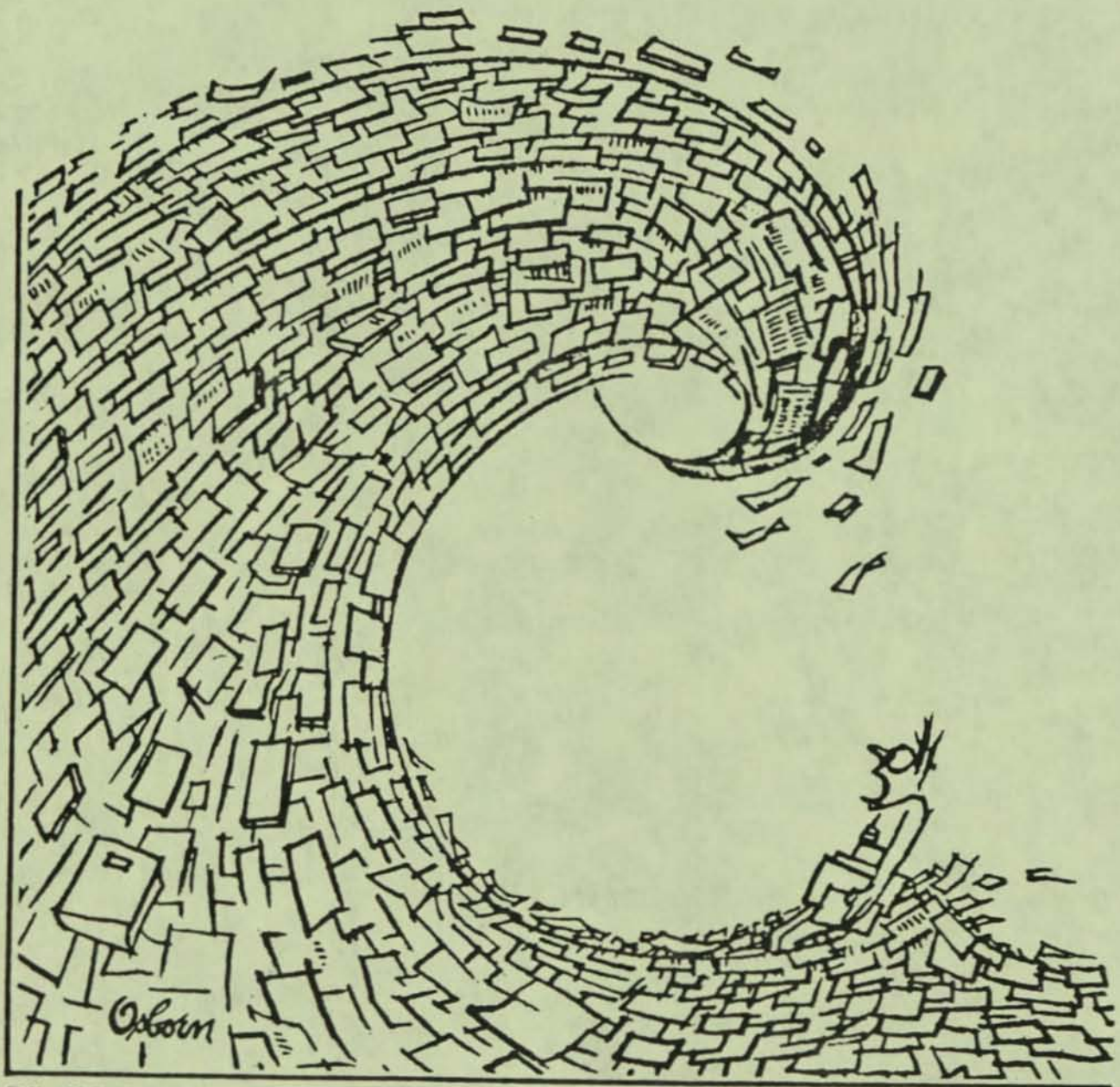
SUBSCRIBERS NEED

- An Introduction to the Network
- A Procedure Manual
- Immediate Network Access
- Administrative Guidelines
- Understanding of the DDN Architecture
- Vendor Product Information
- Protocols and Protocol Implementations
- Help for Their Contractors
- Test and Test Procedures
- Certification
- A Working-group Forum
- Adherence to the DDN Protocol Suite

POCS NEED

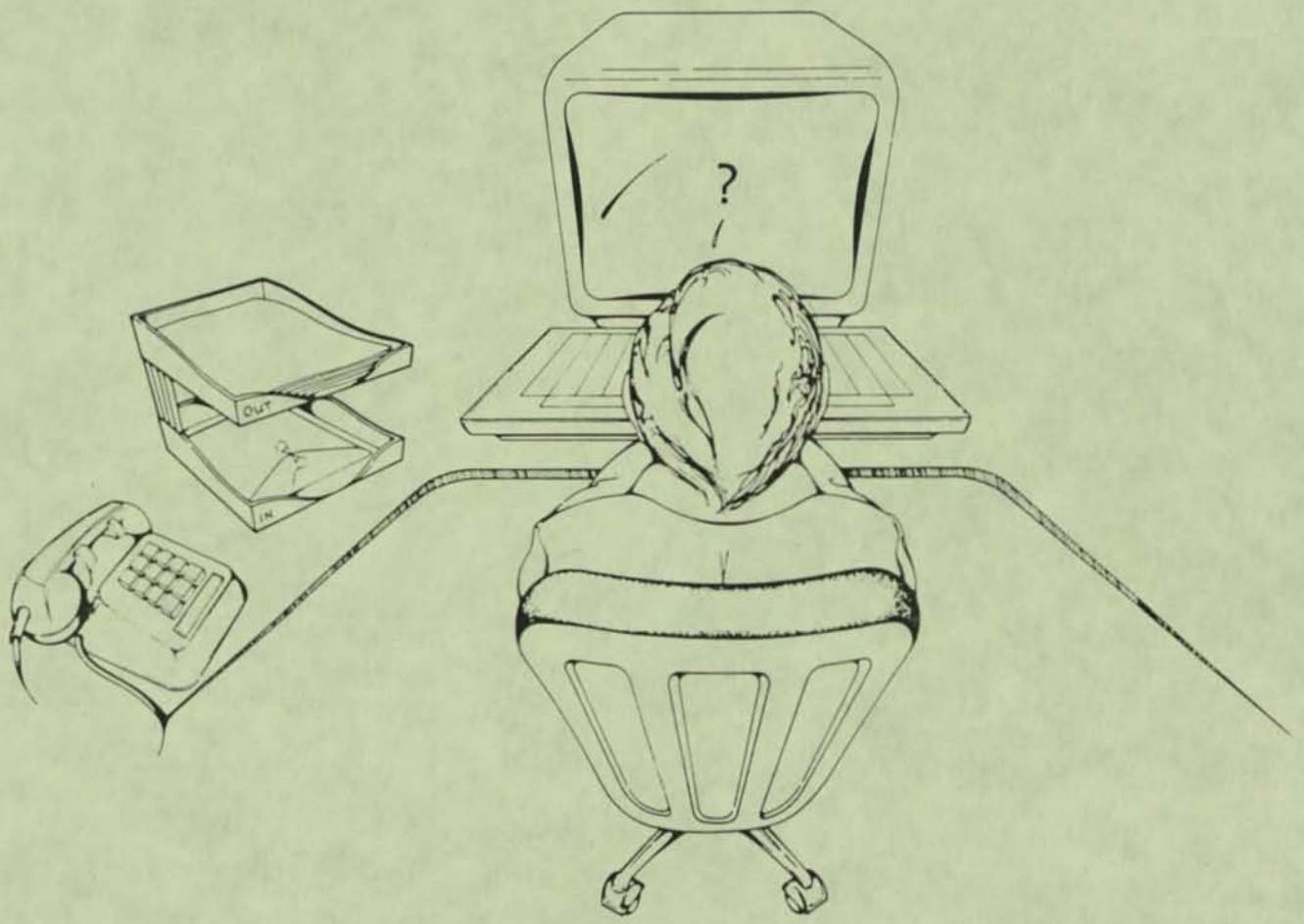
- An Introduction to the Network
- Immediate Network Access
- An Orientation Packet
- Clearly Defined Duties
- A Working-group Forum
- Recognition for the Role They Play

THE PROBLEM

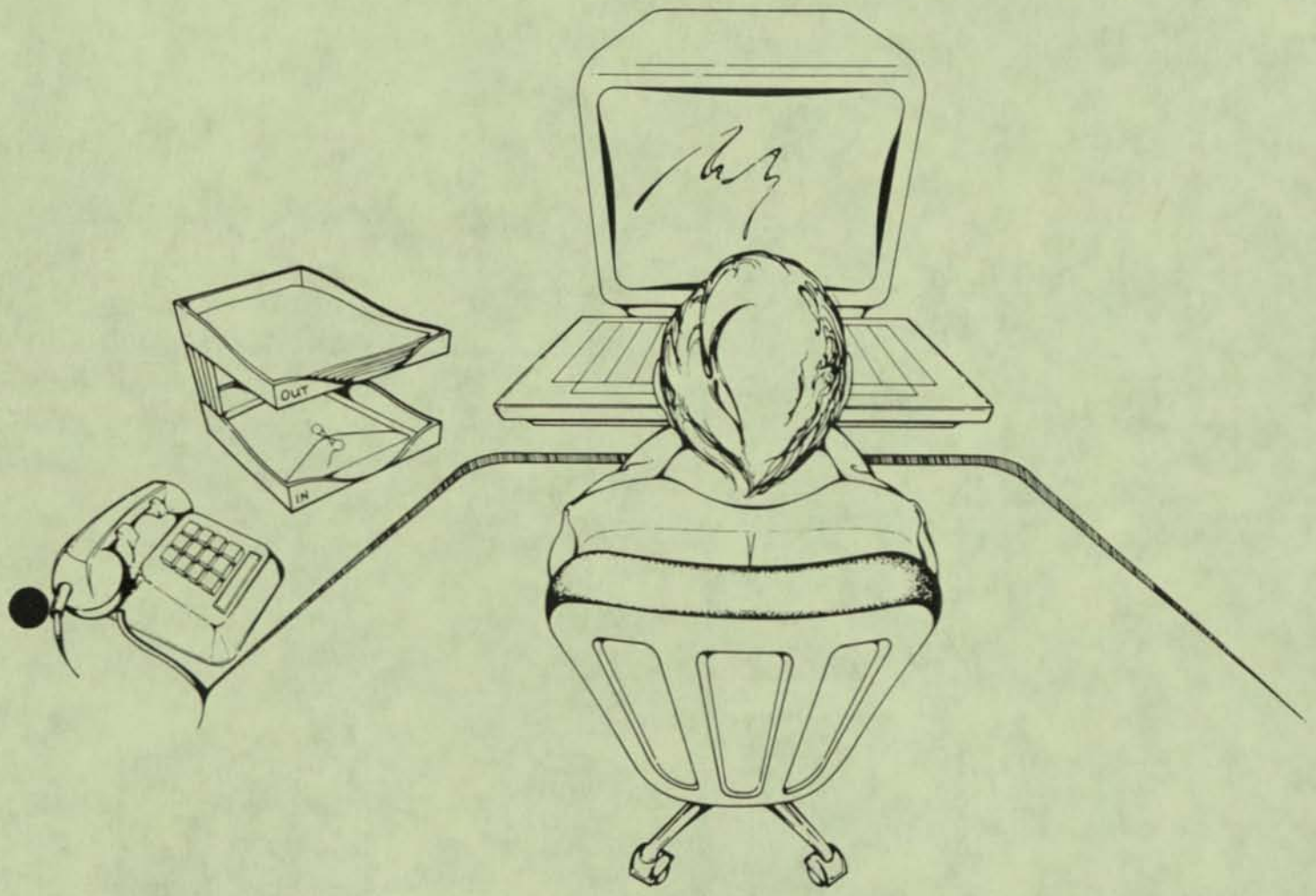


DRAWING BY ROBERT OSBORN

?????


?
OUT
IN

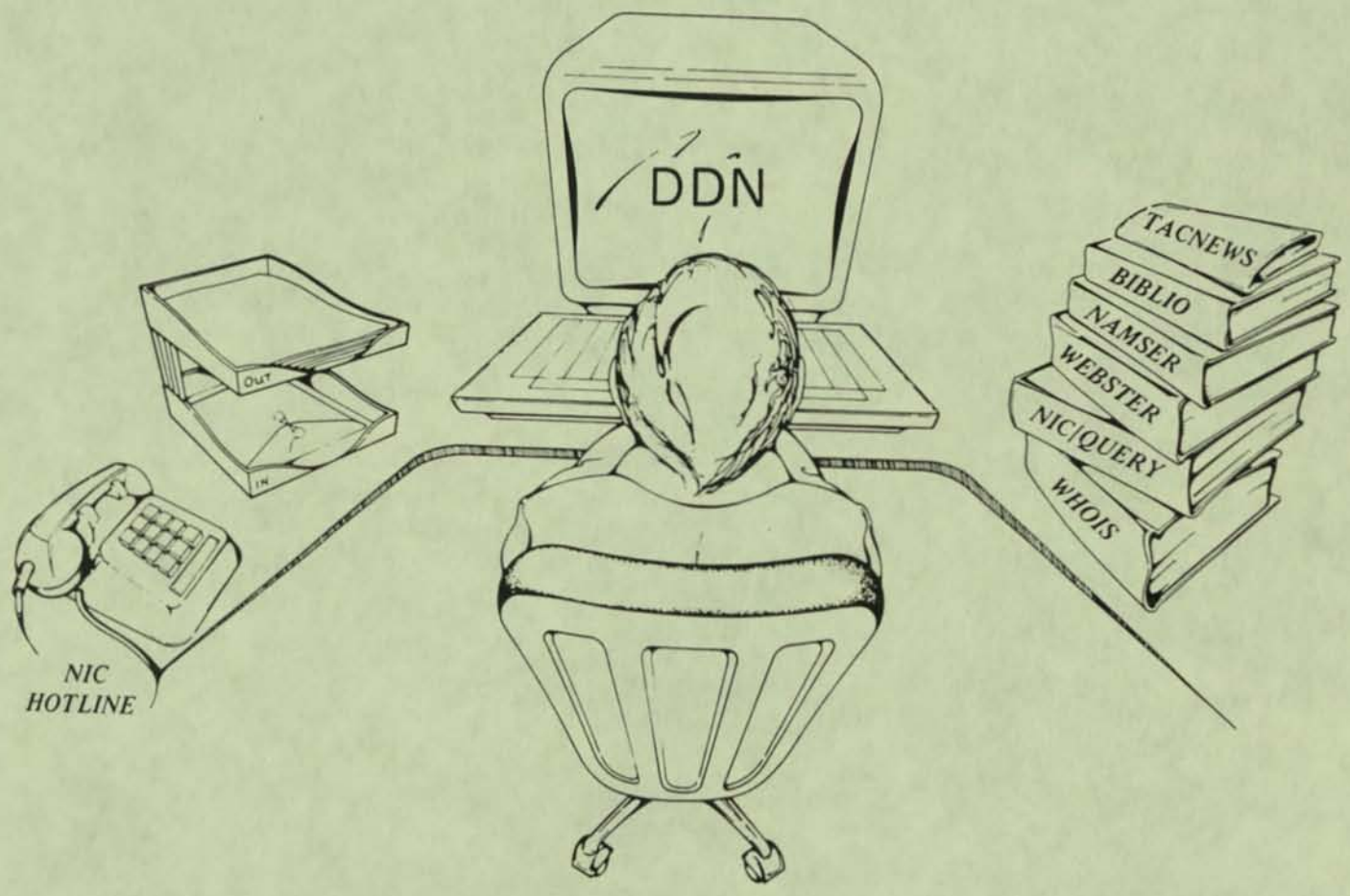
HOW WE HAVE APPROACHED THE PROBLEM



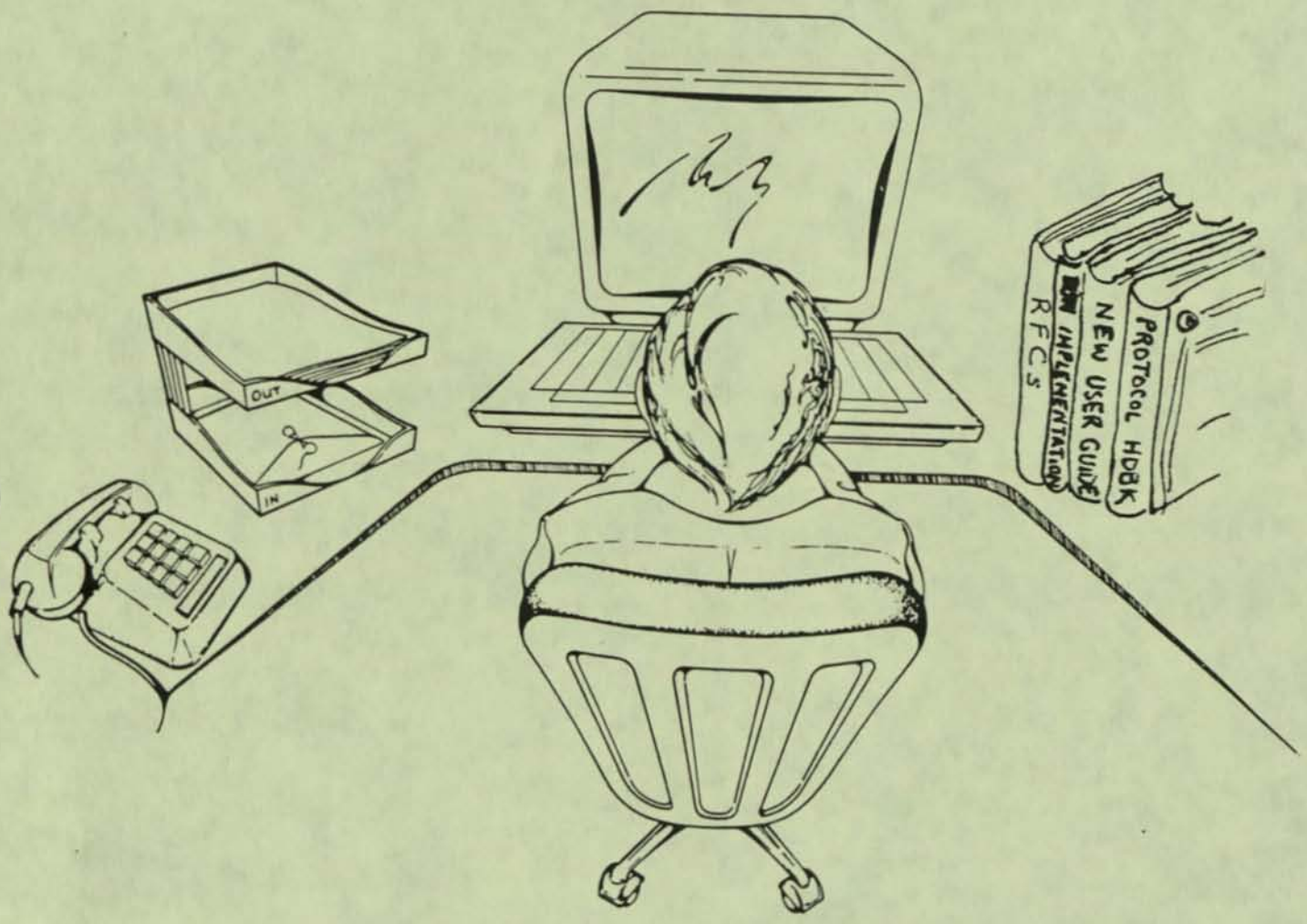
- GIVEN A TELEPHONE, A TERMINAL, AND THE NETWORK

- WE BRING INFORMATION TOOLS TO THE KNOWLEDGE WORKER ELECTRONICALLY

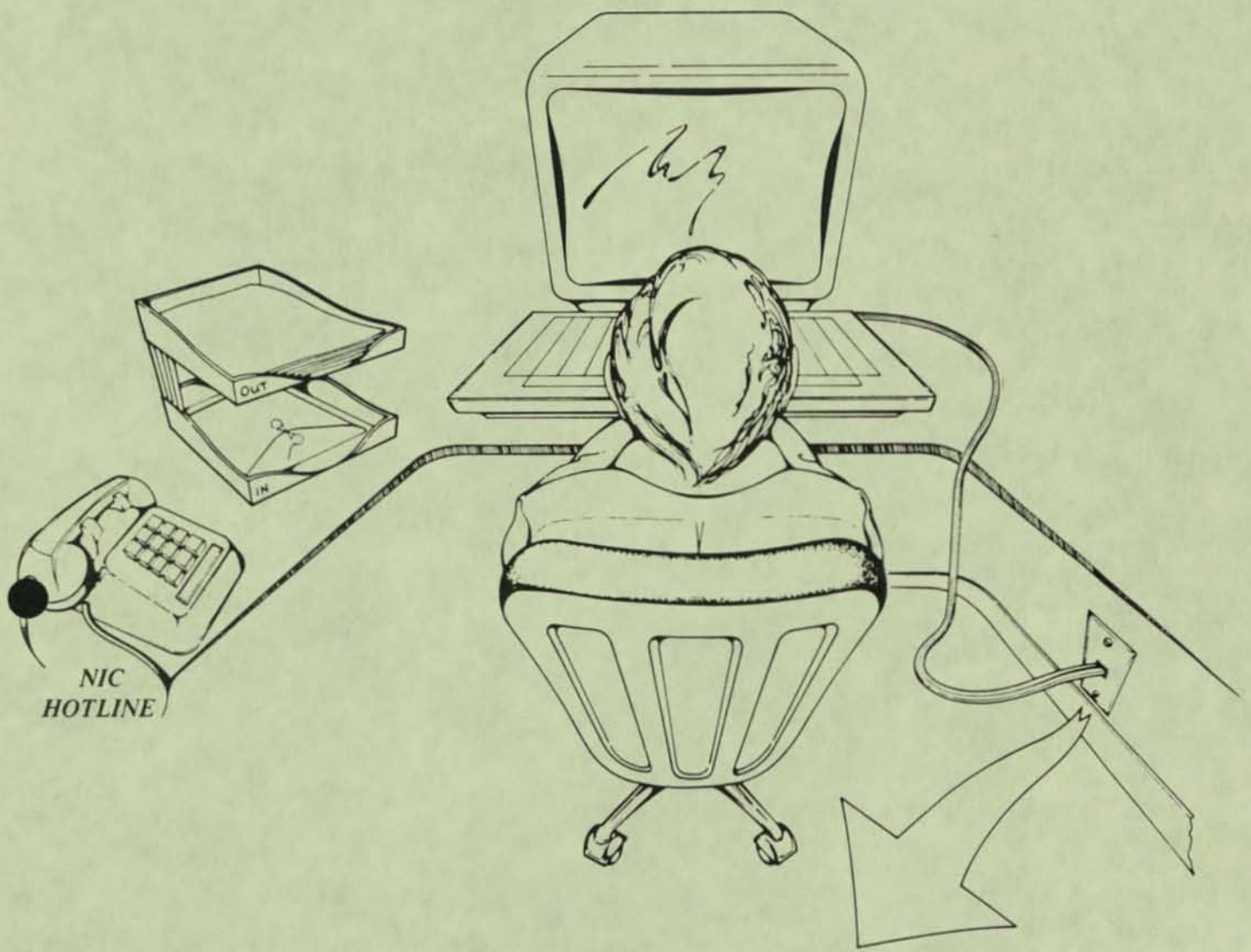
ONLINE SERVERS



USER DOCUMENTS

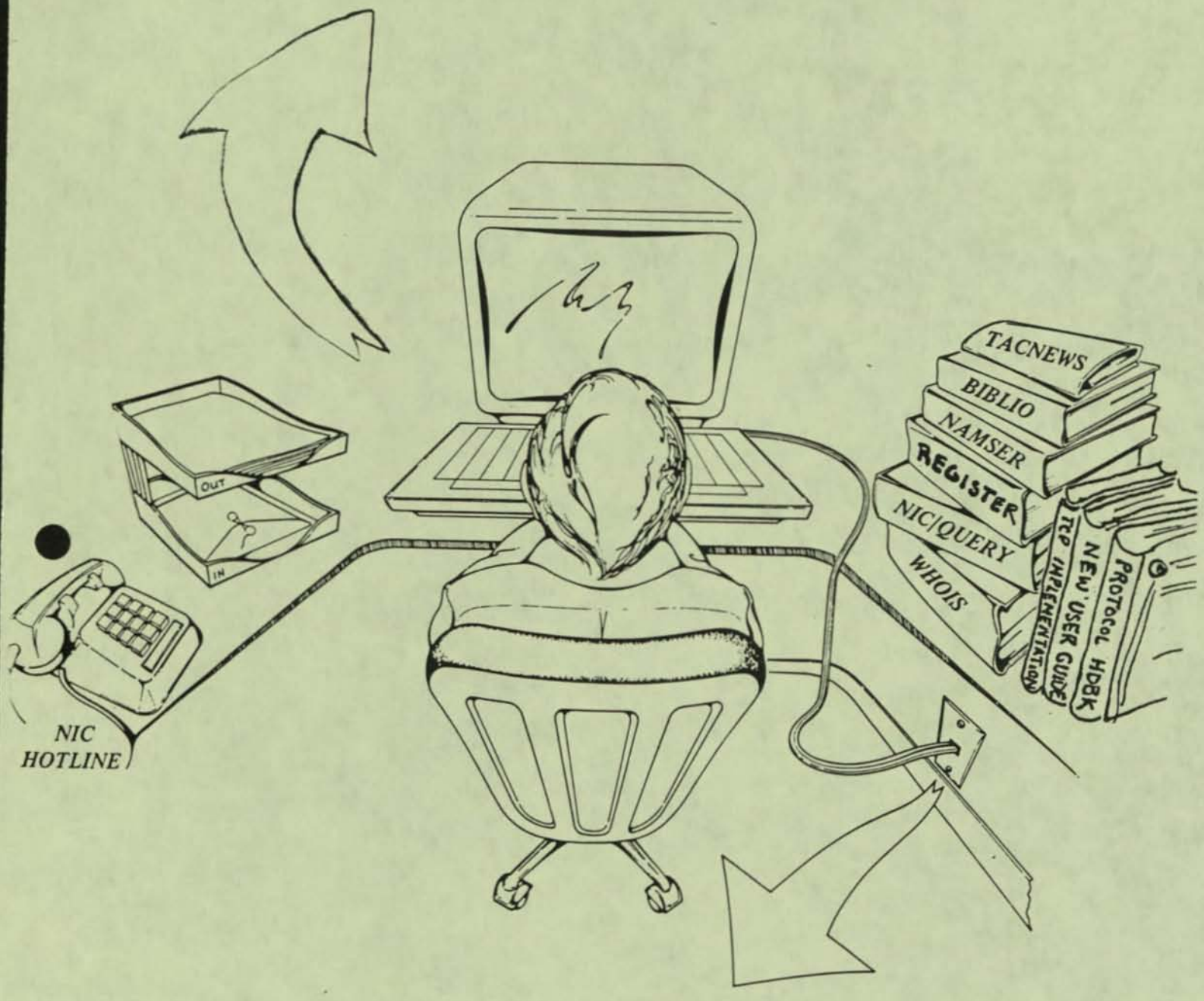


BEHIND THE SCENES



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

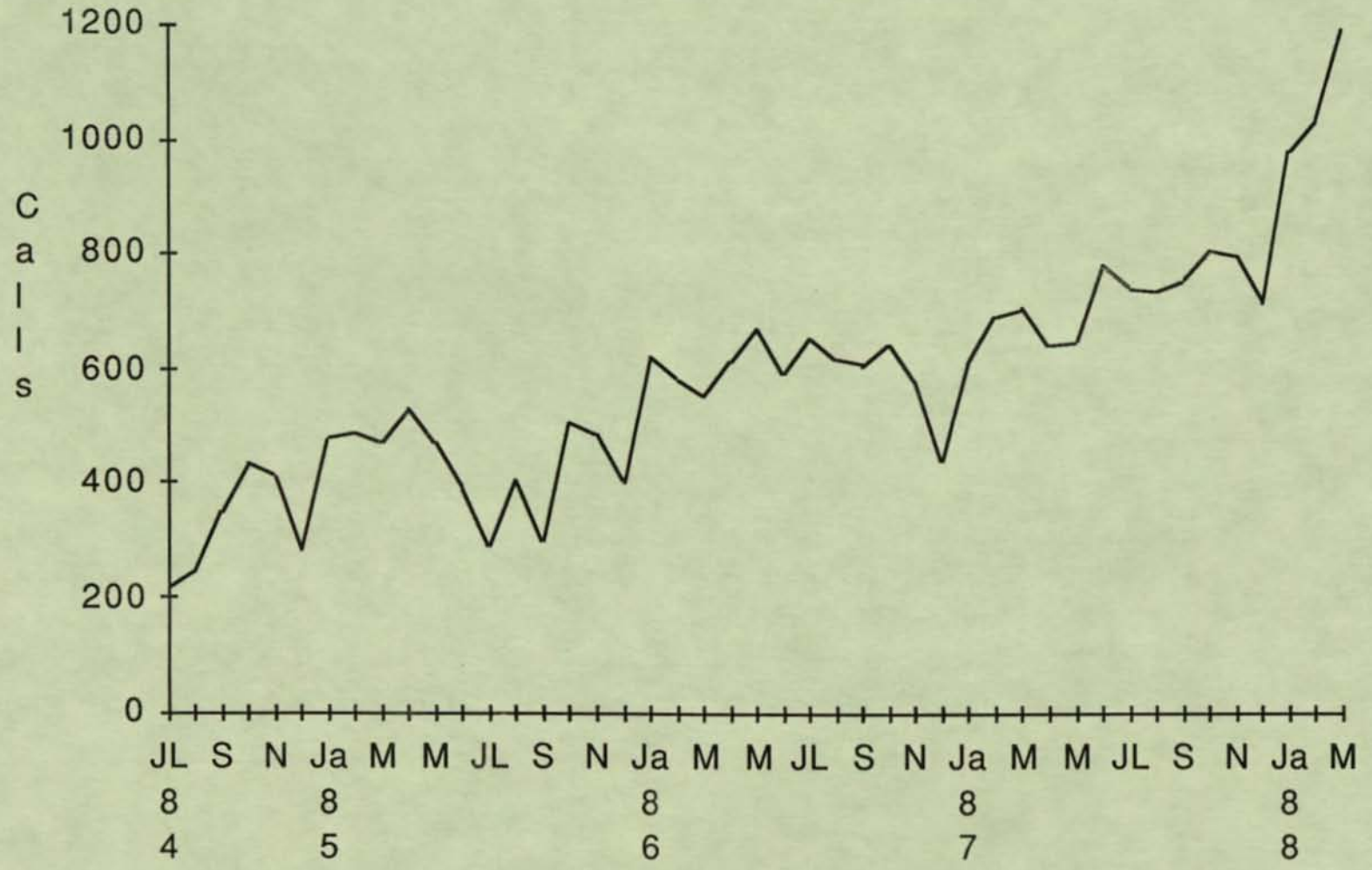
DDN NETWORK



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

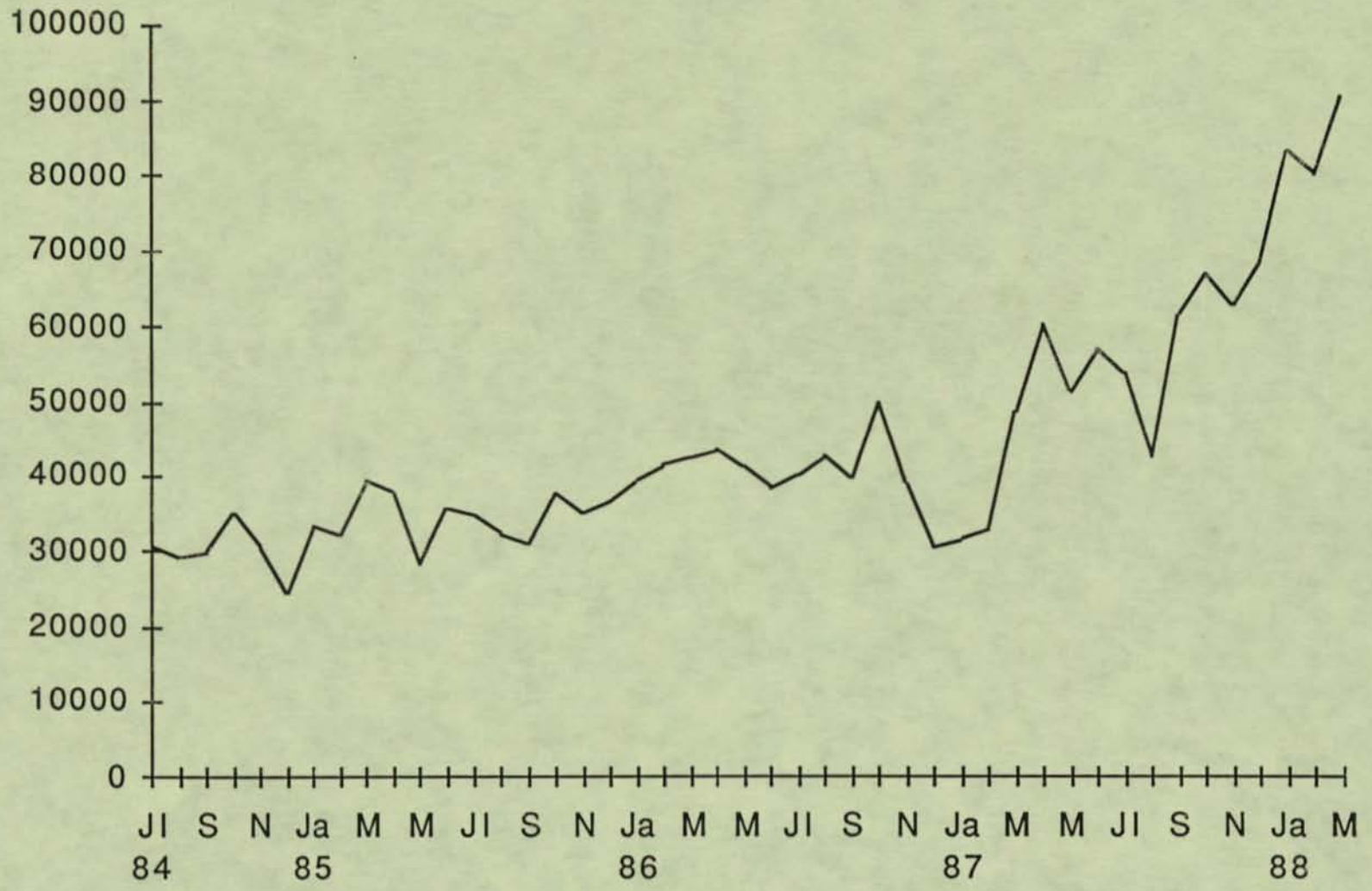
DDN Hotline Usage

July 1984 - Mar 1988



DDN Whois Usage

July 1984 - March 1988



3/11/88

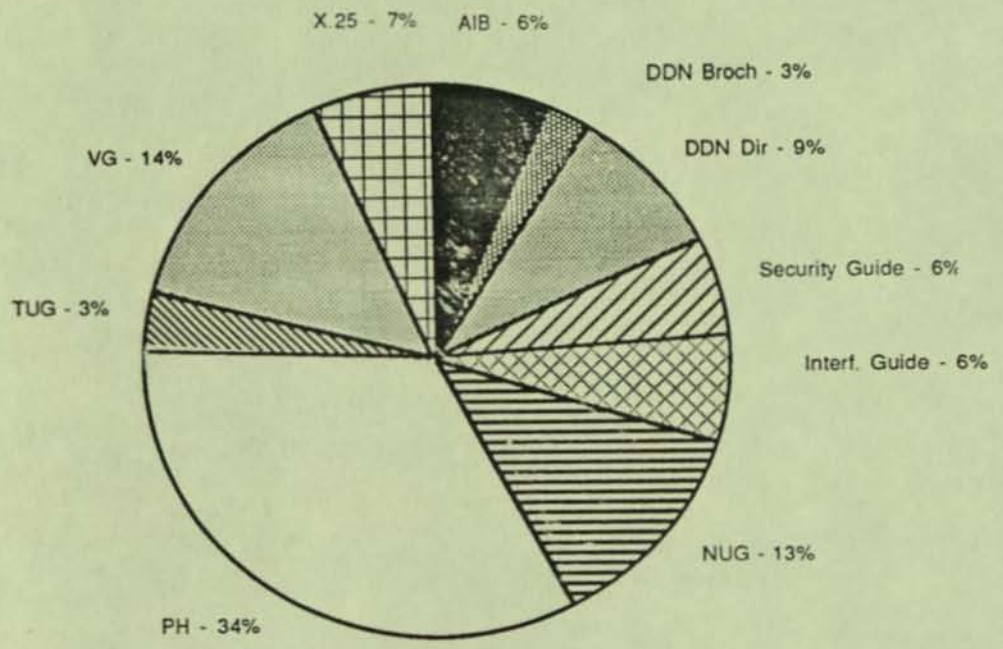
DOCUMENTS SHIPPED, 1987

ARPANET Information Brochure	188
DDN Brochure	62
DDN Directory	237
DDN New Users Guide	337
DDN Protocol Handbook	925
DDN Protocol Impl. and Vend. Guide	380
DDN Subscriber Security Guide	162
DDN Subscribe Interface Guide	165
DDN TAC User Guide	94
DDN X.25 Specifications	175
RFCs	18,300

3/11/88

Documents Distributed by SRI
1987

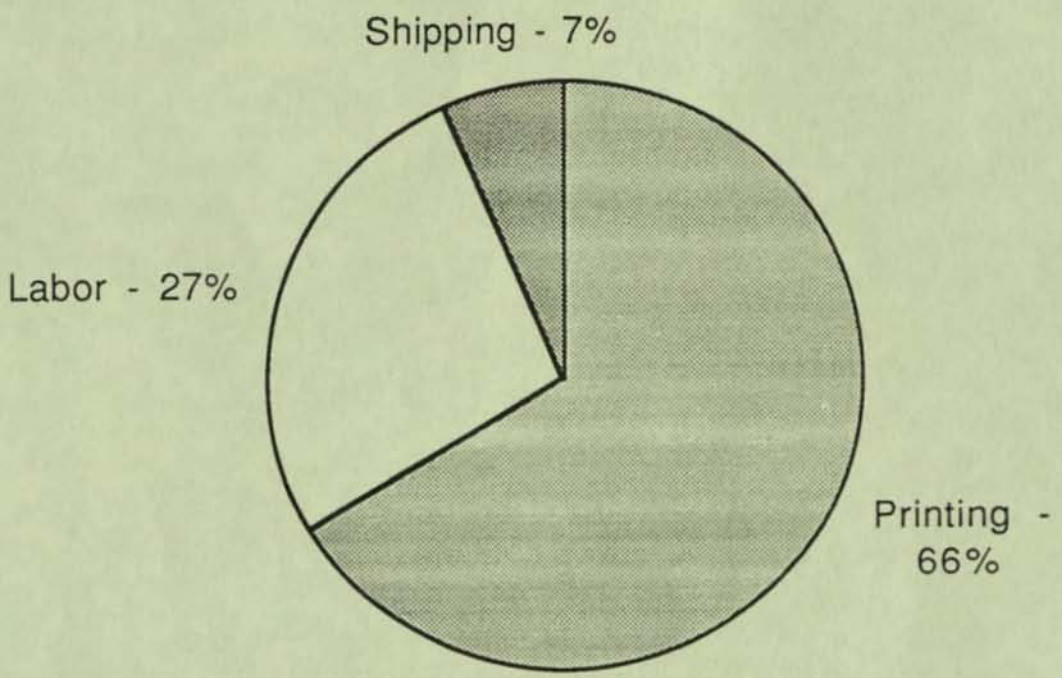
By Document Title (RFCs not included)



3/11/88

SRI Document Expenditures

By Category, 1987



Printing:	$ 51000
Labor:	$ 21000
Shipping:	$ 5000

Total SRI expenditures:	$ 77000

4/7/88

NIC PROVIDES ONE-STOP INFORMATION SHOPPING

- Answer Questions
- Provide POCs
- Identify Related Documents
- Provide Document Ordering Info
- Provide Documents Themselves
  - Low Cost, Pay-As-You-Go Services
  - Special Handling
  - Not Printed With Govt Funds
- Provide Info Products

4/7/88

NIC CREATES GOODWILL

- Welcome Users to the Network
- Orient Subscribers and Contractors
- Go That Extra Step for Answers
- Treat Customers Courteously
- Make a Good Showing on Behalf of DCA

4/7/88

TOPICS TO BE COVERED

- DDN Information Infrastructure
- Augmenting Users and Subscribers
- OSI Naming and Distributed Domains
- Protocol Transition and Technology Transfer
- Email for Military Users
- Information Management Tools
- Audit Trail and Billing System

4/6/88

DDN NAMING AND ADDRESSING

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

NIC Role

- Teamwork -OSD, DCA, DARPA, NSF, NIC, MITRE
- 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

4/6/88

NAME SERVICE RESEARCH EFFORT
DISTRIBUTED WHOIS
OSI DIRECTORY SERVICES

NIC is combining efforts with:

- DSAB WG
- IETF WG
- INTERNICS
- NSF
- NBS
- NARDAC

4/6/88

DDN Growth

Network Naming and Addressing Statistics

	Apr 1987	Apr 1988
Internet Hosts (includes ARPANET/MILNET)	3,372	5,548
ARPANET/MILNET Hosts	776	1683
ARPANET/MILNET TACs	141	182
ARPANET/MILNET GWs	133	179
Internet Gateways	182	233
ARPANET/MILNET Nodes	209	245
Connected Networks	587	865
Domains (top-level, 2nd-level)	282	506
Hostmaster online mail	1422	1626

(Size of current host table = 598,881 bytes)

4/7/88

TOPICS TO BE COVERED

- DDN Information Infrastructure
- Augmenting Users and Subscribers
- OSI Naming and Distributed Domains
- Protocol Transition and Technology Transfer
- Email for Military Users
- Information Management Tools
- Audit Trail and Billing System

4/7/88

SRI IS A WELL-KNOWN PROTOCOL INFORMATION SOURCE

- Helped Design ARPANET/DDN
- Wrote TCP/IP
- Assisted with TCP/IP Transition
- Have Implemented DoD Protocols
- Know all the Players
- Active in Standards Bodies
  - DoD, ISO, CCITT, IFIP, ANSI
- Take a Neutral Stance
  - No "Religion"
  - No Product Line
- Cooperate With
  - PSSG, IETF, MILCOMS
  - DCEC, ANSI, COS
  - NSF, NBS, DARPA
- Coordinate the Host Administrators
- SRI Research Expertise for Back-up

4/7/88

NIC ROLE IN TRANSITION

- Serve as Info Clearinghouse
  - Contractors
  - Vendors
  - Subscribers
  - Researchers
  - Users
- Provide POCs
- Provide Documentation
  - RFCs and IDEAS
  - Directives
  - Protocol Handbook
  - Sound the Alert
  - Mgt Bulletins
  - Heads-Up Broadcasts

Provide Protocol Repository

- Provide Liaison
  - POCs, NMCs, DTIC, Other Military NICs

4/7/88

TOPICS TO BE COVERED

- DDN Information Infrastructure
- Augmenting Users and Subscribers
- OSI Naming and Distributed Domains
- Protocol Transition and Technology Transfer
- Email for Military Users
- Information Management Tools
- Audit Trail and Billing System

4/7/88

NIC IS BOMBARDED BY
USERS
SUBSCRIBERS
POCs
WANTING ACCESS TO EMAIL

4/7/88

MORE THAN A THIRD OF THE HOST ADMINISTRATORS DO NOT HAVE EMAIL ACCESS

4/7/88

PROBLEMS CREATED

- DCA Cannot Manage Net Effectively
- POCs Do Not Receive Required Info
- POCs Do Not Know Environment
- Systems Do Not Function Properly
- Tables Are Outdated
- POCs Cannot Perform Role
- POCs Cannot Assist Users
- Time And $$ Are Wasted

ELECTRONIC MAIL EXPERTISE

Office Environment

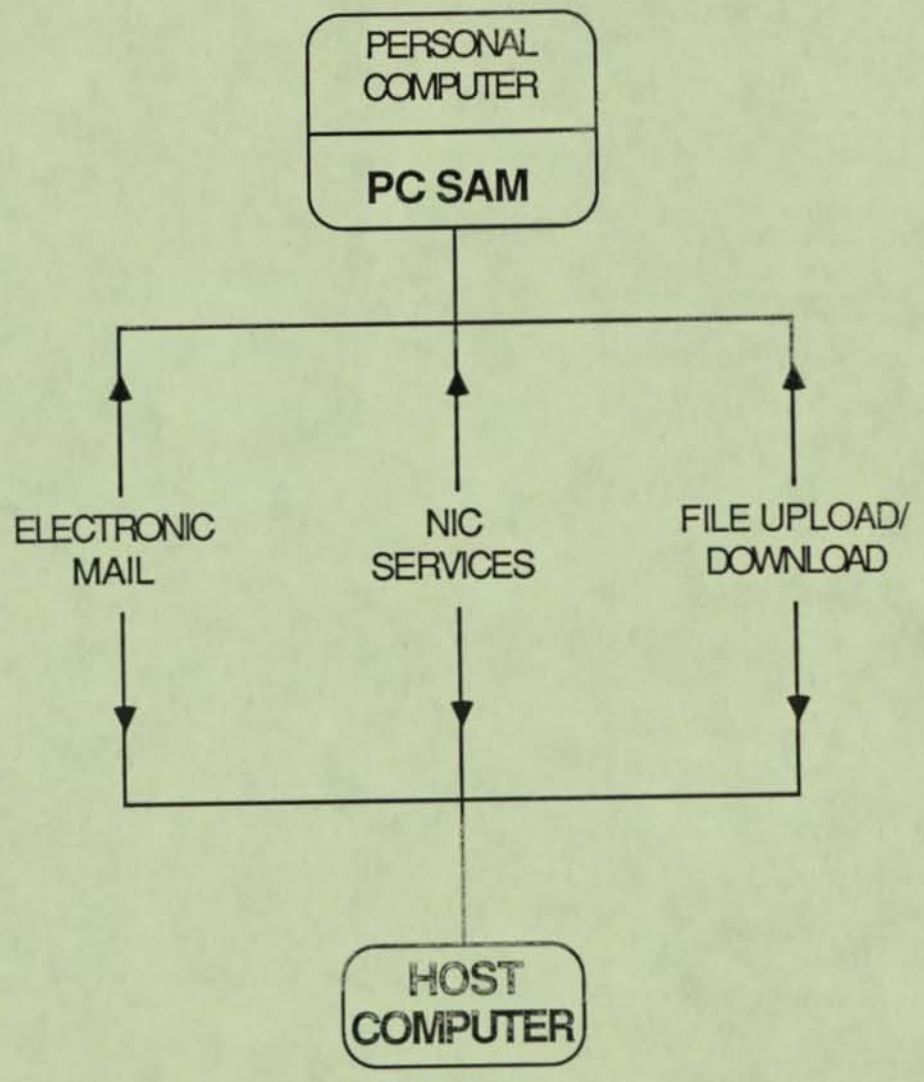
- Extensive PC and Workstation experience
- SAM

Campus Environment - SRINET

- Multiple hosts/operating systems
- Wide variety of mail handling programs
- Covers large campus
- Large number of users (1000+)
- Extensions to SRI Washington office

SRI/NISC MAIL SERVICE POSSIBLITIES

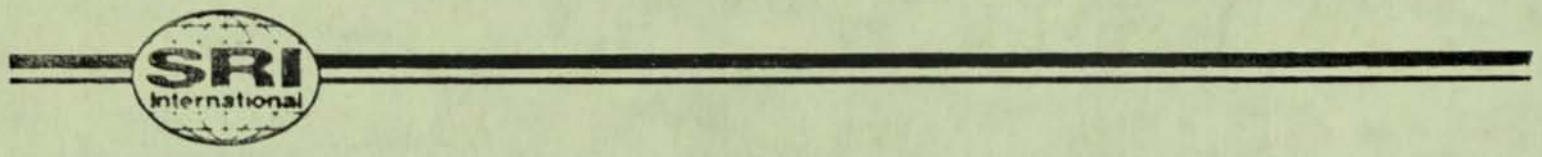
- Provide mailboxes for POCs
  - SRI host or other host
  - Self supporting via subscription
- Provide coordination with military commands
- Set up self supporting mail hosts
- SAM



NETWORK ACCESS VIA PC

PC SAM

Simple Access to e-Mail



Features

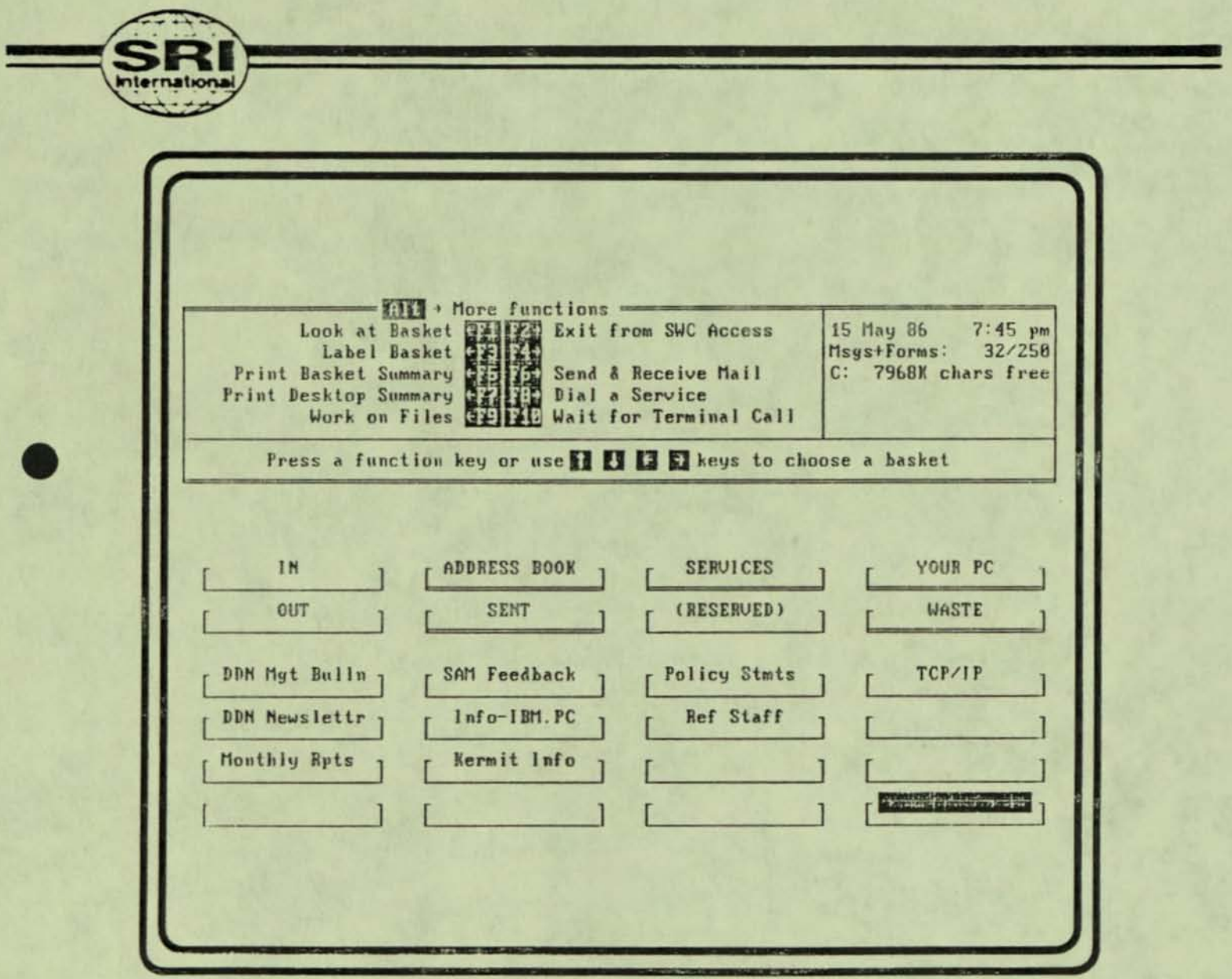
- Friendly User Interface
- Automatic Mail, Automatic Login
- VT100 Terminal Emulation
- Mail and DOS File Management

4/7/88

SAM, VERSION 2

- Background Operation
- Windows (Memory Dependent)
- Editor with Search Capability
- Enhanced KERMIT Capabilities
- Improved Password Protection
- Increased Basket Capacity
- Message Archiving
- Access to NIC Services
- Address Book
- Handles Large Messages as Files
- Online Screen Buffer
- Zenith COM3 Port Support
- VT100 Emulation in Mail Service

S A M Desktop

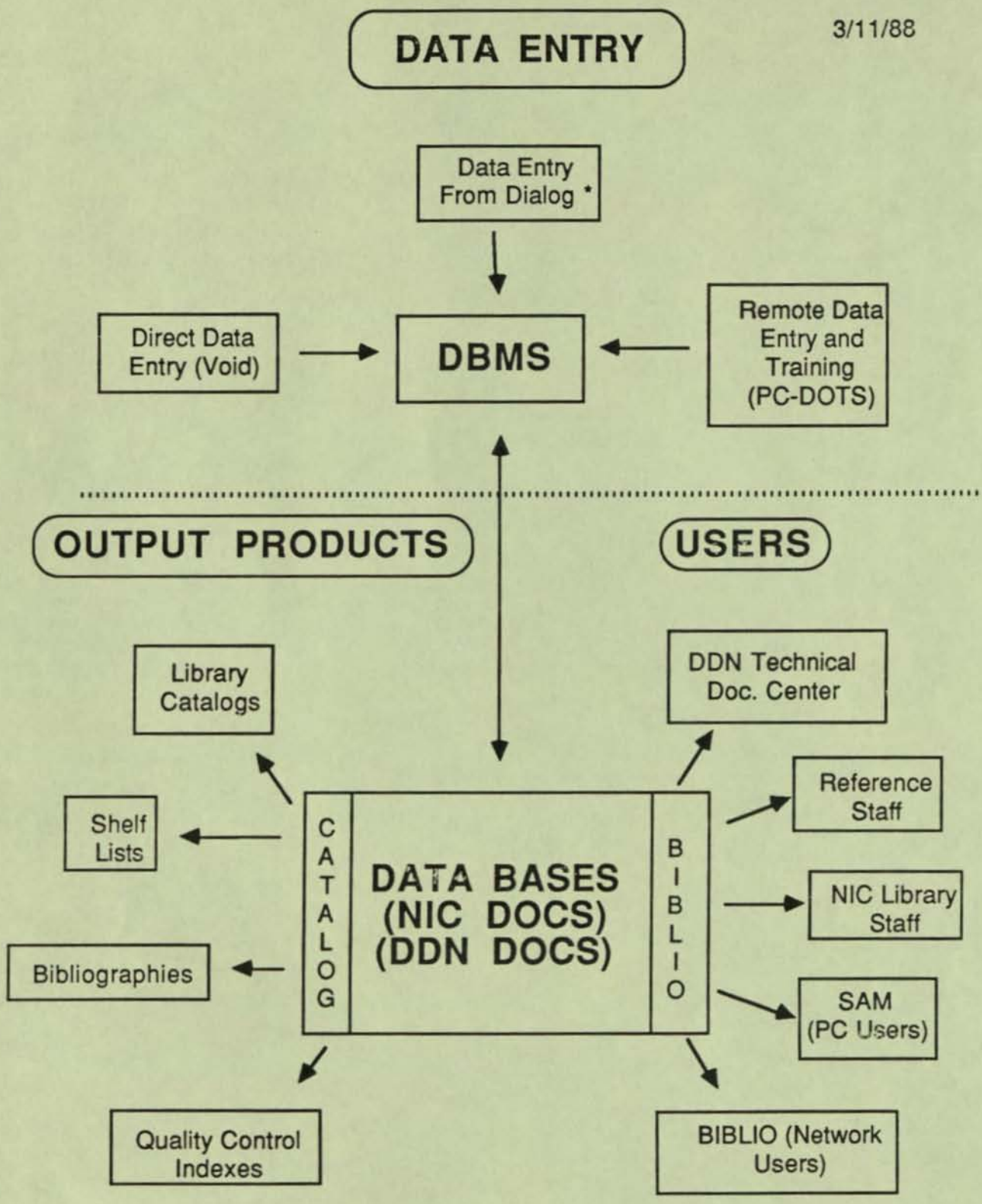

Alt → More functions
Look at Basket
Label Basket
Print Basket Summary
Print Desktop Summary
Work on Files
Exit from SWC Access
Send & Receive Mail
Dial a Service
Wait for Terminal Call
15 May 86 7:45 pm
Msgs+Forms: 32/250
C: 7968K chars free
Press a function key or use keys to choose a basket
IN
ADDRESS BOOK
SERVICES
YOUR PC
OUT
SENT
(RESERVED)
WASTE
DDN Mgt Bulln
SAM Feedback
Policy Stmts
TCP/IP
DDN Newslettr
Info-IBM.PC
Ref Staff
Monthly Rpts
Kermit Info

4/7/88

TOPICS TO BE COVERED

- DDN Information Infrastructure
- Augmenting Users and Subscribers
- OSI Naming and Distributed Domains
- Protocol Transition and Technology Transfer
- Email for Military Users
- Information Management Tools
- Audit Trail and Billing System

3/11/88



NIC Information Tools

* Available but not currently used

4/7/88

NIC SOFTWARE STATUS

- Just Completing "C" Conversion
- Extensive "C" Program Library
- Converting to Relational DBMS
- Many UNIX-Based, Portable Tools
- Converting to Smaller, Cheaper Equipment for Easy Replication
- Can Act As Reference and Shareware Source for DCA
- Positioned for Distributed NIC Services
- All Systems Documented

4/7/88

NIC CAN SHARE RESOURCES

- Host Tables
- WHOIS Server
- Domain Name Server
- "C" Compiler
- VOID DBMS
- User-Interface Programs to Servers
- Remote Data Entry Programs

4/7/88

TOPICS TO BE COVERED

- DDN Information Infrastructure
- Augmenting Users and Subscribers
- OSI Naming and Distributed Domains
- Protocol Transition and Technology Transfer
- Email for Military Users
- Information Management Tools
- Audit Trail and Billing System

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)

TACACS

Terminal Access Control System

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

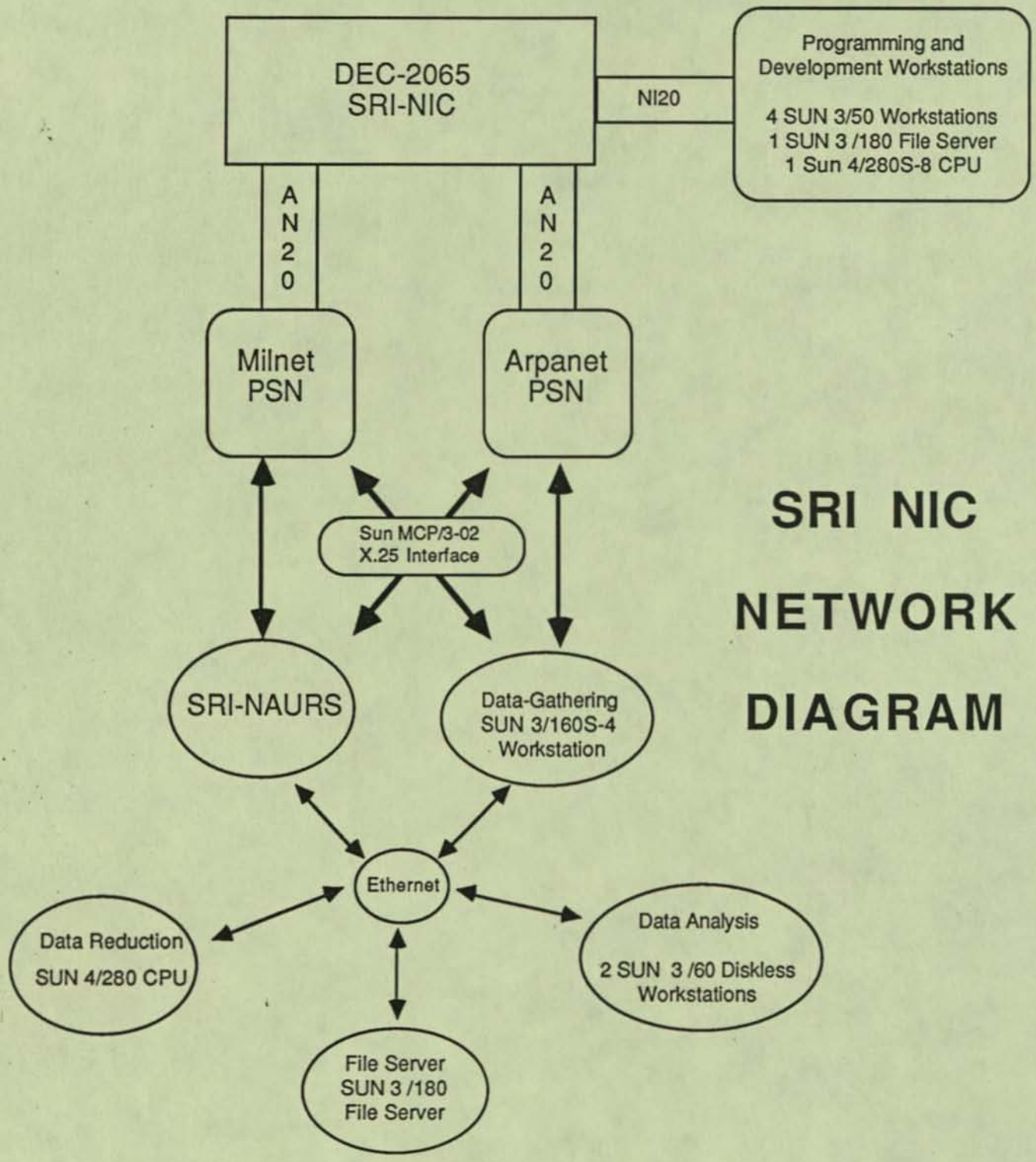
Network Audit Trail System

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

Billing System

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

4/7/88



SRI NIC NETWORK DIAGRAM

4/7/88

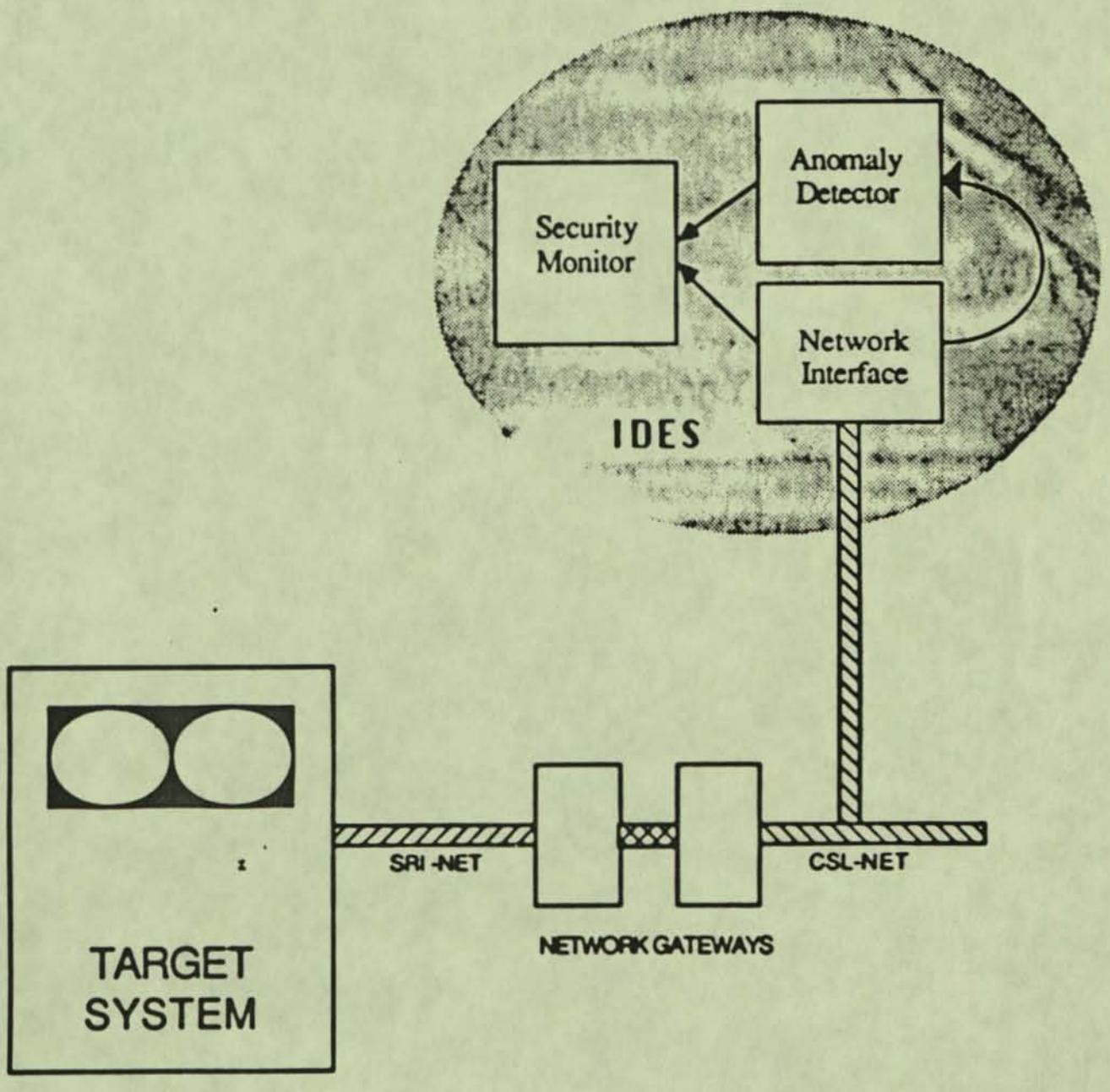
PROBLEMS

- Need Clean Data From NCDs, BBN
- Need Decisions By DCA/DECCO
- Need to Resume NAURS WG
- Stop Delays in Obtaining Equipment (2 1/2 Yrs for 8 Workstations)
- Deadline Is Approaching

Future

- Profile User Activities
    - An IDES application
- Expert system
- Audit-Trail Protocol enhancements
- Portable NAURS
- Applicability to other (classified) networks

SRI Intrusion Detection System



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

2823-87

COMMENTS ON DCA CIRCULAR 310-P70-74 9/30/87
TERMINAL ACCESS CONTROLLER USER'S GUIDE

DDN Network Information Center
By Steve Dennett, Hal Huntley, Steve Mason,
Francine Perillo and Scott Smith

General comments:

The document covers a very broad spectrum of users, from the novice to the experienced. There is a noticeable transition in the text from the introductory to advanced commands and their descriptions. In the overview, the novice and advanced user could be directed to those sections that would be most useful to each respective group.

There are concepts and commands presented that seem to be unique to Release 114 and later, yet in many instances the user is not informed of this fact. Specific examples can be found on page 1-5, section 5-c-(4)-(a) and on page 4-2, section 3-b-(4). Overall, the document is well organized, informative and easy to understand with many helpful examples.

The document should be widely distributed and easy to obtain. In addition to being available through the DCA Circulars office, the document should be obtained through some other source, for the benefit of the many non-military users of the DDN.

Specific comments:

Paragraph	Comment
iii-3	# sign in the right margin on the same line as character size. Is it extraneous? They are scattered throughout the document.
v	NIC. Add a comment about issuing TAC cards. Add ARPANET, MILNET, OCONUS and SAPVAL to the list.
[pg 1-1]	
1	Suggest modifying the first sentence to: "...describes where to get help with TAC access procedures,...".
2-b	For clarity, the first sentence should say: "Terminals can be connected to the DDN through the TAC, or indirectly through a host." The fourth sentence should say: "The terminal may be connected to the TAC by a direct line, or it may be connected through a dial-up line;..." In the last sentence in this paragraph, "into" should be "in to". Comment: Aren't all DDN TACS running TACACS? The sentence that says: "...the system may include the TAC Access Control System..." sounds like there are some TACs that are not.
2-c	Change the first sentence to: "The network can be considered as a way in which a remote computer (usually called a host) and the user's terminal can communicate."

REPORTS

2-d	We prefer TACs & PSNs (without the apostrophe).
3	The second sentence says: "Normally, the protocol is not visible at the terminal." What does this mean? What does one do if one appears? What do they look like?
3a	A better definition of protocol is needed.
Figure 1-1	Need the picture to evaluate.
[pg 1-3]	
4	We're called "Network Information Center (NIC) User Assistance", not "Customer Assistance Desk". Re: "News". The sentence should read: "In addition, there is a "News" command "@N [RETURN]" which connects the user to the NIC's computer. On that computer are various programs containing network information."
4-a	We're called "Network Information Center (NIC) User Assistance", not "Customer Assistance Desk". Re: CONUS. Isn't CONUS considered to include Hawaii? If so, it should say "CONUS and Hawaii". Give the hours of the NIC.
5-b-(1)	Put a hyphen in "at sign".
[pg 1-4]	
5-b-(2)	Hyphen in "at sign". The last sentence would be clearer if stated: "The intercept character may be echoed a third time after typing it twice." As currently stated, the user might expect to see five at-signs.
5-b-(4)	Modify the text to say: "@R [RETURN]" will reset the TAC port and break the connection to the host if it has been established.
5-c-(1)-(a)	What is "a full period communication line" with modems?
5-c-(1)-(b)-2	In the sentence: "At the user provided end..." Omit "provided" or put a hyphen in between user and provided.
5-c-(1)-(b)-3	It is saying acoustic couplers are datasets, correct? "...instructions for usage" could be stated "...usage instructions".
[pg 1-5]	
5-c-(2)-(b)	A data set is a modem? I thought a data set was an acoustic coupler from 5-c-(1)-(b)-3 above. Then, an acoustic coupler is a modem? These terms should be defined possibly in 5-c-(1)-(b)-3. Put a hypen between user and provided.
5-c-(3)	Line speed and baud rate are established conventions, use them. Will the use of [BREAK] [CONTROL-Q] be true in Release 114? If true, say so, because it doesn't work now.

5-c-(4)-(a) In actual operation, the TAC herald does not have this line: "Type @o [address or hostname]. Will that be part of Release 114?

5-c-(4)-(b) Add "(or TAC banner)" after "Tac herald."

It should be indicated that for the Pacific region, the herald says: CALL THE PMMC AT AV 455-1472/3
OR COM 808 655-1472/3 FOR HELP

Also, the text states: "The second line tells how to connect to a host as an aid to users." This is not shown in the example. As a general comment, it should be stated that there is no "prompt" for a TAC. The cursor is at the left of the screen, waiting for a command to be given after the banner is displayed.

5-c-(4)-(c) What is a "normal" TAC login capability? Do you mean to imply that there are TACs on the DDN that do not have TACACS?

5-c-(5)-(a) The connection between the @O and (letter) is not clearly established. It could be interpreted to mean "enter @O, then some letter, and then a host address..."

[pg 1-6]

5-c-(6)-(a) To aid the user, it might be clearer to say "@O (the letter 'o')". Adding the extra words clarifies the explanation of the previous character and not "some letter" that the user needs to type before the [space]. The use of "Enter:" could be misleading, because the person might think they will see the word "Enter:" before they type the "@O". Suggestion: "There is no prompt after the TAC banner, just enter:"

5-c-(6)-(b) Responses from the TAC should have "code" capitalized. As in "Access Code:"

5-c-(6)-(c) "code" in "Access code:" should be capitalized. The TAC responds with "trying" capitalized. As in "TCP Trying..."

5-c-(6)-(d) "Bad Login" should be "Bad login". Should make the point that after three incorrect tries, the TAC will disconnect and the user will have to re-establish a TAC connection.

5-c-(6)-(e) Should say: "TACACS cards are issued by the NIC; the user should contact the Host Administrator to request a TACACS card." This is the first place the Host Administrator is mentioned. The HA should be explained before this point, or mention a section where the HA is explained.

[pg 1-7]

5-d-(1) The first sentence would be clearer if it stated: "As explained in the previous section, the TAC displays its herald once the TAC and the terminal have agreed on the line rate."

5-e Should say..."After logging out from the host, close

the TAC connection to the host.

5-e-(1) Say: "For the sites without TACACS, close the TAC-host connection by entering:"

And : "This command closes the connection between the TAC and host, displaying no response on the screen." It is a good idea to highlight the TAC-host connection.

5-e-(2) "For the sites with TACACS, close the TAC-host connection by entering..." It needs to be clear which connection is being closed by @C.

5-e-(2) After the user enters @C and @L the TAC responds with: "Logged out". This is missing from the text.

5-e-(3) How long after logout does it take the TAC to close the port, if the user does not perform the @C & @L? Is there a timeout period for the TAC? If so, what is it?

Comment: There is a blank page following 1-7. Will there be a diagram? There are no blank pages following subsequent chapters.

[pg 2-1]

2-c ..."Reset to Initial Configuration (@R I C) command..." The "to" could be omitted.

2-d DCAB651@DDN1 should be DCAB651@DDN1.ARPA

[pg 3-1]

2-a Last sentence should be punctuated: "Error messages, as well as procedures for entering an intercept character as text, are also discussed."

[pg 3-2]

2-b-(6) There is not a table with the different device rate settings and the corresponding baud rates. Previous TAC guides have this table.

2-c The intercept character is referred to as (the @ sign), earlier it was (the at sign). Be consistent throughout. "A space is not required between the @ and the first word." Sounds like a space is optional. It would be better to say, "There must not be a space between the @ and the first word or letter."

2-d After an abort, there is no indication from the system to indicate this.

[pg 3-3]

2-f Delete ";the third @ was echoed by the host".

3-a First sentence, delete "in order". Second sentence,

should state: "The user can assume that communication has been established when the TAC herald is displayed."

3-b — "line rates" could be "baud rates".

3-c — First sentence could be edited to: "If the herald message is displayed, the port is set to the correct baud rate." Delete "In either case", in the last sentence.

3-d — OCONUS not defined. Line noise could be a factor in garbled messages.

4-a — Text should contain a commment that some TAC ports used for dial-in access to DDN are either 300 or 1200 only.

[pg 3-4]

4-c-(3) — Does using [BREAK] in this situation behave like @R I C?

[pg 3-5]

6-c-(1)-(c) — Why are padding and parity mutually exclusive? More discussion needed.

6-d-(1) — @DEVICE CODE ASCII (@D C A) [RETURN]
From this point on, none of the TAC commands are followed with "[RETURN]". It was used earlier in the text, so be consistent and use throughout.

[pg 3-6]

7-a — Delete "negotiate a" from the second sentence.

7-b — DCAB651@DDN1 should be DCAB651@DDN1.ARPA

[pg 3-7]

7-c — Good Table 3-1!!

7-d — What does the "Entered @I 13" refer to?

[pg 3-8]

8 — Reverse the order of @R I C and @R as they are discussed later in the text in that order.

[pg 3-11]

10 — The last two sentences in this paragraph are out of place. The way the paragraph is written, the reader must read back to the beginning of the paragraph to find out the causes of two cases. One remedy would be to mention the cause and solution together.

10-a — The NIC does not maintain the information about which type of flow control is enabled at the TAC. Should be MC?

[pg 3-12]

10-b-(1)	Good description!
10-c-(2)-(b)	Typo: Delete the carriage return after the semi-colon.
[pg 3-13]	
10-d-(1)	There are three different references to chapter 5. What are these sections of chapter 5? It could be mentioned that Binary Mode disables the TAC intercept character and local TAC commands.
[pg 4-1]	
2-a	Reverse the order of a and b. Set the terminal baud rate before you dial the TAC.
3-a	"Specify a host by supplying a network address or hostname..." Hostnames have not been available on previous TACs. Will this be true for Release 114?
3-b-(1)	An indication that there is a space between the @OPEN and a.b.c.d would be helpful for new users.
[pg 4-2]	
3-b-(3)	A hostname example would be helpful for new users. Why isn't the hostname example mentioned in the previous section on @O?
3-b-(4)	Is this valid for Release 114 and later? It would be nice feature to allow the use of hostnames with the OPEN command.
3-b-(6)-(b)	TAC actually responds with "TCP Trying..." (trying is capitalized), the same with "Open."
3-b-(6)-(c)	How long does the TAC continue to retransmit? The sentence seems to imply that it would continue indefinitely.
[pg 4-3]	
3-c	Re: Bad & Can't. One refers to the network address and the other refers to the internet address. Use consistent terminology; one or the other.
3-c	"trying" should be capitalized.
4-b	"trying" should be capitalized.
[pg 4-4]	
5-a-(2)	"userid" should be capitalized".
5-a-(3)	Change to: "Enter your TAC user identification, followed by [RETURN]. If your identification is not..."
5-a-(4)	Same as above.
5-a-(5)	Same as above).
5-a-(6)	Should be: "Login Ok

TCP Trying...Open".

5-a-(7)	"trying" should be capitalized.
5-b	Change "Release 113 and beyond" to "Release 113 and later" throughout the draft. The use of "beyond" is not appropriate in this context.
[pg 4-5]	
5-c-(1)	Drop the comma after access code.
5-c-(3)-(a)	"code" should be capitalized.
5-c-(3)	"Bad Login" should be "Bad login".
5-c-(3)-(b)	Should be a <cr> after Bad Login and login should be lowercase.
5-c-(4)	"Login" should be lowercase.
[pg 4-6]	
5-e	"Login" should be lowercase.
[pg 4-7]	
6-d-(2)	SAPVAL not defined.
7-b	Release 114?
[pg 4-9]	
9	"userid" (in Table 4-1) should be capitalized.
[pg 4-10]	
10-a-(4)	Change the last sentence to: "If on TACACS, you may use the Open command without having to go through the TAC login procedure again."
11	The discussion of the @R and @R I C command should be in the same order as they are on the following page.
[pg 4-11]	
11-a-(2)-(b)	Where in chapter 5? Be more specific about the section.
11-c	TAC 114 should be: TAC Release 114.
[pg 4-12]	
12	Log off and log out are used interchangeably, suggest use one or the other.
12	Delete "in order". What happens if you don't log off the TAC?
12-d	Should mention that on dial-up, the phone connection can only be broken by hanging up the phone.

[pg 5-1]

1	Last paragraph is less clear than last definition.

[pg 5-2]

3-c	Must a connection be open for the user to request binary mode? Clarify.
3-f	What must a user do to disable XON/XOFF?

[pg 5-3]

4	It would be useful to have a discussion in this section about why a person might want to transmit on word or on message instead of character or every number of characters.
4-c	Is @T E O (letter or zero?)

Supplement 1

2	@Close...How many minutes have to elapse before port closes on its own? Autologout exist on the TAC?
2	@Flush..."Note" should be followed with a dash or a colon.
3	@Open...Refers to chapter 5 for a discussion of special Open formats. They are located in Supplement 4.
4	@Send Abort Output..."Note" should be followed with a dash or a colon.

Supplement 2

4	Login expired...Refers to the discussion of the @U command. Expired login is not discussed in the @U section.

Supplement 4

2-b-(2)	Use a multiplication symbol in the formula to indicate the operation.

2824-87

COMMENTS ON DCA CIRCULAR 310-P70-74 9/30/87
TERMINAL ACCESS CONTROLLER USER'S GUIDE

DDN Network Information Center

By Jake Feinler, Steve Dennett, Hal Huntley,
Steve Mason, Francine Perillo and Scott Smith

General comments:

The document covers a very broad spectrum of users, from the novice to the experienced. There is a noticeable transition in the text from the introductory to advanced commands and their descriptions. In the overview, the novice and advanced user could be directed to those sections that would be most useful to each respective group.

There are concepts and commands presented that seem to be unique to Release 114 and later, yet in many instances the user is not informed of this fact. Specific examples can be found on page 1-5, section 5-c-(4)-(a) and on page 4-2, section 3-b-(4). Users would find it very helpful to have a table for quick reference which outlines the differences between TAC Release 113 and TAC Release 114. This could be added as an appendix.

One of the most frequent problems that comes up on the NIC "hotline" is that of personal computer (PC) users having difficulty using their computers as terminals to access a TAC. It would be very useful if the TAC User Guide included a section addressing some of these problems.

In Chapter 1, Section 2, "Connecting to the Network Using a TAC", the emphasis is on reaching the DDN through a TAC. This section implies this as the goal of using a TAC. The goal is to use the DDN to get to a host or a service (program) where one either has an account to log into or can find information. It is important to make this clear because many users have been confused about this point. This is particularly true for personal computer users who often believe that just accessing the DDN through a TAC will allow them to communicate with all the other PCs so attached. The concept of a host computer on which one does work or has an electronic mail account seems to be missing as the objective of using the network. It is not clear that the TAC access is merely the closest access point to the DDN backbone and that the backbone will then take the user to the host computer of choice. Perhaps a few sentences could be added or enhanced to make this point.

Consistency in punctuation, capitalization and within secenarios is important. For example, TACs vs. TAC's; "Bad login" rather than "Bad Login" (lower case l for login); and the consistent use of [RETURN] within the user scenarios.

This is a key document for DDN users. It needs very wide distribution and is in high demand. It would be useful if the document were made available through a number of sources, because many non-military users are unfamiliar with DCA Circulars and how to obtain one. In the past the document has been available first from BBN and then the NIC. Users found this useful. If it will no longer be available from these sources, perhaps it might also be deposited at NTIS where it would be more readily

available to non-military users. We strongly suggest that an online reference copy be stored on the SRI-NIC.ARPA host for use by military sites who may wish to incorporate portions of it into documents they are preparing.

Overall, the document is well organized, informative and easy to understand with many helpful examples.

Specific comments:

Paragraph	Comment
iii-3	# sign in the right margin on the same line as character size. Is it extraneous? They are scattered throughout the document.
v	NIC. Add a comment about issuing TAC cards. Add ARPANET, MILNET, OCONUS and SAPVAL to the list.
[pg 1-1]	
1	Suggest modifying the first sentence to: "...describes where to get help with TAC access procedures,...".
2-b	For clarity, the first sentence should say: "Terminals can be connected to the DDN through the TAC, or indirectly through a host." The fourth sentence should say: "The terminal may be connected to the TAC by a direct line, or it may be connected through a dial-up line;..." In the last sentence in this paragraph, "into" should be "in to". Comment: Aren't all DDN TACS running TACACS? The sentence that says: "...the system may include the TAC Access Control System..." sounds like there are some TACs that are not.
2-c	Change the first sentence to: "The network can be considered as a way in which a remote computer (usually called a host) and the user's terminal can communicate."
2-d	We prefer TACs & PSNs (without the apostrophe).
3	The second sentence says: "Normally, the protocol is not visible at the terminal." What does this mean? What does one do if one appears? What do they look like?
3a	A better definition of protocol is needed.
Figure 1-1	Need the picture to evaluate.
[pg 1-3]	
4	We're called "Network Information Center (NIC) User Assistance", not "Customer Assistance Desk". Re: "News". The sentence should read: "In addition, there is a "News" command "@N [RETURN]" which connects the user to the NIC's computer. On that computer are various service programs providing network information."
4-a	We're called "Network Information Center (NIC) User Assistance", not "Customer Assistance Desk".

Re: CONUS. It should say "CONUS and Hawaii". Also, give the hours of the NIC.

5-b-(1) Put a hyphen in "at sign".

[pg 1-4]

5-b-(2) Hyphen in "at sign". The last sentence would be clearer if stated: "The intercept character may be echoed a third time after typing it twice." As currently stated, the user might expect to see five at-signs.

5-b-(4) Modify the text to say: "@R [RETURN]" will reset the TAC port and break the connection to the host if it has been established.

5-c-(1)-(a) What is "a full period communication line" with modems?

5-c-(1)-(b)-2 In the sentence: "At the user provided end..." Omit "provided" or put a hyphen in between user and provided.

5-c-(1)-(b)-3 It is saying acoustic couplers are datasets, correct? "...instructions for usage" could be stated "...usage instructions".

[pg 1-5]

5-c-(2)-(b) A data set is a modem? I thought a data set was an acoustic coupler from 5-c-(1)-(b)-3 above. Then, an acoustic coupler is a modem? These terms should be defined possibly in 5-c-(1)-(b)-3. Put a hypen between user and provided.

5-c-(3) Line speed and baud rate are established conventions, use them. Will the use of [BREAK] [CONTROL-Q] be true in Release 114? If true, say so, because it doesn't work now.

5-c-(4)-(a) In actual operation, the TAC herald does not have this line: "Type @o [address or hostname].
Will that be part of Release 114?

5-c-(4)-(b) Add "(or TAC banner)" after "Tac herald."

It should be indicated that for the Pacific region, the herald says: CALL THE PMMC AT AV 455-1472/3
OR COM 808 655-1472/3 FOR HELP

Also, the text states: "The second line tells how to connect to a host as an aid to users." This is not shown in the example. As a general comment, it should be stated that there is no "prompt" for a TAC. The cursor is at the left of the screen, waiting for a command to be given after the banner is displayed.

5-c-(4)-(c) What is a "normal" TAC login capability? Do you mean to imply that there are TACs on the DDN that do not have TACACS?

5-c-(5)-(a) The connection between the @O and (letter) is not

clearly established. It could be interpreted to mean "enter @O, then some letter, and then a host address..."

[pg 1-6]

5-c-(6)-(a) To aid the user, it might be clearer to say "@O (the letter 'o')". Adding the extra words clarifies the explanation of the previous character and not "some letter" that the user needs to type before the [space]. The use of "Enter:" could be misleading, because the person might think they will see the word "Enter:" before they type the "@O". Suggestion: "There is no prompt after the TAC banner, just enter:"

5-c-(6)-(b) Responses from the TAC should have "code" capitalized. As in "Access Code:"

5-c-(6)-(c) "code" in "Access code:" should be capitalized. The TAC responds with "trying" capitalized. As in "TCP Trying..."

5-c-(6)-(d) "Bad Login" should be "Bad login". Should make the point that after three incorrect tries, the TAC will disconnect and the user will have to re-establish a TAC connection.

5-c-(6)-(e) Should say: "TACACS cards are issued by the NIC; the user should contact the Host Administrator on the host where he or she has an account to request a TACACS card." TAC cards are not issued to users who do not have host accounts. Also, this is the first place the Host Administrator (HA) is mentioned. The HA should be explained before this point, or mention a section where the HA is explained.

[pg 1-7]

5-d-(1) The first sentence would be clearer if it stated: "As explained in the previous section, the TAC displays its herald once the TAC and the terminal have agreed on the line rate."

5-e Should say..."After logging out from the host, close the TAC connection to the host.

5-e-(1) Say: "For the sites without TACACS, close the TAC-host connection by entering:"

And : "This command closes the connection between the TAC and host, displaying no response on the screen." It is a good idea to highlight the TAC-host connection.

5-e-(2) "For the sites with TACACS, close the TAC-host connection by entering..." It needs to be clear which connection is being closed by @C.

5-e-(2) After the user enters @C and @L the TAC responds with: "Logged out". This is missing from the text.

5-e-(3) How long after logout does it take the TAC to close the port, if the user does not perform the @C & @L? Is there a timeout period for the TAC? If so, what is it?

Comment: There is a blank page following 1-7. Will there be a diagram? There are no blank pages following subsequent chapters.

[pg 2-1]

2-c ..."Reset to Initial Configuration (@R I C) command..." The "to" could be omitted.

2-d DCAB651@DDN1 should be DCAB651@DDN1.ARPA

[pg 3-1]

2-a Last sentence should be punctuated: "Error messages, as well as procedures for entering an intercept character as text, are also discussed."

[pg 3-2]

2-b-(6) There is not a table with the different device rate settings and the corresponding baud rates. Previous TAC guides have this table.

2-c The intercept character is referred to as (the @ sign), earlier it was (the at sign). Be consistent throughout. "A space is not required between the @ and the first word." Sounds like a space is optional. It would be better to say, "There must not be a space between the @ and the first word or letter."

2-d After an abort, there is no indication from the system to indicate this.

[pg 3-3]

2-f Delete ";the third @ was echoed by the host".

3-a First sentence, delete "in order". Second sentence, should state: "The user can assume that communication has been established when the TAC herald is displayed."

3-b "line rates" could be "baud rates".

3-c First sentence could be edited to: "If the herald message is displayed, the port is set to the correct baud rate." Delete "In either case", in the last sentence.

3-d OCONUS not defined. Line noise could be a factor in garbled messages.

4-a Text should contain a commment that some TAC ports used for dial-in access to DDN are either 300 or 1200 only.

[pg 3-4]

4-c-(3) Does using [BREAK] in this situation behave like @R I C?

[pg 3-5]

6-c-(1)-(c)	Why are padding and parity mutually exclusive? More discussion needed.
6-d-(1)	@DEVICE CODE ASCII (@D C A) [RETURN] From this point on, none of the TAC commands are followed with "[RETURN]". It was used earlier in the text, so be consistent and use throughout.
[pg 3-6]	
7-a	Delete "negotiate a" from the second sentence.
7-b	DCAB651@DDN1 should be DCAB651@DDN1.ARPA
[pg 3-7]	
7-c	Good Table 3-1!!
7-d	What does the "Entered @I 13" refer to?
[pg 3-8]	
8	Reverse the order of @R I C and @R as they are discussed later in the text in that order.
[pg 3-11]	
10	The last two sentences in this paragraph are out of place. The way the paragraph is written, the reader must read back to the beginning of the paragraph to find out the causes of two cases. One remedy would be to mention the cause and solution together.
10-a	The NIC does not maintain the information about which type of flow control is enabled at the TAC. Should be MC?
[pg 3-12]	
10-b-(1)	Good description!
10-c-(2)-(b)	Typo: Delete the carriage return after the semi-colon.
[pg 3-13]	
10-d-(1)	There are three different references to chapter 5. What are these sections of chapter 5? It could be mentioned that Binary Mode disables the TAC intercept character and local TAC commands.
[pg 4-1]	
2-a	Reverse the order of a and b. Set the terminal baud rate before you dial the TAC.
3-a	"Specify a host by supplying a network address or hostname..." Hostnames have not been available on previous TACs. Will this be true for Release 114?

3-b-(1) An indication that there is a space between the @OPEN and a.b.c.d would be helpful for new users.

[pg 4-2]

3-b-(3) A hostname example would be helpful for new users. Why isn't the hostname example mentioned in the previous section on @O?

3-b-(4) Is this valid for Release 114 and later? It would be nice feature to allow the use of hostnames with the OPEN command.

3-b-(6)-(b) TAC actually responds with "TCP Trying..." (trying is capitalized), the same with "Open."

3-b-(6)-(c) How long does the TAC continue to retransmit? The sentence seems to imply that it would continue indefinitely.

[pg 4-3]

3-c Re: Bad & Can't. One refers to the network address and the other refers to the internet address. Use consistent terminology; one or the other.

3-c "trying" should be capitalized.

4-b "trying" should be capitalized.

[pg 4-4]

5-a-(2) "userid" should be capitalized".

5-a-(3) Change to: "Enter your TAC user identification, followed by [RETURN]. If your identification is not..."

5-a-(4) Same as above.

5-a-(5) Same as above.

5-a-(6) Should be: "Login Ok
TCP Trying...Open".

5-a-(7) "trying" should be capitalized.

5-b Change "Release 113 and beyond" to "Release 113 and later releases" throughout the draft. The use of "beyond" is not appropriate in this context.

[pg 4-5]

5-c-(1) Drop the comma after access code.

5-c-(3)-(a) "code" should be capitalized.

5-c-(3) "Bad Login" should be "Bad login".

5-c-(3)-(b) Should be a [RETURN] after Bad Login and login should be lowercase.

5-c-(4) "Login" should be lowercase.

[pg 4-6]

5-e	"Login" should be lowercase.

[pg 4-7]

6-d-(2)	SAPVAL not defined.
7-b	Release 114?

[pg 4-9]

9	"userid" (in Table 4-1) should be capitalized.

[pg 4-10]

10-a-(4)	Change the last sentence to: "If on TACACS, you may use the Open command without having to go through the TAC login procedure again."
11	The discussion of the @R and @R I C command should be in the same order as they are on the following page.

[pg 4-11]

11-a-(2)-(b)	Where in chapter 5? Be more specific about the section.
11-c	TAC 114 should be: TAC Release 114.

[pg 4-12]

12	Log off and log out are used interchangeably, suggest use one or the other.
12	Delete "in order". What happens if you don't log off the TAC?
12-d	Should mention that on dial-up, the phone connection can only be broken by hanging up the phone.

[pg 5-1]

1	Last paragraph is less clear than last definition.

[pg 5-2]

3-c	Must a connection be open for the user to request binary mode? Clarify.
3-f	What must a user do to disable XON/XOFF?

[pg 5-3]

4	It would be useful to have a discussion in this section about why a person might want to transmit on word or on message instead of character or every number of characters.
4-c	Is @T E O (letter or zero?)

Supplement 1

2	@Close...How many minutes have to elapse before port closes on its own? Autologout exist on the TAC?
2	@Flush..."Note" should be followed with a dash or a colon.
3	@Open...Refers to chapter 5 for a discussion of special Open formats. They are located in Supplement 4.
4	@Send Abort Output..."Note" should be followed with a dash or a colon.

Supplement 2

4	Login expired...Refers to the discussion of the @U command. Expired login is not discussed in the @U section.

Supplement 4

2-b-(2)	Use a multiplication symbol in the formula to indicate the operation.

2825-86

COMMENTS ON DDN USER OPERATING PROCEDURES CIRCULAR 12/21/86

By Francine Perillo and Steve Dennett, with assistance
from Nancy Fischer and Ole Jacobsen

REPORTS

General comments:

Suggest using "login" rather than "logon" throughout document for consistency and for accuracy. For example, the "anonymous login convention" has been known for years on the network as containing the word "login" rather than "logon". Also, use of "logon" in document should be two words: "log on", when used as an action verb. "Logon" or preferably "login" is one word when used as an adjective, as in "login procedures" or "login convention".

This document seems to attempt many things--it serves to enlighten novices and system managers alike to network topics that vary in scope, detail and responsibility. This variation in scope made the document difficult to read because of the adjustment required on the part of the reader. Suggest as a solution to this that there be two main parts to the document: a section for the user and one for the subscriber, with references made to the other section when the information applies to both parties.

Specific comments:

Paragraph	Comment
Page ix	Typo on line "CMMC": Monitoring, not Monitorng.
2-2-c	Incorrect reference; info on subnets is in chapter 5.
2-2-d	We thought the ARPANET was a subnet of the DDN.
2-3-a	Unclear reference; need to state that further information can be found in the document listed there rather than implying that the actual information can be found there.
2-6	Format used for these references is very confusing. Makes it unclear whether underlined words are titles of documents or categories of information. Suggest that titles be italicized or in quotes to make that distinction. Source should be listed last, separately, as follows: "Defense Data Network System Description. References and a basic non-technical overview of the DDN. Includes a brief history....etc. To obtain, contact 8652. "
2-6	These references would be more useful if grouped, either by technical level or by intended audience (users/site personnel/programmers/etc.). Avoid uncertain tone of "...other information may include..." or "may also be provided". Should also include here as reference the "DDN Protocol Handbook" and the "DDN Protocol Implementations and Vendors Guide".
2-6-f	Many section of the DDN New User Guide are included in

this document--why list it here?

3-2-b — "...dial-up access at speeds from 300 to 2400 bps." Need to add a note that only one TAC currently supports 2400 bps.

3-2-f-(1) — Typo: maintain, not maintian.
^^

Table 3-1 — Remove blank lines and bars to improve readability, ie:

Transmission Medium	Typical Data Capacity
Twisted Pair (analog)	9.6 kbps
Twisted Pair (digital)	3 mbps
Microwave	90 mbps
etc...	

3-2-g and 3-2-g-(2) — Don't use "terminal users" for dial-up users; it is confusing, because *all* users use terminals. Call them instead "TAC users", which is clearer and more descriptive. Use "TAC access" rather than "terminal access" for the same reasons.

3-4-a-(3) — Definition of "TELNET" is too close to the commercial network, "TELENET". Suggest "virtual terminal connection".

3-5-d — Make reference here to "DDN X.25 Host Specification" doc.

4-4-a — Difficult to distinguish between classified and unclassified nets. Need to emphasize that on the unclassified nets *only* user traffic is encrypted, whereas on the classified nets user traffic *and* control functions are encrypted.

4-9-c — Third sentence "...these implementations are a user responsibility." Suggest "local Host Administrator" be substituted for "user".

4-9-d — HFEP's and TEP's should be defined.

6-3, 6-4 — User is much more likely to interact with HA than with NSC, so HA information should be put first (in the same way HA is listed first in 6-2).

6-3-b-(4) — Should refer to the section on the NIC here.

6-4-a-(2) — Everywhere else in document Host Administrator is abbreviated to HA; be consistent.

-------- — GENERAL NOTE: make references to other parts of document as specific as possible, rather than referring just to section numbers, ie: "see section 3-2-a" rather than "see section 3".

6-6-b	Incorrect reference to chapter 9; should be to Table 6-2.
	Last two sentences should be in para. 6-a, just before the last sentence of 6-a.
6-9-a	What is meant by "DDN MC's (both organic and contractor)" Are contractors inorganic? Confusing.
6-11 (Table 6-2)	For DDN NIC, put hotline number [(800) 235-3155] and commercial number [(415) 859-3695] after NIC address.
	Mailbox is HOSTMASTER@SRI-NIC.ARPA, not HOSTMASTERS@SRI-NIC.ARPA. ^
	For all other activities, online addresses have type: "*" should be "@", ie. "DCA-MMC*DCA-EMS" should be "DCA-MMC@DCA-EMS". ^
7-1-b-(1)	Don't enclose single-character keys with <>, ie. use @, not <@> (as in example).
	Also, suggest using curly-braces {} instead of angle-braces <> to enclose key names, because angle-braces are used by some systems to delimit directory names, whereas curly-braces aren't used for anything.
7-3	As before, the definition of "TELNET" should be changed. Ditto for all other definitions of "TELNET" in doc.
7-6-a	Should indicate that TACs currently require use of host addresses and not hostnames.
7-6-c	Reference needs to be more specific: refer to section 8-6, rather than just to chapter 8.
7-7-a-(2)	Indicate from whom to get permission.
7-7-a-(4)	Incorrect reference; should be "8-6", not "Chapter 8, paragraph 8".
7-7-b-(1)	Incorrect reference; should be 6-11, not "Chapter 9".
Table 7-1	The "o" for open was omitted from example.
7-8-c-(2)	TAC message is "Bad Login" not "Bad Logon". ^ ^
7-9-b-(2)	The intercept character (@) may be echoed a THIRD time, not THREE times.
7-11-d	Where is Supplement A?
Fig. 7-6	Mailboxs (pl.) should be Mailboxes. ^
7-13	Reference too general; should be 8-6.
8-2-c-(1)	The example of the mailbox should not have spaces in it.
8-3-b	This is accurately called the "anonymous login convention". ^

	"can not" should be one word.
8-3-f-(3)	The example appears to use a TOPS20 system example (with the "@" prompt) rather than a UNIX host as stated.
8-4-b	User should be referred to the latest "Assigned Numbers" RFC rather than to the RFC index for the latest list of of assigned socket numbers.
8-6-e-(5) and 8-6-e-(7)	Typos: WHOIS, not WHOSIS. ^
8-9	Suggest including the file NETINFO:00NETINFO-INDEX.TXT, which lists all files in NETINFO: and gives a brief description of each.
8-9-e	File name is TAC-PHONES.LIST ^
8-9-h	The file containing the list of SIGs is now three files: NETINFO:INTEREST-GROUPS-1.TXT NETINFO:INTEREST-GROUPS-2.TXT and NETINFO:INTEREST-GROUPS-3.TXT
Table 8-18	Please get a new log of the NIC/QUERY menu--it has been updated.
Table 8-19	Please get a new log of the system banner in the TACNEWS example--it too has been updated since.
9-10	Would the "user" do troubleshooting, or DDN Site Personnel?
Table 9-2	Numbering is very confusing because last number in table is (2), and first number on next page (unrelated) is (3). Suggest dropping "a.", "b.", "c." and numbering items with them, ie.: Priority 1 (DDN-RED). a. Any PSN, TAC,... b. Any DDN gateway... etc. Also, priorities should be listed with "Priority 1" at the top and "Priority 3" on the bottom, as this is the way they are listed in Tables 9-1 and 9-3 (and is also more intuitive).
10-1	See 8-9-h above.

COMMENTS ON DEFENSE DATA NETWORK (DDN) SYSTEM DESCRIPTION

By Francine Perillo, 1/23/87

The appendix of references that is referred to throughout the document is missing. Document citations could not therefore be reviewed at this time.

Key documents are not mentioned and should be: In Chapter 5, Section B, RFCs (Requests for Comments) and the DDN Protocol Handbook should be described as containing background information about protocols.

The Network Information Center (NIC) is mentioned in the context of a TCP/IP implementations document (sec. 5-8-b-(4)). This placement in the document is toward the end, and does not tell the reader what the NIC is. The NIC should be described in the introductory chapter (Chapter 2).

Specific typos:

p. ii - repeats i and j in the list

sec. 4-11 - incomplete sentence "The host can only take advantage of network services compatible with this view if the interface."

sec. 5-8-b-(4) - The title of the TCP/IP implementations list should be included here. Full title is "DDN Protocol Implementations and Vendors Guide".

Message 154 -- **********
11-Dec-86 18:03:12-PST,6882;000000000001
Mail-From: PERILLO created at 11-Dec-86 18:03:10
Date: Thu 11 Dec 86 18:03:10-PST
From: Francine Perillo <PERILLO@SRI-NIC.ARPA>
Subject: Snively doc
To: knight@SRI-NIC.ARPA, stahl@SRI-NIC.ARPA, fred@SRI-NIC.ARPA
Message-ID: <12262070165.22.PERILLO@SRI-NIC.ARPA>

Here are comments of Dennett's about the Snively doc you will (may) review. These are provided so you know you don't have to include them in your review.

-Francine

COMMENTS ON DDN USER OPERATING PROCEDURES CIRCULAR DCA-
(Dennett, 12/86)

Page/Paragraph	Comment
2-2-c	Incorrect reference; info on subnets is in chapter 5.
2-3-a	Unclear reference; need to state that further information can be found in the document listed there rather than implying that the actual information can be found there.
2-6	Format used for these references is very confusing. Makes it unclear whether underlined words are titles of documents or categories of information. Source should be listed last, separately, as follows: "Defense Data Network System Description. References and a basic non-technical overview of the DDN. Includes a brief history....etc. To obtain, contact B652. "
2-6	These references would be more useful if grouped, either by technical level or by intended audience (users/site personnel/programmers/etc.).
3-2-b	"...dial-up access at speeds from 300 to 2400 bps." Need to add a note that only one TAC currently supports 2400 bps.
3-6	Table 3-1: remove blank lines and bars to improve readability, ie:

Transmission Medium	Typical Data Capacity
Twisted Pair (analog)	9.6 kbps
Twisted Pair (digital)	3 mbps
Microwave	90 mbps

etc...

3-7-g — Don't use "terminal users" for dial-up users; it is confusing, because *all* users use terminals. Call them instead "TAC users", which is clearer and more descriptive. Use "TAC access" rather than "terminal access" for the same reasons.

4-4-a — Difficult to distinguish between classified and unclassified nets. Need to emphasize that on the unclassified nets *only* user traffic is encrypted, whereas on the classified nets user traffic *and* control functions are encrypted.

6-3, 6-4 — User is much more likely to interact with HA than with NSC, so HA information should be put first (in the same way HA is listed first in 6-2).

6-4-a-(2) — Everywhere else in document Host Administrator is abbreviated to HA; be consistent.

--- — GENERAL NOTE: make references to other parts of document as specific as possible, rather than referring just to section numbers, ie: "see section 3-2-a" rather than "see section 3".

6-8-b — Incorrect reference to chapter 9; should be to 6-11.

6-9-a — What is meant by "DDN MC's (both organic and contractor)" Are contractors inorganic? Confusing.

6-11 — For DDN NIC, put hotline number [(800) 235-3155] and commercial number [(415) 859-3695] after NIC address.

For all other activities, online addresses have type: "*" should be "@", ie. "DCA-MMC*DCA-EMS" should be "DCA-MMC@DCA-EMS".

7-1-b-(1) — Don't enclose single-character keys with <>, ie. use @, not <@> (as in example).

Also, suggest using curly-braces {} instead of angle-braces <> to enclose key names, because angle-braces are used by some systems to delimit directory names, whereas curly-braces aren't used for anything.

7-6-c — Reference needs to be more specific; refer to section 8-6, rather than just to chapter 8.

7-7-a-(4) — Incorrect reference; should be "8-6", not "Chapter 8, paragraph B".

7-7-b-(1) — Incorrect reference; should be 6-11, not "Chapter 9".

7-8-c-(2) — TAC message is "Bad Login" not "Bad Logon".

Suggest using "login" rather than "logon" throughout document for consistancy.

7-9-b-(2) — The intercept character (@) may be echoed a THIRD time, not THREE times.

7-13	Reference too general; should be 8-6.
Fig. 7-6	User input should be underlined, as per your systax guide.
8-9	Suggest including the file NETINFO:00NETINFO-INDEX.TXT, which lists all files in NETINFO: and gives a brief description of each.
8-9-e	File name is TAC-PHONES.LIST
9-10	Would the "user" do troubleshooting, or DDN Site Personnel?
Table 9-2	Numbering is very confusing because last number in table is (2), and first number on next page (unrelated) is (3). Suggest dropping "a.", "b.", "c." and numbering items with them, ie.: Priority 1 (DDN-RED). a. Any PSN, TAC,... b. Any DDN gateway... etc. Also, priorities should be listed with "Priority 1" at the top and "Priority 3" on the bottom, as this is the way they are listed in Tables 9-1 and 9-3 (and is also more intuitive).
10-1	The file containing the list of SIGs is now two files: NETINFO:INTEREST-GROUPS-1.TXT and NETINFO:INTEREST-GROUPS-2.TXT

2826-85

DRAFT

TERMINAL ACCESS CONTROLLER (TAC) USER'S GUIDE

DRAFT

DRAFT

NAVDAC (Code 30)
31 May 1985 (R)

TERMINAL ACCESS CONTROLLER (TAC) USER'S GUIDE

Table of Contents

D R A F T (R) 31 May 1985

TERMINAL ACCESS CONTROLLER (TAC) USER'S GUIDE

1. PURPOSE. This document describes how Navy terminal users who have a current Terminal Access Controller (TAC) access card and a TAC-compatible terminal can access the Defense Data Network (DDN) to connect to hosts, retrieve online network documentation, transfer files, etc.

2. SECURITY. Security measures must comply with reference (a). This document refers only to the unclassified subnetwork of DDN called the Military Network (MILNET). Information covered by the Federal Privacy Act may be transmitted.

3. APPLICABILITY. This document applies to all terminal users at Navy activities who access unclassified Department of Defense (DoD) information systems (IS) and data networks. Only the MILNET portion of DDN, the unclassified DDN subnet, is used and is referred to throughout this document as DDN MILNET.

4. SCOPE. This document provides technical information on TAC access and usage. You must have a current TAC access card to use the information provided in this document. Information on how to obtain a TAC access card is covered in reference (b). Reference (b) also contains information on terminal hardware and software, communications, power, and modem equipment (for dial-up access) requirements. While some familiarity with communications terms and concepts is helpful, users of this document are not expected to know DDN network architecture nor have an extensive background in business data communications.

5. REFERENCES

(a) OPNAVINST 5239.1A, DON Automatic Data Processing (ADP) Security Manual

(b) COMNAVDAC, Procedures for Terminal Connection to the Defense Data Network (DDN)

(c) FED-STD-1037, Glossary of Telecommunications Terms

(d) Defense Communications Agency (DCA), NIC 50000, DDN Directory, of June 1984

(e) Bolt Beranek and Newman Inc., Report No. 4780, TAC Users' Guide, of October 1982

(f) Bolt Beranek and Newman Inc., Report No. 5791, TAC User Guide Update: Release 112, of December 1984

6. SUPPLEMENTARY MATERIALS

a. ATTACHMENTS

(1) Attachment I. TAC Command Summary

(2) Attachment II. TAC Messages to the Terminal User

(3) Attachment III. Available TAC Dial-up Telephone Numbers

b. Figures

(1) Figure 01. Diagram of Terminal and Host Connection to DDN

(2) Figure 02. TAC Access

(3) Figure 03. TAC News Access

(4) Figure 04. Host Connection Via TAC

(5) Figure 05. File Transfer Protocol (FTP)

7. DEFINITIONS. Telecommunications terms are defined in reference (c). The following terms are also used.

a. Host Activity. The activity responsible for the management of host computers and, as such, is concerned with authorized access to data and computing resources. Security issues are the responsibility of the command ADP Security Officer (ADPSO).

b. User Activity. This general category refers to those who need to use ADP facilities to support other mission work. Security issues including the proper access and use of ADP data and facilities are the responsibility of the User ADPSO.

c. Port. A port is the point where the circuit for a device connects it to another device. For example, a host connects to an Interface Message Processor (IMP) via a port on the IMP. (An IMP is a specialized computer that acts as an entry point to DDN MILNET) via a port on the IMP.

*8. HELP!

a. If you have problems with DDN MILNET or need network information, you can contact the Network Information Center (NIC) via:

1) Electronic Mail (you must use an electronic mail system that is DDN compatible (formats messages in Simple Mail Transfer Protocol (SMTP) to use this method).

a) NIC@SRI-NIC.ARPA
For general reference questions and document requests.

b) REGISTRAR@SRI-NIC.ARPA
For WHOIS updates, user registration questions

c) HOSTMASTER@SRI-NIC.ARPA
For questions about host changes and updates.

2) U.S. Mail:

DDN Network Information Center
SRI International
333 Ravenswood Avenue, Room EJ291
Menlo Park, California 94025

3) Telephone, Monday - Friday, 0800 - 1700, Pacific Time

a) Toll free: (800) 235-3155
b) Commercial: (415) 859-3695

4) Telex: 334463

b. If you cannot reach NIC, you can contact the Network Operations Center (NOC), in Cambridge, Massachusetts.

1) Electronic Mail (see note above): CONTROL@BBN-NOC

2) Telephone: Commercial (617) 661-0100

c. To locate electronic mail hosts in your area, call the Naval Data Automation Command (NAVDAC) (Code 32), in Washington, D.C. at AUTOVON 288-4671 or Commercial (202) 433-4671, 0700 - 1530, Eastern Time.

9. INTRODUCTION

9.1 Defense Data Network (DDN) Network Overview. DDN is a packet-switching network that is designed to meet the data communications requirements of the Department of Defense (DoD). Only compatible terminals and communications software may connect to the DDN MILNET. Network functions

are performed by the network backbone and the access network. Figure 01 shows a simplified diagram of host and terminal connections to the DDN.

9.1.1 Network Backbone. The DDN network backbone is composed of packet switching computers called Interface Message Processors (IMPs), transmission lines that interconnect IMPs, and specialized computers for terminal access called Terminal Access Controllers (TACs). The network also includes dedicated transmission lines between terminals and a TAC. These network backbone components are the responsibility of and are paid for by the Defense Communications Agency (DCA).

a. Interface Message Processors (IMPs). IMPs are specialized computers that are the entry points to the DDN MILNET. IMPs are sometimes called communication computers, packet switches, or nodes.

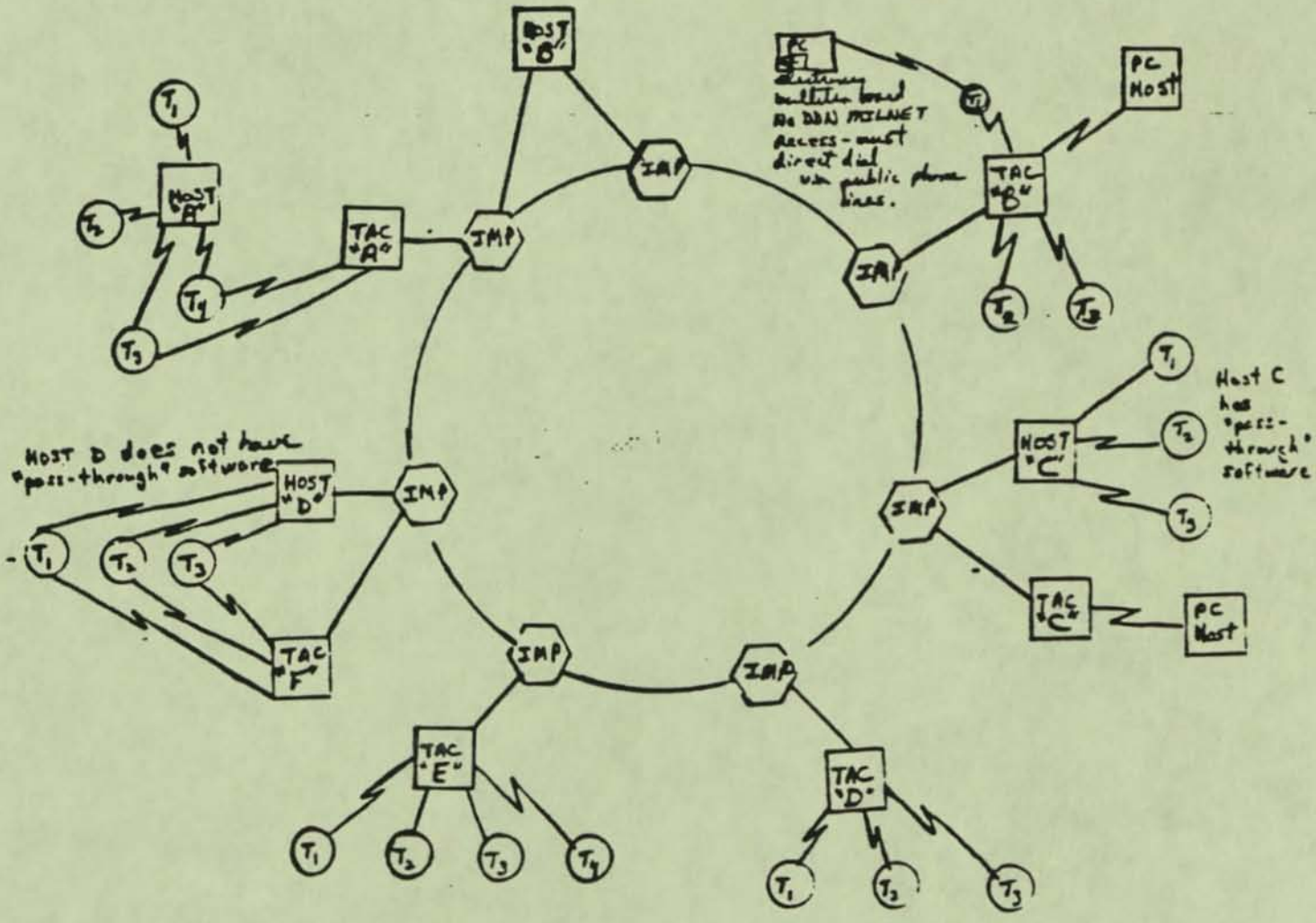
NOTE: The number of hosts/TACs that an IMP can support is determined by the IMPs capacity to handle the data it receives -- this is not a port limitation.

b. Transmission lines. Transmission lines interconnect IMPs. The most commonly used transmission medium is dedicated, leased telephone lines.

c. Terminal Access Controller (TAC). The TAC is a specialized host computer that connects to an IMP. A TAC can support up to 64 terminals. Terminals connect to a TAC via dedicated, leased lines or dial-up transmission lines. There can be more than one TAC connected to an IMP.

9.1.2 Access Network. Terminals can connect to DDN MILNET via a TAC or by using "pass-through" software on a host computer that is connected to an IMP. Pass-through software is vendor supplied software for DDN access by a host. TERMINALS CANNOT CONNECT DIRECTLY TO IMPS.

DIAGRAM OF TERMINAL AND HOST CONNECTION TO THE DDN



T = terminal
PC = personal computer

= leased, dedicated transmission line
= dial-up transmission line

FIGURE 01. DIAGRAM OF TERMINAL AND HOST CONNECTION TO THE DDN 1 OF 1

FIGURE 01. DIAGRAM OF TERMINAL AND HOST CONNECTION TO THE DDN 1 OF 1

10 PROCEDURES

10.1 TAC Access Telephone Numbers for Dial-Up Connection. Attachment III provides a list of currently available TAC dial-up telephone numbers. You may also check with one of the following sources to identify TAC dial-up telephone numbers in your dialing area:

a. The point of contact for the host activity.

b. Another registered TAC user in your area. (A registered user is someone who has a TAC access card. Information on TAC registration for DDN MILNET is described in reference (b).)

c. Defense Communications Agency (DCA) Network Information Center (NIC). See telephone numbers in Section 8, HELP!, above.

d. Once you have a TAC phone number, if you have file transfer capability on your host, you can access an online table of dial-up TAC telephone numbers that are arranged by geographical location. See paragraph 10.5.1 below on File Transfer Protocol (FTP) for more information.

10.2 DDN Directory. The DDN Directory (DCA, NIC 50000) of reference (d) is a directory of DDN users and hosts. It includes the name, online and U.S. mail address, and phone number of individual DDN users; useful contacts; and summary tables of host information.

10.3 TAC Commands. TAC commands are your way to communicate with the TAC. TAC commands need some kind of identifier to flag them for the TAC. The "@" symbol is used as the "intercept character" to flag commands for the TAC. All TAC commands must be preceded by the "@" symbol. Once you keyin a TAC command, enter a carriage return (CR) to send this command to the TAC. A summary of TAC commands and their formats is provided as Attachment I. Some frequently used TAC commands are:

a. @OPEN or @O to open connection to a host.

b. @TACNEWS to get current information on the network from NIC.

c. @WHOIS HELP to get help with the WHOIS program. WHOIS is a DDN "white pages" program that accesses data in the NIC user registration database. All users who have TAC access cards should be registered in the NIC user registration database. To add your name to this database, send your full name, middle initial, U.S. business mail address (without abbreviations or acronyms and include mail stops), network mailbox address (if you have one), and your telephone number. If you have a mail account on a DDN MILNET host mail server, send this information to NIC at REGISTRAR@SRI-NIC; otherwise, send it to the NIC address shown in Section 8, HELP! above.

d. @CLOSE or @C to close the connection to a host.

10.3.1 TAC Command Rules

a. TAC commands can usually be entered at any time. You do not need to start a TAC command on a new line.

b. TAC does not distinguish between upper and lower case letters.

c. TAC commands may consist of one or more words.

d. Since TAC only recognizes the first letter in each word of a command, you may enter the first letter of each command instead of spelling it out, e.g., O for Open, C for Close, etc.

e. Spaces are required between command words and command parameters, e.g.:

@Open (host address) (carriage return), or
@O (host address) (carriage return).

f. TAC does not perform code translation.

g. A carriage return (CR) automatically transmits whatever you enter.

10.4 TAC Protocol Parameters. If you are using asynchronous communications software to communicate access DDN MILNET, here is a sample list of compatible protocol parameter values. The bit rate value depends upon your modem's transmission speed and the speed for the dial-up number that you call -- they must be the same.

Bit rate	:300 (or 1200)
Bits per character	:8
Stop bits	:1
Parity type	:NONE
Full duplex enabled	:YES
Echo received characters to sender	:NO
Force to standard 7-bit ASCII	:NO

10.5 Connecting to the TAC. The TAC allows the termianl user to access a host as if you were directly connected to that host. The procedure for connecting to a TAC is shown in Figure 02.

10.5.1 TACNEWS. When you logon the TAC, you will see some information regarding TACNEWS, finding host administrators, reporting system problems, etc. See Figure 03 for a sample of TACNEWS access.

a. Information available by FTP. NIC maintains online information that is available by FTP. For example, NIC maintains an online table of TAC telephone numbers arranged by geographical location for dialup connection. You can FTP this file, NETINFO:TAC-PHONES.LIST, from SRI-NIC (host address 10.0.0.51 or 26.0.0.73), but if you don't have FTP permission, you will have to call NIC and ask for a copy by mail. FTP is discussed in paragraph 10.5.3 below.

b. Information available via electronic mail. When you sign onto TAC, you may see messages that reference a NIC mail address, e.g., NIC@SRI-NIC.ARPA or REGISTRAR@SRI-NIC.ARPA. If you don't have a mail account on a host that can access DDN and if that electronic mail can't send messages in over DDN MILNET in Simple Mail Transfer Protocol (SMTP), you won't be able to send or receive messages to these mail addresses. Call NIC if you feel it's something you want to know about.

TAC ACCESS

STEP #	SOURCE	ACTIONS/COMMENTS
1	User	Connect to TAC a. For dedicated, leased line connection - turn on terminal. b. For dial-up modem * -- 1) Turn on terminal. 2) Set protocol values compatible with DDN 3) Dial TAC number and make communications connection. (See paragraph 10.1 above.) a) 300 bps -- hit (CR) once or twice b) 1200 bps -- (CONTROL-Q). (Hold the CONTROL key down and press the "Q" key at the same time).
2	TAC	Prints a "herald" message if TAC connection successful. WELCOME TO DDN **FOR OFFICIAL USE ONLY** TAC LOGIN REQUIRED Call the NIC at 1-800-235-3155 for help. (sitename) TAC (version #):(port #) OR Prints a garbled message or nothing if the terminal transmission speed does not match the TAC port's transmission speed.
3	USER	Enter: @n
4	TAC	TAC Userid: [TAC prompt to user.]
5	USER	Enter your TAC userid from your TAC access card.
6	TAC	Access Code: [TAC prompt to user.]
7	USER	Enter your TAC access code from your TAC access card.

*NOTE: Some TAC ports accept data at the rate of 300 or 1200 bits per second (bps) or Baud by detecting your transmission speed and setting themselves to match it. Be sure to dial a TAC number that matches your transmission speed.

FIGURE 2E. TAC ACCESS Page 1 of 2

TAC ACCESS

STEP #	SOURCE	ACTIONS/COMMENTS
6	TAC	If TAC signon successful, TAC displays something like:

```
Login OK
TCP Trying...Open

 SRI-NIC,  TOPS-20 Monitor 5.3(5752)-1
 The system will go down today at  5:30pm until  6:30pm
 for Galaxy testing
***
*
*    The system is up with the release 6 EXEC now.
*
*    For TACNEWS, enter:  tacnews (RETURN)
*    To find the host administrator for host xy-z,
*          enter:  whois xy-z(RETURN)
*    Report system problems to Action@SRI-NIC or call (415) 859-5921
***

@                [This is the TAC system prompt sysmbol.  Now you
                  can enter a command to the system.]
```

FIGURE 02. TAC ACCESS Page 2 of 2

TACNEWS ACCESS

STEP #	SOURCE	ACTION/COMMENTS
1	USER	Connect to the TAC (see Figure 02 above).
2	TAC	Displays TAC messages, and the the system prompt:
		@
2	USER	Enter: TACNEWS
3	TAC	Gives TACNEWS information, such as:

```
SRI-NIC TACnews 1.3(34)-2 on Tuesday, 26-Mar-85 7L53an-PST
Send bugs or comments to TACNEWS@RSI-NIC.ARPA
Stop output every 24 lines? (Y/N/length/?)
```

4	USER	Respond Y or N.
5	TAC	Displays information available, such as:

```
  1. Announcements (updated [date])
* 2. Dial-ups (MILNET TAC telephone numbers, updated [date], 5K chars)
* 3. Login (Help with TAC login, updated [date])
  4. Newsletters (DDN News, updated [date])
  5. Bulletins (DDN Management bulletins, updated [date])
Type a menu number ('HELP(CR)' for more info):
```

6	USER	Enter the number of the item you want to view, OR enter HELP (CR) for more information.

FIGURE 03. TACNEWS ACCESS Page 1 of 1

10.5.2 Opening and Using a Host Connection. Use the @OPEN or @O TAC command to open the connection to a host through DDN MILNET. The following information relates to host addresses used with the @OPEN command. Each host on the DDN MILNET has a host address.

a. The older address format which is still being used but is being phased out is:

Format	Example
a:b/c	@OPEN 10:2/49

WHERE: a = network number
b = host number
c = IMP number

b. The newer, preferred format of the host address is:

Full Format	Example
a.b.c.d	@OPEN 26.4.0.106

Shortened Format	Example
b/d	@OPEN 4/106

WHERE: a = network number
b = host number
c = constant value of 0
d = IMP number

Once the connection to a host is open, you may use that host as though you were directly connected to it, e.g., to send data, access host applications. At the end of your session, logoff from the host as you normally would. The steps for accessing a host are shown in Figure 04.

NOTE: If you want to include an "@" symbol in the data stream sent to a host, enter the "@" symbol twice so that TAC will pass the second occurrence of the "@" symbol on to the host.

10.5.3 File Transfer Protocol (FTP). File Transfer Protocol (FTP) is a protocol enables the transfer of files between computer systems. When you sign onto a TAC, some of the information displayed refers to documents that can be obtained by FTP. The sample steps for FTP shown in Figure 05 may differ slightly on each host computer depending on the host operating system. Contact your host activity for commands appropriate for its operating environment. To use FTP you must meet the following requirements:

a. Both hosts must be connected to a DDN MILNET IMP and you must know the host address for each host.

b. You must be able to sign onto the sending and receiving hosts. In the example in Figure 05, SRI NIC has provided users with a guest logon userid/password for FTP transfers.

c. You must have permission to use the host's FTP. This may mean getting permission to use the host's operating system. For example, on some electronic mail hosts, you may have an authorized mail account, but you may not have access to all operating system commands, e.g., FTP. If you try to enter an FTP command and get an error message, you may not have FTP capability. Contact your host activity for request procedures if you need this capability.

10.5.4 Electronic Mail. Electronic mail (EM) may be one of many application programs on a computer or it may be the major application on one computer. When electronic mail (EM) software is the major application on a computer, that computer is often referred to as a "mail host" or a "mail host server." ONLY USERS WHO HAVE ESTABLISHED A MAIL ACCOUNT ON A MAIL HOST CAN USE ITS ELECTRONIC MAIL SYSTEM. The steps for

Accessing EM are the same as those listed in Figure 04 for Host Access. To locate mail hosts in your area, contact NAVDAC as indicated in Section 8, HELP! above. In Step 9 of Figure 04, you access EM as described in the procedures for your host.

10.5.5 Electronic Bulletin Boards. The computers used to run electronic bulletin boards are not usually connected to DDN MILNET. Unless the computer on which an electronic bulletin board resides is connected to DDN MILNET and has a host address, it cannot be accessed via a TAC; you have to direct dial a bulletin board.

10.6 Closing a TAC Connection. To close the connection between the TAC and the host, enter:

@CLOSE ⟨CR⟩ or @C ⟨CR⟩

The TAC should print "Closed" when the connection to the host is ended. Once a connection to a host is closed, you may open a new connection by enter another @OPEN command for the next host you want to access.

HOST CONNECTION VIA TAC

Step #	Source	Entries/Displays	Explanation
1	USER	@OPEN 10:2/49 @O 10:2/49	To access a host. Specify the address of the host you want to access (e.g., 10:2/49).
2	TAC	TAC Userid:)	TAC prompt to enter TAC userid.
3	USER	Enter TAC userid from your TAC access card.	Self explanatory.
4	TAC	Access Code:)	TAC prompt to enter TAC access code.
5	USER	Enter TAC access code from TAC access card.	
6	TAC	Login OK TCP Trying...Open	TCP program on TAC opens up connection to host address specified in OPEN command in Step 1 above.
7	HOST	Requests your userid/ password	System prompt from host for you to enter your userid/password.
8	USER	Enter your userid/ password for the host.	Follow usual logon procedures for accessing host.
9	USER	User conducts normal session with host.	
10	USER	User logs off (signs off) host.	
11	USER	@CLOSE	Closes the connection between the TAC and the host.
12	TAC	CLOSED	TAC has terminated the connection to the host.

FIGURE 04. HOST CONNECTION VIA TAC Page 1 of 1

FILE TRANSFER PROTOCOL (FTP)

Step #	Source	Entries/Displays	Explanation
1	USER	Logon host system (Host A)	See Figure 04.
2	USER	FTP	Run FTP.
3	HOST A	FTP)	Prompt from operating system of Host A.
4	USER	FTP)SRI-NIC	Enter name of second host (Host B).
5	HOST A	(Sri-Nic TFP Server Process 5A(3)-7	FTP processor information
6	HOST A	FTP!	FTP prompt from Host A - enter userid/password for Host B.
7	USER	FTP!LOGIN ANONYMOUS GUEST	This is a "guest" signon that allows you to logon the Network Information Center's (NIC's) host computer - Host B in this example.
8	HOST B	*(User ANONYMOUS logged in at....	Host B logon messages
9	HOST A	FTP!	FTP prompt from Host A
10	USER	FTP!GET filename [redacted]	"Get" named document from Host B (NIC's host computer).
11	HOST A		Host A prompt you to enter name you want to call received file on Host A.

FIGURE 05. FILE TRANSFER PROTOCOL (FTP) Page 1 of 3

FILE TRANSFER PROTOCOL (FTP)

Step #	Source	Entries/Displays	Explanation
12	USER	WHATEVER-FILENAME-YOU-WANT	Enter name you want to call received file on Host A (must follow Host A's file naming conventions.
13	HOST A	(Paged retrieve of NETINFO:TCP-IP-IMPLEMENTATIONS.TXT started. (Transfer completed. FTP!	
14	USER	FTP!BYE	To end FTP program.
15	USER	FTP!QUIT	

FIGURE 05. FILE TRANSFER PROTOCOL (FTP) Page 2 of 2

ATTACHMENT I

TAC COMMAND SUMMARY

ATTACHMENT I

TAC Command Summary

The following list reflects TAC commands available as of TAC Release 112, December 1984.

@Binary Input Start

Causes the TAC to attempt to negotiate Telnet binary mode if the connection is open. While the negotiation proceeds, user input is not accepted. If no connection is open, the port is marked as willing to accept a binary negotiation from the host when a connection is open.

@Binary Input End

Causes the TAC to attempt to negotiate out of Telnet binary mode if the connection is open. While the negotiation proceeds, user input is not accepted. If no connection is open, the port is marked as unwilling to accept a binary negotiation from the host when a connection is opened. (Note that no commands can be given from a port already in binary input mode.)

@Binary Output Start
@Binary Output End

Similar to Binary Input commands, except there is no restriction on accepting user commands when the TAC is in binary output mode.

@Clear Device Wild

Resets wild mode so that the TAC will no longer accept connection requests from a host for this port.

@Clear Insert Linefeed

Causes the TAC to pad ‹CR› with ‹NUL› instead of ‹LF› in Telnet connections.

@Close

Causes the TAC to try to close the connection. It will not close until the host responds or (if the port is dial-in or wild) until five minutes have gone without response.

@Device Code Ascii

Clears all device codes and any flow control.

@Device Code 37

Causes the TAC to set even parity on output.

@Device Code Extra

Causes the TAC to pad ‹CR› with ‹NUL› characters on output.

@Device Code Other

Should not be used: unsupported.

@Device Rate ‹decimal value›

Sets device rate according to the formula in TAC Users' Guide (TUG). No split rates are supported as TAC Release 112 is used only on C/30s. If value is zero, resets hunting port to hunting mode.

@Echo Local

Negotiates TAC local echoing, if the connection is open. Otherwise, the TAC sets a flag so that it will not attempt to negotiate remote echo when a connection opens.

@Echo Halfduplex

Turns off all echoing. The TAC will refuse an echoing offer from the host, and if a connection is open, the TAC will negotiate away from remote echo.

@Echo Remote

Causes the TAC to attempt to negotiate remote echo if the connection is open. Otherwise, the TAC sets a flag to initiate remote echo negotiation on connection open.

@Flow Input Start
@Flow Input End
@Flow Output Start
@Flow Output End

Enables or disables XON/XOFF flow-control in the specified direction. Incompatible with any special device codes (i.e. port must be in "device code ASCII" mode before a flow-control code can be set).

@Flush

Discards any untransmitted data from the input buffer. Note: In character-oriented-transmission, data is transmitted almost instantly, therefore there is rarely any data to flush.

@Insert Linefeed

Causes the TAC to insert ‹LF› after ‹CR› in non-binary-mode Telnet connections.

@Intercept ‹decimal ASCII value›

Sets intercept character to the character represented by the value.

@Intercept Escape

Sets intercept character to default '@'.

@Intercept None

Turns off command processing on the port.

@Intercept ‹decimal value of ASCII code›

Sets TAC's intercept character to the ASCII value specified.

@Give Back

"Uncaptures" an owned port. Ownership is gained by prefacing any command with a port number, e.g., "@44 open..." causes port 44 to open a TCP connection and give the issuing port ownership of port 44.

@Logout

Marks the port as logged out for TACACS purposes.

@News
@User-database-host

Opens a TCP connection to the address configured into the TAC. If no address has been set for the appropriate server, or if a TCP connection is already open, says "can't".

@Open ‹address›

Opens a TCP connection to the specified address in the format specified in the TAC Users' Guide. For specific port (';' format), port must have "low-level permission".

@Reset

Does the following:

- resets any TCP connection
- uncaptures any owned port
- withdraws ownership of this port from any owner
- resets binary modes.

@Reset Initial Config

Resets all parameters back to initially loaded

configuration. If port is hunting, this is exactly equivalent to typing BREAK on a closed connection.

@Send Abort Output
@Send Are You There
@Send Break
@Send Erase Character
@Send Erase Line
@Send Interrupt Process
@Send Sync

Sends the corresponding Telnet function code if a connection is open. Note: "interrupt process" is not implemented yet (command says "can't").

@Set Device Wild

Puts port in "wild" mode so that, when closed, it will accept incoming TCP connections; only allowed when the port has no open connection.

@Transmit Every ‹decimal value›

Tells the TAC to trigger a send at least every ‹value› characters if value > 0. The TAC will usually not send before ‹value› characters, but is allowed to do so.

If value = 0, this command sets the transmission value to 1 and clears transmit on ‹LF› and transmit on "message end".

Functions like "@t o 1" but uses ^S as transmission trigger.
Cannot be used in conjunction with flow-control output.

@Transmit Now

@Transmit on Linefeed

Causes a transmission of any buffered data.
Sets the TAC to transmit at least every time a <LF> character is inserted by the TAC after a <CR>). It also sets the character transmission constant to 3/4 of the input buffer size.

@Type Herald

Causes the TAC to type out the current net herald and port info.

@Transmit On Message-end

ATTACHMENT II

TAC MESSAGES TO THE TERMINAL USER

TAC Messages to the Terminal User

Following is a list of messages the TAC may, at times, give the terminal user.

<sitename> TAC <version#>:<port#>

The TAC has acknowledge the user attempt to connect to the TAC. <version#> is the software version number running in the TAC. <port#> is the octal port number the user is connected to. The user can now use the TAC to connect to a remote host.

Bad

The TAC does not recognize the command.

Can't

The TAC could not execute the command.

Closed

The TAC's connection to the remote host is closed.

Destination host dead

The remote host is not communicating with the network.

Destination unreachable

There is no path from the TAC to the remote host through the communication networks.

Host closing connection

The remote host has closed its connection to the TAC. The TAC will close its connection to the host. The port will then be idle.

Host down until <day> at <hour>:<minutes> <timezone>. The remote host is not communicating with the network. The day and time when the host was most recently scheduled to come up is indicated.

Host reset connection

The remote host has reset the connection to the TAC.

NCP Trying...

The TAC is attempting to open a NCP connection.

No

Parameters cannot be set for the specified port.

Not authorized

Low-level protocol authorization is needed. Contact the NOC.

Num

The TAC expects a number. The command is aborted.

Open

The TAC's connection to the remote host is open.

Open error

An error occurred while the OPEN attempt was in progress. This probably indicates a host error and should not happen often. If it is recurrent, contact the NOC (see Section 5.1).

Refused

The remote host rejected the attempt to establish a connection. This may occur if the remote host does not support TCP and/or Telnet. The TAC port will now be idle.

Retransmitting

This indicates that TCP has to retransmit many times to open a connection to a remote host, or to get TAC data accepted by that host. The message will occur after TCP has retransmitted five times. It will appear about once a minute until the data is accepted, or the user resets the connection.

Set Input Rate, Then Type Q

The TAC has hunted to an acceptable output rate, but too high an input rate. The user must set the input rate to 2400 baud or less, then type <Control-Q>. (This applies only to H-316 TACs.)

TAC's IMP going down in <mins> mins for <hrs> hrs <mins> mins.

The TAC's IMP is going down in the time indicated. Although the TAC will still respond, it will be isolated from the network.

TAC's IMP going down NOW

The TAC's IMP is going down immediately.

TAC's IMP down

The TAC's IMP is down. The TAC is isolated from the network.

TAC going down in <mins> mins for <hrs> hrs <mins> mins.

The TAC is going down in the time indicated.

TAC going down NOW

The TAC is going down immediately.

TCP Trying...

The TAC is attempting to open a TCP connection to a remote host.

ATTACHMENT III

AVAILABLE TAC DIAL-UP TELEPHONE NUMBERS

ATTACHMENT III

Available TAC Dial-up Telephone Numbers

[NETINFO:TAC-PHONES.LIST] [5/85, DBDOC]

MILNET TAC DIALUPS SORTED BY LOCATION 7-MAY-85

State/Country	300 Baud	1200 Baud	1200 Type
ALABAMA			
Anniston Army Depot			
(ANNIS-MIL-TAC)	(205) 235-6285 (R4)	(205) 235-7650	B/V
	(205) 237-5731 (R8)	(205) 237-5731 (R8)	B/V
	(205) 237-5770 (R8)	(205) 237-5779 (R8)	B/V
	(205) 237-5805 (R8)	(205) 237-5805 (R8)	B/V
*Please note: When accessing the Anniston TAC you must first enter a <RETURN>, then enter DDN <RETURN>. After you receive CLASS DDN START, proceed as normal.			
Gunter AFS			
(GUNTER-TAC)	(205) 279-3576		
	(205) 279-4682		
Redstone Arsenal			
(MICOM-TAC)	[none known]		
ARIZONA			
Ft. Huachuca			
(HUAC-MIL-TAC)	[none known]		
Yuma			
(YUMA-TAC)	[none known]		
CALIFORNIA (NORTHERN)			
Menlo Park			
(SRI-MIL-TAC)	(415) 327-5440 (R3)	(415) 327-5440 (R3)	B
(USGS3-TAC)	[no dialups]		
Moffett Field			
(AMES-TAC)	[no dialups; contact NSC for access]		
Monterey			
(NPS-TAC)	[none known]		
CALIFORNIA (SOUTHERN)			
Edwards AFB			
(EDWARD-MIL-TAC)	[none known]		

El Segundo (AFSC-SD-TAC)	(213) 643-9204		B/V
China Lake (NWC-TAC)	[none known]		
San Diego (ACCAT-TAC)	(619) 225-1641 (R4) (619) 225-6946 (R3) (619) 226-7884 (R2)	(619) 225-6903 (619) 223-2148	V V
Santa Monica (RAND2-MIL-TAC)	[none known]		
COLORADO Denver Fed Ctr (USGS2-TAC)	(303) 232-0206	(303) 232-0206	B/V
D.C. Washington [Andrews AFB] (AFSC-HQ-TAC)	(301) 967-7930 (R16)	(301) 967-7930 (R16)	B
(PENTAGON-TAC)	(202) 553-0229 (R14)	(202) 553-0229 (R14)	B
FLORIDA Eglin AFB (AFSC-AD-TAC)	(904) 882-3242 (904) 882-3248 (904) 882-8202 (904) 882-8201	 (904) 882-8202 (904) 882-8201	 B/V V
Naval Air Station - Jacksonville (JAX1-MIL-TAC)	[none known]		
Naval Air Station - Orlando (ORLANDO-MIL-TAC)	[none known]		
GEORGIA Robins AFB (ROBINS-TAC)	(912) 926-2725 (912) 926-2726 (912) 926-3231 (912) 926-3232 (912) 926-2204	 (912) 926-2204	 B/V
HAWAII Camp H.M. Smith (HAWAII2-TAC)	(808) 487-5545		

ILLINOIS

Scott AFB			
(SCOTT-TAC)	[none known]		
(SCOTT2-MIL-TAC)	[none known]		

KANSAS

Ft. Leavenworth			
(LVN-MIL-TAC)	[none known]		

LOUISIANA

Navy Regional Data Automation Center			
(NORL-MIL-TAC)	(504) 944-7940	(504) 944-7940	B
	(504) 944-7948 (R2)	(504) 944-7948 (R2)	B
	(504) 944-7951 (R5)	(504) 944-7951 (R5)	B
	(504) 944-8702 (R8)	(504) 944-8702 (R8)	B

MARYLAND

Aberdeen Proving Ground			
(BRL-TAC)	(301) 278-6916 (R4)	(301) 278-6916 (R4)	B/V
Bethesda			
(DAVID-TAC)	(202) 227-3526 (R16)	(202) 227-3526 (R16)	B/V
Patuxent River			
(PAX-RV-TAC)	(301) 863-4815	(301) 863-4815	B/V
	(301) 863-4816	(301) 863-4816	B/V
Silver Spring			
(WHITEOAK-MIL-TAC)	[none known]		

MASSACHUSETTS

Hanscom AFB			
(AFGL-TAC)	(617) 861-3000 (R8)	(617) 861-3000 (R8)	B
	(617) 861-4965 (R8)	(617) 861-4965 (R8)	
Cambridge			
(BBN-MIL-TAC)	[none known]		

MICHIGAN

U.S. Army Tank Automotive Command (TACOM) - Warren			
(TACOM-TAC)	[none known]		

MISSOURI

St. Louis			
(STLA-TAC)	[none known]		

NEBRASKA

Offutt AFB			
(SAC1-MIL-TAC)	[none known]		
(SAC2-MIL-TAC)	(402) 292-4638 (R10)	(402) 292-4638 (R10)	B

NEW JERSEY

Dover

(ARDC-TAC)	(201) 724-6731	(201) 724-6731	B/V
	(201) 724-6732	(201) 724-6732	B/V
	(201) 724-6733	(201) 724-6733	B/V
	(201) 724-6734	(201) 724-6734	B/V

Fort Monmouth
(FTMONMOUTH1-MIL-TAC) [no dialups]

(FTMONMOUTH2-MIL-TAC)	(201) 544-4254 (R3)	(201) 544-2430	B
		(201) 544-2636	B
		(201) 544-2638	B
		(201) 544-2777	B

NEW MEXICO
Albuquerque
(AFWL-TAC) [none known]

White Sands
(WSMR-TAC) [no diaups; contact NSC for access]

NEW YORK
Griffiss AFB

(RADC-TAC)	(315) 339-4913 (R5)	(315) 337-2004		B/V
	(315) 337-2004	(315) 337-2005		B/V
	(315) 337-2005			
	(315) 330-2294	(315) 330-2294	(FTS) 952	B/V
	(315) 330-3587	(315) 330-3587	(FTS) 952	B/V

NORTH CAROLINA
Ft. Bragg
(BRAGG-MIL-TAC) [none known]

OHIO
Wright-Patterson AFB
(WPAFB-TAC) (513) 258-4218
(513) 258-4219
(513) 258-4987
(513) 258-4988
(513) 258-4989
(513) 258-4990

(WPAFB2-MIL-TAC) [none known]

OKLAHOMA
Tinker AFB
(TINKER-MIL-TAC) [none known]

PENNSYLVANIA
New Cumberland Army Depot
(NCAD-MIL-TAC) [none known]

(NCAD2-MIL-TAC)	[none known]		
TEXAS			
Brooks AFB (BROOKS-AFB-TAC)	(512) 536-3081 (R6)	(512) 536-3081 (R6)	B/V
UTAH			
Dugway Proving Ground (DUGWAY-MIL-TAC)	[none known]		
VIRGINIA			
Alexandria (DARCOM-TAC)	(202) 274-5300 (202) 274-5320 (R6)	(202) 274-5300 (202) 274-5320 (R6)	B B
Arlington (ARPA1-MIL-TAC)	[none known]		
(ARPA2-MIL-TAC)	[none known]		
Dahlgren (NSWC-TAC)	[no dialups; contact NSC for access]		
McLean (DDN-PMO-MIL-TAC)	[none known]		
(MITRE-TAC)	(703) 442-8020 (R15) (703) 893-0330 (R10)	(703) 893-0330 (R10)	B/V
Norfolk (NORFOLK-MILTAC)	(804) 423-0241 (R2) (804) 423-0247 (R2) (804) 423-0346 (R4) (804) 423-0480 (804) 423-0486 (R2) (804) 423-0489 (804) 423-0570 (804) 423-0572 (R2) (804) 423-0577 (R2) (804) 423-0651 (804) 423-0654 (R3) (804) 423-0841 (R2) (804) 423-0845 (804) 423-0849 (804) 423-0858 (804) 423-0950 (804) 423-0952 (804) 423-0955 (R3) (804) 423-0959	(804) 423-0241 (R2) (804) 423-0247 (R2) (804) 423-0346 (R4) (804) 423-0480 (804) 423-0486 (R2) (804) 423-0489 (804) 423-0570 (804) 423-0572 (R2) (804) 423-0577 (R2) (804) 423-0651 (804) 423-0654 (R3) (804) 423-0841 (R2) (804) 423-0845 (804) 423-0849 (804) 423-0858 (804) 423-0950 (804) 423-0952 (804) 423-0955 (R3) (804) 423-0959	B B B B B B B B B B B B B B B B B B B
Reston (DCEC-MIL-TAC)	(703) 437-2892 (R5) (703) 437-2925	(703) 437-2928 (703) 437-2929	B B

(703) 437-2926
(703) 437-2927

GERMANY
(FRANKFURT-MIL-TAC)
(M) 2311-5641 (R8) B

(RAMSTEIN2-MIL-TAC) [none know]

KOREA
(KOREA-TAC) (M) 264-4951 (R8) B

SPAIN
(MILNET-TJN-TAC) [none known]

(ROTA-MIL-TAC) [none known]

Notes:

1. "(R10)" following phone number indicates a rotary with 10 lines.

2. For alternate phone numbers, FTS=Federal Telephone System.

3. (M)=Military DoD Telephone System.

4. "1200 Type" refers to the modem compatibility for 1200 baud only:
   B/V = Bell and Vadic
   B = Bell 212A only
   V = Vadic 3400 only

5. This list is contained in the file NETINFO:TAC-PHONES.LIST at SRI-NIC.

---------- End of Issue ----------

2827-87

PLEASE READ

4 DECEMBER 1987

TO: MANAGEMENT STAFF, BARKER

FROM: B HALEY

SUBJECT: DECCO MINUTES

ATTACHED ARE THE MINUTES FROM THE NOV 23, 24 IN-PROGRESS MEETING. I URGE YOU TO LOOK AT YOUR TASKS AND TAKE NOTE OF THE " ACTION" ITEMS. IF YOU ARE IN DISAGREEMENT WITH ANY ITEM, PLEASE GIVE ME YOUR INPUT IN WRITING. I'LL PASS IT ALONG TO JAKE AND BARBARA CAMPH.

REPORTS

DEFENSE COMMUNICATIONS AGENCY
DEFENSE COMMERCIAL COMMUNICATIONS OFFICE
SCOTT AIR FORCE BASE, ILLINOIS 62225-6300

IN REPLY
REFER TO:

D560

02 December 1987

SRI International
ATTN: Ms. Barbara Camph, Sr. Contracts Administrator
333 Ravenswood Ave.
Menlo Park, CA 94025

SUBJECT: Minutes of Program Review at SRI International 23 - 24 Nov. 1987

Dear Ms. Camph:

Enclosed please find a copy of the minutes that took place last week. As you can see, there are a lot of action items that the Government and SRI need to adhere to. Because of the holiday season coming up, some issues may not be addressed in as timely a fashion as previously stated. However, it is hoped that such matters will be brought to the attention of the responsible person, through the proper channels of communication.

There are still some concerns about the direction, as well as pace that the DBMS selection is taking. In this regard, the Government will research SRI efforts/recommendations to date in order to ensure that it can meet its requirements. If you have any questions or comments, please feel free to call me at (618)256-3094.

Sincerely,

Cecelia M. Jones

CECELIA M. JONES
Contract Specialist

Encl. a/s

Copy to:
SRI International (E. Feinler)

DCA/Code B622 (Mr. Smallwood)

MINUTES OF MEETING BETWEEN SRI AND GOVERNMENT - 23 NOV. - 24 NOV. 1987

Note: All action items will be annotated with the responsible person/entity named.

23 NOV. 8:30 a.m.

Introductions were made for SRI, DECCO, and DCSDS. In attendance: Trudy Barber (SRI), Steve Dennett (SRI), Elizabeth Feinler (SRI), Cecelia Jones (DECCO), Barbara Haley (SRI), Ken Harrenstien (SRI), Vivian Neou (SRI), Fred Ostapik (SRI), Francine Perillo (SRI), Elizabeth Redfield (SRI), Captain St. Johns (DCA), Tyrone Smallwood (DCA), Mary Stahl (SRI), Captain Tatum (DECCO)

Captain Tatum opened up the meeting with an explanation of the purpose of the meeting was to do a program review in light of the fact that we were nearing the end of the contract period. All contracts were being reviewed. Everyone has a copy of the agenda to follow along.

NIC Accomplishments and Efforts for the DDN -

Ms. Feinler presented a slide presentation of SRI International. Handouts were given to everyone to follow. An organization chart which had previously been requested from SRI was included in the handout. There was some brief discussion on various parts of the presentation that were marked for later discussion. Purpose of user and system services - main function to direct traffic on and through the network. There is a major problem because there are many "users" without mailboxes. Question: How much of the network is on-line and how much is hard copy. There has been a lot of biblio cataloging. Service (Server) New item to government. Some comments about value added items. Discussion about providing documents. An arrangement had been made with Major Tucker instead of an actual tasking of the contractor. There is a schedule of fees. Will discuss later.

DBMS Selection/Licensing -

Government raised the question with SRI,"Where are we with the DBMS selection?" Previous notes indicate that SRI had asked to purchase a commercial DBMS in the past. Also some information with the proposal package indicated some research had been done into DBMS selection. SRI comments: TACACS - Could rewrite with no problem. TOPS 20 presents a problem. Can't run UNIX on TOPS 20. No commitments have been made with Sybase or Ingres. There is only one machine available at SRI for test purposes. At this point SRI doesn't know if one relational DBMS is possible for the DDN requirement. Lucy Sanders at DCSDS is looking into the report from SRI which recommended further testing of Sybase and Ingres. It will be approximately two to three weeks before she can complete her review. ACTION ITEM Need time suspense for review from DCSDS.

Question from Government, "What is the reason for this?" SRI stated that the DBMS is not as portable as stated. Some adaptations have to be made. Discussion then ensued about the purpose of the equipment. Captain St. Johns stated it was for use of the Audit Trail (Task 4 and 6). SRI disagreed and stated it was more than that. Discussion continued briefly concerning this matter. Ms. Jones then asked that the DBMS Selection discussion be tabled until we had more definite information.

Award of Equipment -

Discussion to be moved to Tuesday morning. Still under review.

Software Conversion - Most of the conversion of Augment has taken place.

Discussion ensued around the issue of the difference between commercial and portable software and being able to move into a competitive environment.

NAURS - Prototype has been converted except actual interface. It will take one to two months testing to complete.

Mailer - All C code.

Status Report Conversion versus Portable by module - ACTION ITEM - SRI directed to provide this to the government. They had begun this effort prior to leaving on Tuesday evening. Gave government a rough draft for verbal review

Register - Coded C. Interfaces to be worked out.

WHOIS - All C coded.

(NIC) Query Locator - A lot of raw files.

Protocol Locator and Host Name Server - All C coded. Domain Name Server - Generating data for programs in C.

Services - Assembler language.

Detailed discussion followed concerning what kind of time line or performance line should be indicated and how. SRI stated they would color code handout page. (Schema on NIC SERVICES pages given to C. Jones by E. Feinler 24 Nov.)

Lengthy discussion followed concerning VOID DBMS and IFPAC. SRI stated these two data bases belong to DBMS. SRI wants to convert this into C even though this is not a requirement. IFPAC is an assembler language. The concern for the government is what rights we would have to this data if conversion efforts are done at this time. SRI stated the government could use it but they didn't want their competitors to have access to it.

Mr. Harrenstien again raised the question, "What level of detail do we want on the conversion efforts?" Discussion. ACTION ITEM SRI is to present this information on a quarterly basis, in the monthly document; the first report being due in the January monthly report.

Mr. Smallwood raised the concern whether or not SRI had a TASK ORDER PLAN. It had not been previously required of SRI. This will be discussed for the option year contract.

Government Issues -

Travel - Discussed at length. Mr. Smallwood had concerns about the way travel was being handled in that it was not going through the COR. He stated that changes would be made for the option year. Capt. St. Johns said this was discussed in detail during negotiations and what was supposed to happen is that certain meetings/trips should go through DECCO or COR first e.g. trips outside of a 50 mile radius.

Service Server - This server was new to DECCO and DCSDS. SRI stated this was built because of military requests in conjunction with the CORE NIC. The requests were verbal. SRI didn't know who to ask. SRI stated this really isn't something new. Discussion ensued at length concerning lines of communication and the contractor doing over and above what the contract calls for.

800 Calls - Explanation provided by SRI. Whereas stats are given on the number of calls per month there is no line item for this. ACTION ITEM The costs for this item are to be spelled out either on the invoice or in the cost status report. SRI will provide.

Biblio - Catalogued deliverables. Discussion. ACTION ITEM DCSDS will have to review what they want to do with Biblio since SRI says it's needed and some at DCSDS don't feel the need for it.

Develop - What does this actually mean as it is repeated several times throughout the tasks. SRI response. This does not always mean new initiation as such but actually means to set up.

Publicity - Discussion. DECCO will probably okay if needed and printing prices warrant SRI providing copies of government documents since they can do them in a more timely fashion. ACTION ITEM SRI is to provide a price list to DECCO for review.

Newsletter - How often is this done? SRI - On a random basis. Does DCSDS want to set a schedule? ACTION ITEMS DCSDS needs to implement a policy. Also, reference to the DDN PMO needs to be corrected to DDN DCS.

TASKS:

1f - SRI says they use it for NCDs. Government sent e-mail to SRI stating they will continue to provide this information to SRI. Costing has been worked up for price adjustment for deleting this task.

1h -

2b - Table documentation - COR needs to see this on a quarterly basis. Annually, is not often enough. S006H is the deliverable. Since this is the end of the contract year. It was decided this would be changed during the option year contract. ACTION ITEM This is to be provided by SRI for the current contract 60 days from Nov. 30.

2c - Service - Further discussion. Didn't get prior approval from the COR. How do we want the source code? - SRI. Government - Printout. ACTION ITEM SRI to provide by the end of the contract year. Source code - Only what government owns. Further discussion on protocols. ACTION ITEM DCSDS will have to address this issue of protocols. Discussion concerning RFCs. SRI stated no one would want the Protocol since it's user accessible. Government approves. Therefore SRI has to provide. ACTION ITEM Describe as RFC, not as a protocol. COR approves based on task monitor input. Government use only.

2d - Discussion - User/Service Overlap.

3c - Hotlist will go away. UDH/Microvax installed. Question raised about interaction between BBN and SRI. BBN provides the check of user ID. SRI provides user database. BBN maintains the equipment background. Data sent to SRI to analyze and determine who should get what. Programming funding cut. BBN to load. 950 is the average monthly trend. 1200 is the limit. There should be no problems for a year. Question: no deliverable? Answer - Task 4 reports on Task 3. Only report or milestone at end of contract year?

4 - ACTION ITEMS St. Johns to respond to format for Audit Trail Functional Description. DCSDS to develop this requirement for misuse of the network. This is to be done by B602 who implement administrative procedures and policy guidelines.

Discussion about who the security officer was for DCSDS in the past. No one currently knows who that is. ACTION ITEM COR to provide the name of the current security officer as a point of contact when necessary.

6 - Discussion concerning accounting and analysis procedures and the cost recovery scheme. ACTION ITEM DECCO to provide when the equipment is in place and has been tested and is operational.

Skipped Task 5 since person responsible for Task 6 was present and Task 5 action person was not.

ACTION ITEM DECCO to provide corrected copy of S.O.W. to SRI. Some page numbers were different between DECCO copy and SRI copy.

Adjournment: 4:25 p.m.

11-24-87 8:30 a.m.

Government Issues/Tasks Continued -

5 - DCSDS has provided the TAC User Guide to SRI for comments. There may have been one submitted by the User's Requirement Group. Mr. Snively at DCSDS is the task monitor who normally provides this information. The DDN Operating Procedures has been reviewed before. SRI makes comments within 30 days. SRI has revised the 1985 DDN User's Guide by updating with minor changes. SRI would like to send out 200 copies per Europe DCA request. ACTION ITEM DECCO will respond within a week once the price list is received.

SRI is concerned about lines of communications with DCSDS concerning DCSDS updates of some documents without SRI input or prior knowledge. Also, SRI has been told they can't receive copies of the DDN Brochure for distribution which they feel would be helpful to DCSDS. ACTION ITEM COR needs to check on DCSDS policy and forward to SRI.

The monthly report concerning a new table hasn't started yet. This is based on need. Because of all the extra time that has been mandated for this task, an extra person will be added to the staff.

Capt. asked SRI did they have a Product Support Plan. No they don't. Task 4 mentions this somewhat but it doesn't tell the contractor how to do this. ACTION ITEM Capt. Tatum said he will forward a couple of samples.

Discussion centered around purpose of this task. SRI attempted to clarify this. They stated the problem with the task is the way the tasks were broken out. In reality, this task should be under the CORE NIC. ACTION ITEM SRI to put in writing what we actually get from this task. Three RFCs have been received by Capt. St. Johns for this task. ACTION ITEM Capt. St. Johns is to provide this information to Mr. Smallwood.

7 - Discussion again centered on biblio. "MITRE didn't want it." Check this conflict. SRI maintains this is imbedded in many of the required efforts. ACTION ITEM DCSDS - Repeat - should this be deleted?

Monthly Reports - Mr. Smallwood would like to see the reports done differently. SRI says the format is done according to 7935 Standard. The following changes for monthly report and cost status schedule report are ACTION ITEMS for SRI. (1) Identify the tasks for areas of concern. (2) Travel is to be included on page two of the Cost Status Schedule report. (3) Both travel and salaries are to be broken out by tasks. (4) A chart should be established with expenditures by tasks. Ms. Haley copied the format that Mr. Smallwood presented on the board, which included such items such as staff hours, estimated funds, resources used monthly/cumulative. (5) Eliminate CDRLs Sec. 3 of the Cost Status Schedule report. (6) There is to be separate section for Tasks/Travel only for SRI NIC Contract. (7) Combine Task 5 with CORE NIC. ACTION ITEM for DECCO - Send follow-up letter to Barbara Camph concerning invoices. Invoice format is done by DCAA after SRI sends invoices

to them. That can't be changed. Changing the cost status schedule report will resolve the invoicing solution by tasks.

8 - Document Center - Discussion centered around use of this Center. Is this a library service? What is unique about this center? What is the usage? SRI stated that it's on the premises. Usage has been low because they have had to move twice. They could provide a service if they knew what the policy was to be. Everything is supposed to be deposited at the Document Center not at DTIC. SRI doesn't feel DCSDS staff can really give accurate feedback on the Center because it hasn't been there long enough. ACTION ITEM DCSDS is to provide a policy and direction to SRI about the Documentation Center.

Areas of Concern by SRI - Disks are sorely needed. Too many things being done on too little equipment. Can get some through government surplus. What is the procedure? ACTION ITEM DECCO to check immediately and get back with SRI. However no action is to be undertaken by SRI unless directed by DECCO. Also, items under Areas of Concern in the monthly reports are not to be acted on until authorized by the COR. Mr. Smallwood has indicated that issues under Areas of Concern in the monthly reports will be addressed more quickly in the future.

9 - Mr. Smallwood requested an inventory list of equipment (GFE) at SRI. ACTION ITEM for SRI to provide. He stated this was not adequate enough to provide receipt information of equipment to SRI. Discussion. ACTION ITEM Mr. Smallwood is to check government documentation (form) for acceptance of GFE.

Ms. Jones asked what has happened to the Kurzweil lease since correspondence came in from SRI that the lease was to go away in August and in September an evaluation was still being done for replacement equipment. ACTION ITEM SRI is to send into DECCO a proposal for adjustment of this lease or what replaced it.

Discussion on equipment indicated that SRI has not bought all the proposed equipment under the facilities contract. Also some items were bought cheaper than proposed. Some of the equipment is actually peripheral. They would like to buy some other needed equipment such as disks/work stations. ACTION ITEM SRI will have to send in a request for other equipment and show what it would be replacing and the necessity for the buy.

Question: "When will the Foonley be phased out?" Within 6 months after the new equipment is in place. DEC 2065 will be around until the end of the contract of the option year.

9b - Provide 10 directories. Discussion. Capt. St. Johns has been monitoring because it serves the CORE billing. Discussion centered around points of contacts at DCSDS. It was reemphasized by the Government what the lines of communications are and always have been. SRI maintains they have gone through the right persons. ACTION ITEM Mr. Smallwood will send out the current task monitors list for the NIC contract immediately.

CDRLs/Milestones tabled.

ACTION ITEM Mr. Smallwood will review and send out a revised list based on any changes at this meeting as well as some deliverables that say annually at end of contract period, but do not specify 30 days or 60 days after contract expires.

Award of Equipment -

Capt. St. Johns asked SRI the following questions or made comments about the proposals and evaluation on the NAURS equipment submitted to DECCO and DECCO's preliminary input.

1. How can Falcon offer source code and SUN did not?
2. Did SRI go back to SUN about optical equipment? Yes and they still didn't quote.
3. Meantime from DEC - Should have only given 0 points concerning nondisclosure.
4. 260 - SUN Went back twice to SUN. Still can't meet spec.

5. Clarification about hard copy terminals.

6. Did SUN have available the laser printers?

7. Clarification about cost summary - evaluating non-responsiveness - adding equivalent prices.

8. Why did only 3 companies of 45 companies respond to RFP. ACTION ITEM SRI to provide the original list of those who requested RFP package.

9. Has SRI asked Falcon about partial source code? Yes. SRI felt on Option equipment that they would get quotes from anywhere. That didn't happen. Only one vendor could supply everything within environment asked for. Spec was not restrictive. Option for the 360s from Falcon offered. The 350s won't be able to do the job. The equipment would only be good for 4 or 5 years. Maybe they would just have some of the work stations upgraded. Disk storage however is the priority with SRI.

10. Miscellaneous equipment, is not optional equipment. DCSDS gave the verbal authorization to go ahead for the purchase of the miscellaneous equipment. ACTION ITEMS DCSDS to send to DECCO purchase request for the miscellaneous equipment. DCSDS to provide recommendation to DECCO in writing immediately so that SRI can go ahead with award of the equipment.

11. ACTION ITEMS SRI to provide to DECCO a list of persons who were on the evaluation team for the equipment selection; a copy of vendor requests and a follow-up to negotiations whereby SRI stated they had followed up with the quoters; and a PNM which is being written by Julie. SRI provided copies of the vendor requests and a list of evaluation team participants before DECCO left SRI.

Open Items -

Publicity - A copy of copying charges already requested from SRI. Discussion concerning funds built up from carryover of other copying. There's a balance of $57,000, where SRI has recouped their charges and is able to get items copied and bill for the effort.

Organization Chart - Received in packet at beginning of Monday's session.

Invoices - Letter to be forwarded to Barbara Camph. Resolved.

Data Rights - Biblio- SRI needs the tool to know what they have, for tracking purposes. A suggestion was made that SRI should document why biblio is the backbone. ACTION ITEM From SRI if they want to defend their position. VOID DBMS issue hasn't been resolved to the extent of what level of rights the Government has. Ms. Feinler on record that the matter is a contractual issue for legal to resolve. However, Ms. Jones acknowledged the fact that it has to be resolved prior to including it as part of the contract, Section H.

Discussion about subcontractors - though this is not an open item. To be reviewed again for option year if any cuts are or have been made. Sherwood Associates did the biblio and conversion to C efforts. Kariel did or will do the bind (Unix). USC is the designer of naming domain (Namer on Tops 20). They're also responsible for the Milnet transition. Telematics is responsible for the protocol locator (OSI). SRI interacts with the subcontractors in a working group environment.

Overtime - There are two kinds of premiums: other premium and overtime premium. There is no problem with the other premium. Overtime is paid at the rate of time and a half to hourly workers and not salaried personnel. There are two full time persons for hourly operations. Captain Tatum commented that SRI is to pay their people because it's a management issue but they have to notify DECCO that overtime was worked. ACTION ITEM DECCO and DCSDS resolve by next Friday.

Monthly meeting - Discussion centered around who will come and what the Government will expect. It was suggested that all tasks be presented on one chart.

SRI wanted to know if there was a working group looking at data elements? Also, is DCSDS developing data base strategies? Who's the point of contact clearinghouse for these type issues? SRI feels there's some duplicate work with the data flow and is unable to determine who's doing what. Discussion around these areas along with comments concerning URDB, the NAC, and TACACS. ACTION ITEM Captain Tatum will arrange a meeting between the Government people and SRI on Tuesday, Dec. 8 so that these concerns can be addressed. Aydin and BBN CORs will also be asked to attend. This will be a step towards bringing SRI "back into the loop."

Communication channels - Discussion. Additional comment from SRI "cognizant of who are your customers."

ACTION ITEM - DECCO to change mod P00006 to Contract DCA20087C0020 to Dec. 2 in order for it to meet 30 day response time. This will correspond to the cover letter which had 2 Dec. date. The reduction for Task 1f will be $8900.00.

NIC Brochure delivered under Contract DCA20084C0024. SRI presented another copy to Mr. Smallwood for review since another previously sent to DCSDS had not been approved. ACTION ITEM The COR is to approve and send written response. SRI is ready to send these out to the public.

Ms. Jones asked what account is mail under since invoices aren't broken out. No one was sure. ACTION ITEM SRI to provide response to DECCO.

Videotape - Mr. Smallwood is still awaiting the costs for the videotaping. SRI is putting together text script and some costs.

SAM/Transend - Discussion about invoices and Transend's involvement. SRI made a counteroffer that we pay the invoice "with no dates" for work done in November and December, and that we not pay the one that has service date of 6/1/87 through 6/30/87. Ms. Jones stated this was still unacceptable because there was no clear evidence when the work for the previous invoice was done. The company kept poor books while someone was out of town. There was some hours printed up by SRI but the information is not "original evidence." Further discussion ensued on SAM license for the software and Transend's agreement. Source code built on top of commercial software. Government owns everything except what Transend owns. SRI still has a letter from DECCO to respond to.

Ms. Feinler indicated that some persons had not previously been hired because the contract had only been incrementally funded. Therefore some things not operational. This led into discussion about the remainder of the contract year whereby there will be funds leftover because the effort of work is behind. SRI asked that the contract be extended for a month. It was explained to her that we would not extend the contract for a year because we already had an option year requirement set to start immediately following expiration of the current contract. Since SRI already had personnel lined up for contract purposes a verbal agreement was given to Ms. Feinler that they go ahead and hire the programmer and domain staff. Training that was to be done for this year's contract will have to be added to the option year. ACTION ITEM for when the option year contract is looked at again. SRI asked if positive log-in scheme could go in. They were advised if this is in addition to the contract they would need to submit a proposal.

Discussion again ensued concerning Sybase and Ingres and whether or not SRI had authorization to buy the source code. DCSDS asked SRI weren't they able to get performance standards for the source code. Discussion centered around the VOID DBMS again and SRI's desire to convert this to C. The concern is what happens if they convert this is on government money and whether or not this really needs to be converted. Captain Tatum asked if the database is only a backup, and why convert VOID to Unix. SRI responded that the VOID can also be compared to the Sybase environment. However, they would have to buy the Sybase. Question also raised by Captain Tatum, "What happens to Ifpac?" This can be converted.

ACTION ITEM Captain Tatum directed Trudy to schedule a CDR for the NAURS equipment and to include it on the milestone time line. SRI says the milestones are already in the monthly reports. Government not sure which report and if it is in the monthly report that Ms. Jones gets, actions are discussed but milestones are not clearly defined.

Formal discussion ended at 5:30 p.m. A tour of the computer facilities was provided to Government staff by SRI.

2829-90

DEFENSE COMMUNICATIONS AGENCY

DEFENSE COMMUNICATIONS SYSTEM ORGANIZATION
WASHINGTON, D.C. 20305-2000

IN REPLY REFER TO DODM

MEMORANDUM FOR DISTRIBUTION

SUBJECT: Defense Data Network User Operating Procedures

Reference: DCA Circular 310-P70-81, Defense Data Network User Operating Procedures, March 1990 (Revised Draft)

1. Reference prescribes the policy, assigns responsibility, and provides procedures concerning the operation, maintenance, and use of the Defense Data Network (DDN). It was released for review as DCA Circular 310-P70-79, Defense Data Network User Operating Procedures in December 1988. Comments from the previous review have been incorporated. In addition, DDN has now been integrated into the standard Defense Communications System (DCS) Outage Procedures by modifying existing circulars. The outage procedures contained in the current draft address the unique procedures used in addition to the standard DCS procedures.

2. Request reference (enclosed) be reviewed and comments and/or concurrence be provided by 15 May 1990.

3. Point of contact is Mr. Ramon Butler or Mr. Jeff Johns, DCA DODM 202-692-7580, DSN 222-7580.

FOR THE DIRECTOR:

1 Enclosure a/s

JOHN W. MILTON
Chief, Data Systems
Management Division

DRAFT

Distribution:
The Joint Staff, ATTN: J6T, Washington, DC 20318-6000
Director, National Security Agency, ATTN: P6, Coins, T133, C63, Ft. George G. Meade, MD 20755
Director, Defense Intelligence Agency, ATTN: DSE-2, DSI-ID, DSE-4, Washington, DC 20301-6111
Director, Defense Logistics Agency, ATTN: DLA-Z, Cameron Station, Alexandria, VA 22314
Secretary, Department of Energy, ATTN: CSTM MA253.3, Washington, DC 20545
Commander, Defense Communications Agency-European Area, ATTN: DED, APO New York 09131-4103
Commander, Defense Communications Agency-Pacific Area, ATTN: DPD, Wheeler AFB, HI 96854-5000
Headquarters, U.S. Air Force, ATTN: SCMM, Washington, DC 20330
Chief of Naval Operations, ATTN: OP941C, Washington, DC 20305
Department of the Army, ATTN: DAPC-PSO-SN, DAIM-C45-W, Washington, DC 20310
Director, Joint Data Systems Support Center, ATTN: JW, Washington, D.C. 20305-2000
Commander, National Communications System/Defense Communications Agency Operations Center, ATTN: DOCO, Washington, D.C. 20305-2000
Director, Defense Communications Engineer Center, ATTN: DRF, Washington, D.C. 20305-2000
SRI International, 333 Ravenswood Avenue, Room EJ291, Menlo Park, CA 94025
Bolt, Beranek and Newman Communications Corporation, 8000 Westpark Drive, 6th Floor, McLean, VA 22102

Copy to:
Commander, U.S. Army Information Systems Command, ATTN: ASOP-OI, Ft. Huachuca, AZ 83613-5000
Commander, Naval Telecommunications Command, ATTN: Code N6, N62 Massachusetts Avenue, NW, Washington, DC 20390-5290
Headquarters, Air Force Communications Command, ATTN: DO, Scott AFB, IL 62225-6001
Commandant, U.S. Marine Corps, ATTN: CCT, Washington, DC 20380
Commander, Naval Telecommunications Automation Support Center, ATTN: 431B, Washington, D.C. 20397-5310
Director, Defense Mapping Agency, 8613 Lee Hiway, Fairfax, VA 22031-2139
Director, Defense Nuclear Agency, ATTN: Director of Operations, 6801 Telegraph Road, Alexandria, VA 22301
Headquarters Software Support Center, ATTN: AQFC, Gunter AFB, AL 36114
Headquarters Air Force Systems Command, ATTN: SCXP, Andrews AFB, MD 20334-5000
Commander, 7th Signal Command, ATTN: ASQN-op-sd-p, Ft Ritchie, MD 21719
Commander, Army Aviation Systems Command, ATTN: AMSAV-MSB3, St. Louis, MO 63120
Navy Military Personnel Command, ATTN: 1666C, Washington, D.C. 20370
Commander, Naval Data Automation Command, ATTN: Code 30, Washington, D.C. 20734

DCA Cicular 310-P70-81

7th Draft
23 February 1990

METHODS AND PROCEDURES

Defense Data Network User Operating Procedures

1. Purpose. This Circular prescribes the policy, assigns responsibility, and provides procedures concerning the operation, maintenance, and use of the Defense Data Network (DDN).

2. Applicability. This Circular applies to Headquarters, DCA, DCA field activities, military departments, other Department of Defense (DoD) and authorized Government agencies, and commercial activities that assist in the management, operation, maintenance, or use the DDN.

3. Authority. This Circular is published in accordance with the authority contained in DoD Directive 5105.19, Defense Communications Agency (DCA), 10 August 1978, as amended. It implements Joint Chiefs of Staff (JCS) policy as set forth in Memorandum of Policy (MOP) 195, Defense Data Network and Connected Systems, 9 September 1987.

4. Procedures and Responsibilities. The procedures and responsibilities are contained in the chapters.

FOR THE DIRECTOR:

OPR: DDO
DISTRIBUTION: A, B, J through Q; Special

This page is intentionally left blank.

ILLUSTRATIONS

Table

Figure

This page is intentionally left blank.

GLOSSARY OF ACRONYMS

ACC	Access Control Center
ACOC	Area Communications Operations Center
ADP	Automated Data Processor
AFCSC	Air Force Cryptographic Support Center
AFOSI	Air Force Office of Special Investigation
AHIP	ARPANET Host Interface Protocol
ALC	Air Logistics Center
ALLDISNETSTA	All Defense Integrated Secure Network Stations
ALLWINSTA	All WWMCCS Inter-computer Network Stations
AMC	ARPANET Monitoring Center
ARPANET	Advanced Research Projects Agency Network
ATA	Audit Trail Analyzer
AT&T	American Telegraph and Telephone
ATTN	Attention
AUTODIN	Automatic Digital Network
BBN	Bolt, Beranek and Newman Communications Corporation
BFE	BLACKER Front End
BPS	Bits Per Second
C/70	Monitoring Center Equipment
C/30	Packet Switching Node (or Terminal Access Controller) Processor
CAD	Collective Address Designator
CCG	Configuration Control Group
CCO	Circuit Control Office
CCSD	Command Communications Service Designator
CERT	Computer Emergency Response Team
CDMC	CONUS DSNET1 Monitoring Center
CM	Configuration Management
CMC	Cambridge Monitoring Center
CMI	Configuration Management Item
CMMC	CONUS Military Network MILNET Monitoring Center
CMO	Communications Management Office
COI	Community of Interest
COMPUSEC	Computer Security
COMSEC	Communications Security
COMSPOT	Communications Spot (Report)
COMSTAT	Communications Status (Report)
CONUS	Continental United States
CONUSMILNETSTA	CONUS Military Network Stations
COOP	Continuity of Operations
CPU	Central Processing Unit
CR	Encryption (Crypto) Deficiencies - Used in Problem Reporting
CRC	Cyclic Redundancy Check
CRI	Collective Routing Indicator
CSA	Communications Service Authorization
CSCI	Computer Software Configuration Item
CSIF	Communications Services Industrial Fund

CSU	Channel Service Unit
CT	Cyphertext
DCA	Defense Communications Agency
DCAC	Defense Communications Agency Circular
DCA-EUR	Defense Communications Agency - European Area
DCA-PAC	Defense Communications Agency - Pacific Area
DCAOC	Defense Communications Agency Operations Center
DCE	Data Communications Equipment
DCEC	Defense Communications Engineering Center
DCS	Defense Communications System
DCSDS	Defense Communications System Data Systems
DDN	Defense Data Network
DECCO	Defense Commercial Communications Office
DH	Distant Host
DIA	Defense Intelligence Agency
DISNCAN	Discretionary Network Change Action Notice
DISNET	Defense Integrated Secure Network
DISNETMGR	DISNET Manager
DLA	Defense Logistics Agency
DOCC	Defense Communications Agency Operations Control Complex
DOD	Department of Defense
DOE	Department of Energy
DSN	Defense Switched Network
DSNET	Defense Secure Network
DSU	Data Service Unit/DDN Software Update
DTE	Data Terminal Equipment
DTG	Date-time Group
DTIC	Defense Technical Information Center
ECP	Engineering Change Proposal
EDAC	Error Detection and Correction
E-MAIL	Electronic Mail
EMH	Electronic Mail Host
EMS	Electronic Mail System
EMMC	European MILNET Monitoring Center
ENR	Enroute
EURMILMGR	European MILNET Manager
EURMILNETSTA	European Military Network Stations
FACID	Facility Identification
FBI	Federal Bureau of Investigation
FOT&E	Follow-on Test and Evaluation
FTP	File Transfer Protocol
FY	Fiscal Year
GMT	Greenwich Mean Time

HA	Host Administrator
HDH	HDLC Distant Host Protocol
HDLC	High-Level Data Link Control
HE	Host End Deficiency - Used in Problem Reporting
HFEP	Host Front-End Processor
HIT	High Interest Telecommunications
HW	Hardware
INTL	International
IP	Internet Protocol
IR	Investigation Request
ISO	International Organization for Standards
IST	Inter-switch Trunk
IT&A	Installation, Test, and Acceptance
IVV&T	Independent Verification, Validation, and Test
JCS	Joint Chiefs of Staff
KBPS	Kilobits Per Second (1,000 bits)
KDC	Key Distribution Center
KG	Key Generator
LAN	Local Area Network
LCM	Life Cycle Manager
LN	Line Deficiency - Used in Problem Reporting
LSP	Logistic Support Plan
MB	Mailbridge
MC	Monitoring Center
MGR	Manager
MILDEP	Military Department
MILNET	Miltary Network
MILNETMGR	MILNET Manager
MIL-STD	Military Standard
MOA	Memorandum of Agreement
MT	Management Threshold
MTAC	Mini-Terminal Access Controller
MTBF	Mean Time Between Failure
MTTR	Mean Time To Repair
NAURS	Network Audit-Trail and Usage Reporting System
NCAN	Network Change Action Notice
NCD	Network Change Directive
NCR	Network Change Request
NCS	National Communications System
NIC	Network Information Center (Stanford Research Institute)
NIS	Naval Investigative Service
NSA	National Security Agency
NSC	Node Site Coordinator
NSO	Network Security Officer
NU	Network Utilities
NURS	Network Usage Reporting System
OC	Operations Center
O&M	Operations and Maintenance
OCONUS	Outside Continental United States
OP	Operations Deficiency - Used in Problem Reporting
O/S	Operating System

PACDISMGR	Pacific DISNET Manager
PACDISNETSTA	Pacific DISNET Stations
PACMILMGR	Pacific MILNET Manager
PACMILNETSTA	Pacific MILNET Stations
PDB	Protocol Data Blocks
PDMC	Pacific DSNET1 Monitoring Center
PMMC	Pacific MILNET Monitoring Center
PO	Performance Objective
POC	Point of Contact
PPBS	Planning, Programming, and Budgeting System
PR	Problem Report
PRB	Problem Review Board
PSN	Packet Switching Node
PT	Plaintext
PTF	Patch and Test Facility
PW	Power (Environmental) Deficiency - used in Problem Reporting
QA	Quality Assurance
RFC	Request for Comments
RFO	Reason for Outage
RMKS	Remarks
RP	Restoration Priority
SAVPIN	Standard Audio-Visual Product Identification Numbers
SCC	Security
SCI	Sensitive Compartmented Information
SCINET	Sensitive/Special Compartmented Information Network
SCINETMGR	SCINET Manager
SCO	Systems Control Officer
SCP	System Change Proposal
SDD	System Documentation Deficiency
SI	Special Interest
SMC	Sensitive Compartmented Intelligence Network (SCINET) Monitoring Center
SMTP	Simple Mail Transfer Protocol
SOD	System Operating Deficiency
SOP	Standing Operating Procedure
SRR	Software Release Request
SSD	System Software Deficiency
STU	Secure Telephone (Terminal) Unit
SW	Software Deficiency - Used in Problem Reporting
SY	System Problem - Used in Investigation Requests
TAC	Terminal Access Controller
TACACS	TAC Access Control System
TACNEWS	TAC News
TCF	Technical Control Facility
TCP	Transmission Control Protocol
TELCO	Telephone Company
TELNET	Telecommunications Network
TSO	Telecommunications Service Order
TSR	Telecommunications Service Request
UDCP	Usage Data Collection and Processing System
UID	User Identification

USAF	United States Air Force
WESTHEM	Western Hemisphere
WIN	WWMCCS Intercomputer Network
WINCS	WWMCCS Intercomputer Network Communications Subsystem
WINCSMGR	WINCS Manager
WMC	WINCS Monitoring Center
WWMCCS	Worldwide Military Command and Control System
ZIP	Zone Improvement Plan

This page is intentionally left blank.

GLOSSARY OF TERMS

Access Line. A circuit that connects a DDN subscriber (host or terminal equipment) to DDN node equipment (a PSN, TAC, or MTAC).

Analog Signal. A signal in the form of a continuously varying physical quantity, such as voltage, that reflects variations in information states.

Area Communications Operations Center (ACOC). The ACOC exercises day-to-day operational direction over the DCS control facilities, DCS switching facilities, satellite facilities, and other DCS operating elements, either directly or indirectly, through its subordinate regions within the assigned geographical area. The ACOC is part of the DCA Operations Control Complex (DOCC).

ARPANET. An experimental packet switching network developed by the Defense Advanced Research Projects Agency (DARPA). The ARPANET was the progenitor of the DDN packet switching network.

Asynchronous. Transmission in which the intervals between transmitted characters may be of unequal length. Transmission is controlled by start and stop elements at the beginning and end of each character.

Automatic Digital Network (AUTODIN). The DoD worldwide, common-user, general purpose, record communications network that serves both the Defense Special Security Communications System (DSSCS) and General Service (GENSER) communities.

Availability. The percentage of time a circuit or facility is capable of processing traffic including authorized service interruptions in the computations.

Baud Rate. A unit of signaling speed. The baud rate is the number of discrete conditions or signal elements per second. This applies only to the actual signals on a communications line. If each signal event represents only one bit condition, the baud rate is the same as "bits per second." When each signal event represents other than one bit, as with advanced encoding techniques, such as phase-shift keying, the baud rate does not equal "bits per second."

Bi-synchronous Binary synchronous.

Bit. A contraction for "binary digit." A bit can assume one of two states: on or off. It is the smallest unit of information in a digital system.

Bits Per Second (bps). A measure of the rate of information transfer, i.e., the number of bits passing a particular point per second.

C/30. The BBNCC processor used as a Defense Data Network packet switching node (PSN) (C/30E or C/300 version) or as a terminal access controller (TAC) (C/30 version).

C/70. The BBNCC processor used in the Defense Data Network Monitoring Center.

Circuit Control Office (CCO). The facility identified by DCA as responsible for overall restoration actions of a circuit. A CCO is designated in the Telecommunications Service Order (TSO).

Clock. A repetitive, precisely timed signal used to control a synchronous process such as logic or transmission. Sometimes clock refers to the device used to generate the signal.

Command Communications Service Designator (CCSD). The Defense Communications System (DCS) circuit number.

Communications Security (COMSEC). Cryptographic equipment and ancillary devices for communications that provide for link encryption or decryption on circuits.

Configuration Management (CM). CM provides an orderly and accountable control over a network and its backbone components as they exist and as they change.

Connection. The term connection means the physical path allowing the subscribers terminal to communicate with a Host TAC or MTAC. It also indicates the physical path between the Host, TAC or MTAC and the PSN.

Contractor Investigation Request (IR) Manager. The Contractor IR Manager is a DCA contractor designated person responsible for receiving, recording, analyzing, tracking, correlating applications across networks, and reporting on the status of Investigation Requests.

CONUS (Continental United States). The 49 contiguous states, Alaska, and the District of Columbia. This excludes Hawaii, as well as territories and possessions.

Data Circuit-Terminating Equipment (DCE). The device and the connections that are placed at the interface to a network by the network provider and to which the user's equipment (DTE) is connected.

Data Service Unit (DSU). A device that performs a signal processing, control signaling, and other functions necessary to transmit data over a digital data transmission system.

Data Terminal Equipment (DTE). The device, generally belonging to a data communications user, that provides the functional and electrical interface to a communications medium. The DTE is the source or destination of data messages or transactions, such as a host computer, a synchronous or an asynchronous terminal, a teleprinter, or a CRT. DTE also describes, in telephony, a device that is connected to a modem (data set).

Database. A comprehensive collection of related data organized for quick access.

Dataphone Digital Service (DDS) (AT&T Trademark). A system that provides a private-line, two-point, dedicated, full-duplex transmission capability at synchronous data rates up to 56 kbps.

Defense Communications Agency Operations Control Complex (DOCC). The DOCC is the collection of DCA control centers that are assigned the responsibilities of levels 1 and 2 of the system control hierarchy. This includes the DCAOC, ACOC"s, RCOC's, and associated emergency relocation sites (ERS's).

Defense Communications System (DCS). The DCS is a composite of DoD-owned and leased telecommunications subsystems and networks composed of facilities, personnel, and material under the management control and operational direction of the DCA. It provides the long-haul, point-to-point, and switched network telecommunications needed to satisfy the requirements of DoD and certain other Government agencies.

Defense Communications System Data Systems (DCSDS). The principal assigned to manage the Defense Data Network, to include business management, acquisition and development management, testing and evaluation, operations and maintenance, configuration management, subscriber interface for CONUS and outside of CONUS (OCONUS).

Defense Data Network (DDN). A highly survivable, dependable, and cost-effective common user data communications network that will satisfy all current requirements and is expandable and adaptable to meet all projected requirements for the 1990's and is based on proven technology from existing operational networks. The DDN is an umbrella for several subnetworks. The subnetworks are described in Chapter 2 of this Circular.

Defense Switched Network (DSN). A computerized voice network, configured to interconnect a multiple number of voice switches and their subscribers on a worldwide basis. (Replacement for the Automatic Voice Network (AUTOVON.)

DCSDS Investigation Request Manager. The DCSDS IR Manager is the DCA management control focal point for IR actions, and is responsible for evaluating, forwarding, monitoring, filing, distributing, and authorizing opening and closing of IR's.

Delay. The sum of queuing, servicing, and propagation times across a transmission medium from network source to destination.

Digital Signal. Signals that are completely separate from one another, changing from a high state to a low state with an insignificant transition time lapse.

Domains. Domains are administrative entities that divide the name management required of a central administration and assign it to sub-administrations. For example, one first level domain is "MIL" standing for military. The second level domain further delineates the "MIL" domain by identifying the specific Service or Department, i.e., "AF" for Air Force, "ARMY" for Army, "NAVY" for Navy, "DLA" for Defense Logistics Agency.

Dual Homing. The connection of a DDN user device so that it is served by two DDN nodes.

Front-End Processor. A dedicated communications computer at the "front end" of a host computer. It may perform line control, message handling, code conversion, error control, and applications functions such as control and operation of special-purpose terminals.

Gateway. A device or a pair of devices that interconnect two or more subnetworks, enabling the passage of data from one subnetwork to another.

Greenwich Mean Time (GMT). The time used to provide a common worldwide reference time base. Also, referred to as Zulu Time.

Header. The initial segment of a data block or a packet that provides information about handling the rest of the blocks.

High-Level Data Link Control (HDLC). A synchronous, full-duplex, link-level, bit-oriented type of frame transmission. Information is represented as individual bits, which are not organized into characters.

High-Level Data Link Control (HDLC) Distant Host (HDH) Protocol. The HDH protocol supports the connection of a device to a packet switch when the device and the packet switch are separated by more than 2,000 feet. This protocol permits any subscriber host with an HDLC protocol capability to use the 1822 protocol.

Host. Any device that has sufficient intelligence to execute the protocols required to connect directly to a network packet switch and that can properly execute an "open connection" from the network, thus forming an active, usable connection.

Internet. A collection of heterogeneous networks that are interconnected by gateways. All hosts and gateways in an internet speak a common internet protocol in addition to specific network protocols. The term catenet is used to refer to an internet.

Inter-switch Trunk (IST). A communications line that connects two PSN's.

Investigation Request (IR). An IR is a documented investigation of escalated operational problems, requiring additional technical and/or managerial resources to resolve or which need subnetwork-wide implementation.

Kilobit Per Second (kbps). A measurement of the rate of data transmission; i.e., 1,000 bits per second.

Local Host or Terminal. A host or terminal that is located close enough to the PSN or TAC so that it may be directly connected; i.e., does not require any intermediate modems or signal conditioning equipment.

Mini Terminal Access Controller. Similar to a TAC in that it is a special purpose computer designed solely to interface terminals to the network. Different from the TAC in that it only provides sixteen connectors but allows the use of asynchronous, bi-synchronous, and IBM synchronous Data Link Control (SDLC) with System Network Architecture (SNA) protocols.

Modem. Contraction for modulator-demodulator. A device that modulates and demodulates signals transmitted over communications facilities. The modulator is included for transmission and the demodulator for reception. A modem permits digital signals to be sent over analog lines. Also called data set.

Monitoring Center (MC). The MC performs the functions of network monitoring, problem resolution, database configuration, installation, test and acceptance, and network status administration.

National Communications System/DCA Operations Center. The central control element of the DOCC, located at Headquarters, DCA, that exercises operational direction of the DCS either through the ACOC's for overseas areas or directly in the CONUS, Alaska, and Panama.

Netlog. The netlog displays real time event messages received by the Network Utilities program from the network entities (e.g., PSN's, TAC's, AND MB's). Event messages consist of status, trap, and controller action messages.

Network. A DDN segment including all its inter-switch trunks, packet switches, and access lines.

NIC. The Network Information Center provides network registration, TAC access control, network auditing, and general assistance services for the DDN and its subscribers.

Node. A location that supports DDN hardware. Usually includes communications equipment, PSN's, TAC's, and support devices. The node site may have many of these devices and circuits.

Node Site Coordinator. A person who has site access control and coordination responsibility for DDN matters at a DDN node site.

O&M Elements (O&M Activities). Organizations responsible for the operation, maintenance, or management for a DCS station.

Packet. A group of binary digits, including data and call control signals, that are switched as a composite whole. The data, call control signals, and error control information are arranged in a specified format.

Packet Switching Node (PSN). The packet switch in the DDN that provides full-service network access ports for host computers and IST connectivity between PSN's.

Patch and Test Facility (PTF). The PTF is the part of a DCS station that functions as a supporting activity under the technical supervision of a TCF. It has the physical and electrical capability to perform required functions.

Port. A physical connection outlet on a communications device through which it is connected to another device.

Problem Report (PR). A Problem Report documents an occurrence and possible resolution of an operational problem.

Problem Review Board (PRB). A PRB is established for each Monitoring Center with operational technical support, and other appropriate representatives to review all PR's generated by that MC for tracking purposes, closure or possible escalation to an Investigation Request (IR) recommendation.

Protocol. Strict procedures that are required to initiate and maintain communication. An ordered set of defined, published procedures that regulate interaction throughout the network. Protocols may exist at many levels in one network, such as link-to-link, end-to-end, and subscriber-to-switch. Protocols specify the order of activity in a communications session and the meanings of commands. Options available and responses to choices in network operation are also specified.

Raday. The 24-hour day in Greenwich Mean Time. (See Greenwich Mean Time.)

Reliability. The percentage of time a circuit or facility was capable of processing traffic, excluding authorized service interruptions in the computation. Circuit reliability excludes authorized service interruptions, preemptions, and PSN or TAC outages.

Remote Host or Terminal. Host or terminal equipment located at a distance that requires the use of intermediate modems or signal conditioning equipment on the access line.

Restoration Priority (RP). The NCS Circuit Restoration Priority System applies to communications circuits of Federal Government departments and agencies, to include DCS circuits. The RP system is designed to identify in which order circuits should be restored in the event of a failure.

Shadow Mode. Shadow Mode is a term describing the state of the multiple MC's (NU systems) and nodes when they are cooperating in providing the multiple monitoring center backup environment. If Shadow Mode is configured on the network, it is invoked automatically when NU is turned on.

Single-Homing. The connection of a DDN user device so that it is served by one DDN node.

Subscriber. Synonymous with User.

Synchronous. Having a constant time interval between successive bits, characters, or events. (See: "Asynchronous.")

TAC Access Control System (TACACS). The TACACS restricts network access for users connecting to the MILNET through a TAC.

Technical Control Facility (TCF). The TCF is the part of a DCS station that functions as the interface between the transmission elements of the DCS and the users of the system. It has the physical and electrical capabilities necessary to perform the required functions.

TELCO. Whatever agency provides local telephone facility service. TELCO connectors refer to the commercially available connectors that are in wide use by the telephone industry in the U.S.

TEMPEST. A test and certification program that attempts to preclude compromising electromagnetic emanations from communications equipment.

Terminal. A data input/output device that can be connected to the network. Most terminals consist of a keyboard for data entry and a screen or printer for data display. (Can be a user device such as a video display terminal, a portable printing terminal, or a personal computer.) Also refers to a connection point on an electrical component or device.

Terminal Access Controller (TAC). A special-purpose computer designed solely to interface terminals to the network which can support up to sixty-four synchronous terminals.

Trap Messages. Messages sent from PSN's, TAC's and MTAC's to report on unusual network behavior. These messages are collected by the Network Utilities Software System at the appropriate MC and evaluated by the network analysts.

User. A term used to identify a directly connected communications computer or automatic data processing equipment, which uses the DDN for the exchange of traffic with other distant communications computers, or automatic data processing equipment. For reporting purposes, user includes any host or terminal connected to a PSN or TAC.

User Access. The term "access" means the capability to use a particular path to conduct a session with the device to which a connection has been made.

Zulu Time. The time used to provide a common worldwide reference time base. Also, referred to as Greenwich Mean Time (GMT).

CHAPTER 1. INTRODUCTION

1. General. In April 1982, the Department of Defense (DoD) directed that the Defense Data Network (DDN), based upon Advanced Research Projects Agency Network (ARPANET) technology, be implemented as the DoD common user data-communications network to allow for the phasing out of expensive, single-user, high-speed circuits between host computers and their remote users. The DDN, an element of the Defense Communications System (DCS), is now the primary means of providing long-haul (e.g., beyond post, camp, or station boundary) data communications for all DoD sponsored data systems. It provides a highly reliable and fast, worldwide computer-based packet switched communications capability for the military departments and defense agencies.

2. Mission. The mission of the DDN is to provide common-user data communications services in support of military operational systems, to include intelligence systems, command and control systems, general purpose ADP, and other long-haul data communication systems.

3. Policy. This Circular prescribes procedures to standardize functional operations areas, promulgates network policy, and details the responsibilities of various associated network elements. This Circular prescribes user operating procedures and provides specific responsibilities, guidelines, and general information to improve network effectiveness.

4. DDN Publications.

a. The following listed documentation contain pertinent procedures, policies, and instructions which the users of this Circular may refer to for more details regarding a particular area. A brief description of the contents of each publication is provided to assist in selecting the proper document when a specific subject matter is desired. It is not necessary or desired that all users hold all of the referenced documents.

(1) DCAC 270-P120-3, Logistics Support Plan for the Defense Data Network. Provides logistical support information, instructions, guidance, and direction to DoD elements and other Government agencies concerned with support of the DDN.

(2) DCAC 300-85-1, Reporting of DCS Facility and Link Data RCS: DCA(AR) N3303. Procedures for the preparation and submission of initial reports and subsequent change reports required to maintain data accuracy and currency of DCS Facility and Link information, pertaining to DoD-owned and leased facilities, in the DCA database.

(3) DCAC 310-50-5, Defense Communications Agency Operations Control Complex and Operational Direction Over the Defense Communications System. Establishes the policy for the operational direction over the DCS and prescribes the operational principles and functions of the Defense Communications Agency Operations Control Complex (DOCC).

(4) DCAC 310-55-1, Status Reporting for the Defense Communications System. Prescribes instructions for status reporting of the DCS.

(5) DCAC 310-70-1, DCS Systems Control, Vol 1 and Vol 2. Contains DCS facilities descriptions, and prescribes the policy and procedures for performing quality assurance, quality control, technical supervision, service restoral, and status reporting. Volume 1 provides a general overview of DCS policy and responsibilities. Volume 2 provides specific operational procedures, e.g., DDN outage procedures.

(6) DCAC 310-70-57, DCS Quality Assurance Program. Establishes the procedures, organizational responsibilities and relationships, and reporting for the DCS Quality Assurance Program.

(7) DCAC 310-P70-69, BBN O/S PEN Editor User's Guide. Overview of and the procedures for the operation of PEN, a video text editor used with electronic mail (E-Mail).

(8) DCAC 310-P70-70, InfoMail Primer. Provides an overview and the procedures for the use of the InfoMail information management and E-Mail system.

(9) DCAC 310-P70-71, Infomail Reference Manual. Provides procedures for the InfoMail information management and E-Mail system.

(10) DCAC 310-P70-74, Terminal Access Controller User's Guide. Prescribes the procedures for a user accessing a TAC.

(11) DCAC 310-P70-75, Host Administrator Guide-C/70. A guide for C/70 host management and administration.

(12) DCAC 310-P70-76, Node Site Coordinator Guide. Describes the role, responsibilities, and procedures of a Node Site Coordinator.

(13) DCAC 310-130-1, Submission of Telecommunications Service Requests. Prescribes instructions for the preparation and submission of Telecommunications Service Requests (TSR's) applicable to requirements for DCS service.

(14) DCAC 310-130-2, Defense Communications Management Thresholds and Performance Objectives. Establishes DCS management thresholds and performance objectives.

(15) DCAC 350-85-3, Communication Status (COMSTAT) Report. Prescribes procedures and delineates responsibility for preparation and distribution of the COMSTAT Report.

(16) DCAC 350-135-1, Defense Commercial Communications Acquisition Procedures. Delineates responsibility, prescribes procedures, and establishes the policy for the centralized procurement of commercial communications services to satisfy the telecommunications requirements of the departments, agencies, and offices of the DoD and other U.S. Government agencies authorized by the Secretary of Defense to procure service through DECCO.

(17) DCAC 300-175-9, DCS Operations-Maintenance Electrical Performance Standards. Specifies technical schedules and standards necessary to operate and maintain Government-owned circuits at the expected level of performance for the DCS and contains information on the availability and performance of leased circuits in the CONUS, tariff requirements, and commercial carrier performance objectives.

(18) DCAC 370-P195-4, DDN Installation, Test and Acceptance Procedures. Sets standards and procedures for DDN installation and acceptance testing.

(19) DCAC 370-P195-5, DDN Host Interface Qualification Testing-Link and Network Layers. Specifies that all X.25 host interfaces must be qualified by DCA. Defines the DCA developed X.25 link and network layers comformance testing program.

(20) JCS PUB. 19, Volume I, Annex L, Operation and Management of the WWMCCS Intercomputer Network (WIN). The general policy and procedures for the effective operation and management of the WIN.

(21) JCS Memorandum of Policy No. 195, Defense Data Network and Connected Systems. Provides policy and direction for the DDN.

b. Requests.

(1) DCA Documents. Government agencies may request a publication by submitting a DCA Form 117: Publication or Blank Form Request. Other organizations may request a publication by submitting a letter with appropriate justification. The DCA Form 117 is used by Government agencies only. Send all requests for DCA documentation to:

Defense Communications Agency
Attn: BIAR (H316)
Washington, DC 20305-2000
Telephone: 202/692-6972 - (DSN) 222-6972

(2) Other Documents.

Defense Technical Information Center
Attn: DTIC-DDA
Cameron Station
Alexandria, VA 22314
Telephone: 703/274-7633 - (DSN) 284-7633

National Technical Information Center
5801 Tabor Avenue
Philadelphia, PA 19120
Telephone: 215/697-2000 - (DSN) 442-4120

National Technical Information Serice
5285 Port Royal
Springfield, VA 22161
Telephone: 703/487-4650

5. Network Responsibilities. The generalized responsibilities of the various supporting network elements include the following:

a. Joint Chiefs of Staff (JCS) Responsibilities.

(1) Review and approve all requirements for FLASH, EMERGENCY COMMAND, and CRITIC precedence capability.

(2) Provide support of the DDN through the Planning, Programming, and Budgeting System (PPBS), including contractor and foreign-government support.

(3) Provide guidance, and as appropriate, tasking to DCA, on military and communications doctrine and operational policies and procedures with regard to the development and operation of the DDN.

(4) Validate the use of DDN by non-DoD Federal, state, and local Government departments and agencies; foreign governments; allied organizations; and contractor-controlled systems.

b. Defense Communications Agency (DCA) Responsibilities.

(1) Prescribe, in coordination with the appropriate DoD components, policies, procedures, standards, and practices for the effective use of DDN.

(2) Prescribe the interface protocol standards to be used on DDN.

(3) Authorize the implementation of DDN backbone software and hardware changes.

(4) Perform the acceptance test of new DDN backbone software or hardware.

(5) Provide current traffic statistics with narrative analysis of trends, deficiencies, and corrective actions.

(6) Exercise operational direction and management control of the DDN.

(7) Provide the appropriate information, protected according to security classification, upon which all DoD elements can implement usage-sensitive billing.

(8) Safeguard the security and privacy of user traffic.

(9) Monitor and control network performance to comply with DDN Performance Objectives (PO's) and Management Thresholds (MT's).

(10) Design DDN to provide efficient communications between both similar and dissimilar computers so that hardware, software, data resources, and circuitry can be conveniently and economically shared by a wide community of users.

c. National Security Agency (NSA) Responsibilities. In accordance with the provisions of DoD Directive C-5200.5, 6 October 1981, "Communications Security (COMSEC)(U)," recommends basic doctrine, methods, and procedures to minimize DDN information security vulnerabilities.

d. Defense Intelligence Agency (DIA) Responsibilities. As appropriate, validates all DoD requirements and accredits each system requiring Sensitive Compartmented Information (SCI) access to DDN. Manages and operates the DSNET3 Monitoring Center (MC).

e. Military Departments (MILDEP's) and DoD Agency Responsibilities.

(1) Review and, if appropriate, approve all sponsored hosts' precedence level requests. Forward all approved FLASH, EMERGENCY COMMAND, and CRITIC precedence requests to JCS.

(2) Review and, if appropriate, approve requests for DDN access. Forward approved requests to DCA.

(3) Provide COMSEC equipment installation, operation, maintenance, control, and accounting.

(4) Program, budget, fund, and provide support for assigned portions of DDN through the PPBS.

(5) Maintain communications and physical security, meeting the DDN security architecture requirements.

(6) DCA Circular defining DDN operating policy and procedures are implemented.

(7) Ensure procedures for usage-sensitive billing are implemented to the lowest practical user level.

(8) Develop and implement management procdures for coordinating, installing, testing, and maintaining user access.

f. DDN Node Site Coordinator (NSC) Responsibilities.

(1) Act as a DDN Packet Switching Node (PSN) site focal point for coordinating all network support activities.

(2) Comply with role and responsibilities as outlined in DCAC 310-P70-76, Node Site Coordinators Guide.

(3) Notify the NIC of any changes to the assigned primary and alternate NSC's.

g. DDN Host Administrator (HA) Responsibilities.

(1) Assist DCA by ensuring that network policies and procedures are observed by their host users.

(2) Administer the Terminal Access Controller (TAC) Access Control System (TACACS), to ensure all host subscribers, using the network or the TAC's, have been authorized for DDN and TAC access, and are registered in the Network Information Center (NIC) User Registration Data Base (WHOIS/NICNAME).

(3) Manage their host's network access control procedures and password system; be responsible for reporting network-related host unauthorized intrusions and assist with investigative effort as needed.

(4) Coordinate with DCA on installation, connection and removal of hosts on the DDN. Provide the DCS Data Systems (DCSDS) directorate with required descriptive information for each new host addition or host change. Coordinate the host certification procedure with the DCS Data Systems Directorate prior to passing traffic or testing on the network.

(5) Implement and maintain DDN protocols at the host level.

(6) Serve as local point of contact for the respective hosts and local users and coordinate suspected network-related problems directly with the appropriate DDN Trouble Desk or Monitoring Center for correction.

(7) Provide network information to the NIC, and assist local subscribers and other interested personnel with network-related matters.

(8) Notify the NIC of any changes to the assigned HA and the host technical representative.

NOTE: DCAC 310-P70-75 can be used by HA's as a general guide for host management and administration. Due to the variety of host hardware and software in the DDN, it is not feasible to develop specific document.

CHAPTER 2. NETWORK DESCRIPTION

1. General. This chapter provides a brief overview of the DDN composition and elements. A detailed system description is published in DCAC 310-P70-1, Defense Data Network (DDN) System Description.

2. Network Composition.

a. Functional Areas. The elements of the DDN are grouped into two functional areas:

(1) The network backbone is comprised of Packet Switching Nodes (PSN's), Inter-switch Trunks (IST's), Terminal Access Controllers (TAC's), MTAC's, Mailbridges (MB's), and Monitoring Centers (MC's).

(2) User access, consisting of dedicated or dial-up circuits, interface equipment, and compatible protocols.

b. Subnetwork Description. The DDN is an umbrella for several subnetworks: the Military Network (MILNET) and the three Defense Secure Networks (DSNET's). In the future, the three DSNET segments will be integrated into one subnetwork named Defense Integrated Secure Network (DISNET).

(1) Military Network (MILNET). Unclassified segment of the DDN. Network backbone composition is as described in paragraph 2a(1) above.

(2) DSNET1 (formerly, Defense Integrated Secure Network, DISNET). Classified segment of the DDN that carries up to SECRET level information. Network backbone composition is similar to the MILNET (except MB's), but all facilities and circuits are protected at the SECRET level.

(3) DSNET2 (formerly, WWMCCS Intercomputer Network Communications Subsystem, WINCS). Classified segment of the DDN that carries up to TOP SECRET level information. Network backbone composition is restricted to PSN's and IST's, and includes preplanned alternate data circuits as approved in JCS PUB 19, Annex L, Vol I. All facilities and circuits are protected at the TOP SECRET level.

(4) DSNET3 (formerly, Sensitive Compartmented Information Network, (SCINET). Classified segment of the DDN that carries up to Sensitive Compartmented Information (SCI) level information. Network backbone composition is restricted to PSN's and IST's. All facilities and circuits are protected at the SCI level.

(5) DISNET (Defense Integrated Secure Network). The DSNET's will be integrated into a single network, the DISNET, when an approved end-to-end encryption device is available. Until then, the DSNET's will operate as separate, dedicated networks.

3. Network Elements.

a. Packet Switching Nodes (PSN's). The PSN's serve as the interface points between the host computers and the network backbone.

(1) Hardware. The packet switch permits a variety of input and output configurations so that a mixture of high-speed trunks and hosts can be connected. The configurations can accommodate hosts that are either collocated with the PSN at a site, or remotely located.

(2) Software. The PSN's software includes an adaptive dynamic routing algorithm that continuously monitors network delays, and forwards transiting packets via routes that minimize the delay time. In addition, the PSN software ensures packet integrity through the use of a 16-bit cyclic redundancy check (CRC) and an error detection and correction (EDAC) memory. Congestion control allows the packet switch to continuously monitor shared resources and responds to traffic conditions that could result in oversubscription of these resources; as a result, the network adjusts traffic flows to resolve any oversubscription. For example, one resource that must be managed in this way is the supply of data buffers.

(3) Standard PSN Suites.

(a) Unclassified Node Suite. The standard unclassified node consists of a five cabinet suite. These cabinets are:

1. A processor cabinet, which holds the PSN and TAC.

2. Two encryption cabinets, which contain Fixed Plant Adapters and KG-84A's.

3. Two communications cabinets, which contain space for modems.

(b) Classified Node Suite. The standard classified node consists of a four cabinet suite. These cabinets are:

1. A processor cabinet, which holds the TEMPEST-equipped PSN and TAC.

2. Two encryption cabinets.

3. One communications cabinet.

b. Inter-switch Trunks (IST's). IST's are common-carrier, dedicated data circuits interconnecting the PSN's. They range from 9.6 to 56 kilobits per second in speed. All IST's of the DDN are, or will be, protected with KG-84A encryption devices. Currently, DSNET2 uses KG-34's for IST link encryption but replacement KG-84A's are being phased in. All IST's on DSNET1 and DSNET3 use KG-84A's for link encryption. IST's on the MILNET are being encrypted with KG-84A's on a phased implementation plan.

c. Terminal Access Controllers (TAC's) and Mini-TAC's (MTAC's). The TAC's and MTAC's serve as the interface points between direct-connect and dial-up terminal users, and the network backbone. Detailed procedures for using TAC's and MTAC's are included in the DCAC 310-P70-74, Terminal Access Controller User's Guide.

d. Mailbridges (MB's). The MB's serve as specialized internet gateways with the limited function of transferring electronic mail between the networks, specifically MILNET and the ARPANET. An individual MB will not permit network users interactive access to hosts on the connected networks without authorization.

e. Monitoring Center (MC). The MC description and functions are contained in Chapter 4.

(Note: All network backbone elements, except the MC, are designed to operate unattended during normal operations. Normally, monitoring, diagnostics, fault isolation, service restoral, and software reconfiguration can be handled remotely by the MC. In some cases, the MC will request assistance from the NSC or EA to enhance troubleshooting and restoral.)

4. Network Access. All user components and connecting circuits that collectively access the network compose what is referred to as the access area. User devices configured with DCA approved hardware, software, and network access protocols are connected to a PSN and are commonly called hosts. User devices without these protocols are connected to a TAC or MTAC and are commonly called terminals. (See Figure 2.1.)

a. Host Access. DCAC 370-P195-5, Defense Data Network Host Interface Qualification Testing-Link and Network Layers, defines the DCA-developed X.25 link and network layers conformance testing program. All host interface products must be qualified under this program prior to connection to DDN. A qualified X.25 host interface list is available from the NIC.

(1) Mandatory Protocols.

(a) DDN network access protocols are: DDN X.25 Standard, DDN X.25 Basic, and ARPANET Host Interface Protocol (AHIP) 1822.

1. Standard X.25 provides interoperable communications between an X.25 Data Terminal Equipment (DTE) and 1822 hosts using the DoD standard protocols.

2. Basic X.25 provides interoperable communications between X.25 DTE's using only compatible higher-level protocols.

3. AHIP 1822 protocols provide a common base for supporting higher level protocols. The DDN is migrating away from the AHIP protocol and will use the DDN X.25 Standard as a baseline protocol.

(b) Internet Protocols (IP) allows the transmission of data across multiple packet-switched data communications networks.

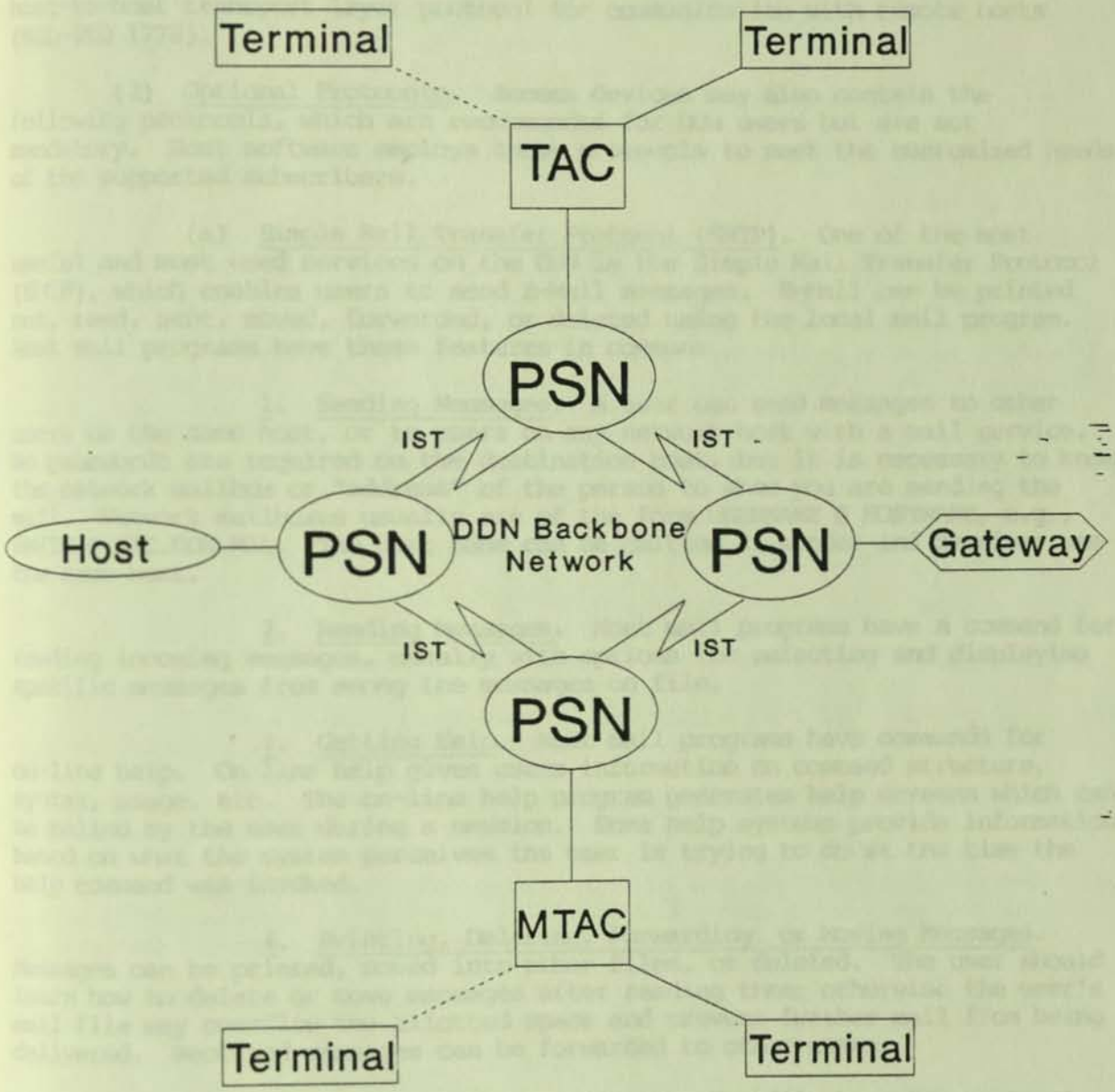


FIGURE 2-1. VARIOUS NETWORK CONNECTIONS

(c) Transmission Control Protocol (TCP) is the standard host-to-host transport layer protocol for communication with remote hosts (MIL-STD 1778).

(2) Optional Protocols. Access devices may also contain the following protocols, which are recommended for DDN users but are not mandatory. Host software employs these protocols to meet the customized needs of the supported subscribers.

(a) Simple Mail Transfer Protocol (SMTP). One of the most useful and most used services on the DDN is the Simple Mail Transfer Protocol (SMTP), which enables users to send E-Mail messages. E-Mail can be printed out, read, sent, moved, forwarded, or deleted using the local mail program. Most mail programs have these features in common:

1. Sending Messages. A user can send messages to other users on the same host, or to users on any network host with a mail service. No passwords are required on the destination host, but it is necessary to know the network mailbox or "address" of the person to whom you are sending the mail. Network mailboxes usually are of the form USERNAME @ HOSTNAME, e.g., SMITH @ NIC.DDN.MIL. The host name can be omitted if sender and receiver use the same host.

2. Reading Messages. Most mail programs have a command for reading incoming messages, usually with options for selecting and displaying specific messages from among the messages on file.

3. Getting Help. Most mail programs have commands for on-line help. On line help gives users information on command structure, syntax, usage, etc. The on-line help program generates help screens which can be called by the user during a session. Some help systems provide information based on what the system perceives the user is trying to do at the time the help command was invoked.

4. Printing, Deleting, Forwarding, or Moving Messages. Messages can be printed, moved into other files, or deleted. The user should learn how to delete or move messages after reading them; otherwise the user's mail file may overflow the allotted space and prevent further mail from being delivered. Received messages can be forwarded to other users.

(b) File Transfer Protocol (FTP). The file transfer protocol (FTP) makes it possible to move a file from one computer to another, even if each computer has a different operating system and file storage format. Files may consist of data, programs, text, or anything that can be stored digitally. An active host is the computer to which the user is logged on. The passive host is either the source or destination of the files to be transferred. The following are the general steps for transferring a file:

1. Log on to the active host and invoke the FTP program.

2. Provide the host name or host address of the passive host.

3. Once connection has been established to the passive host, log on with user name and password.

4. Issue commands to copy or send files.

5. When finished, log off from the remote host and exit from the FTP program.

(c) Telecommunications Network (TELNET). One other common use of the DDN is for users to log on to a remote computer from a local host by using the TELNET protocol. Once connected and logged on to the remote host, users can enter data, run programs, or do any other operation, just as if they were directly connected. This is similar to a user who logs on to a TAC and uses a remote network host. The difference is that in this case, the network access component is a local host. A specialized use of TELNET is to connect to a particular "assigned port" on a remote host. This type of connection takes the user directly to the program or service offered on that port. A summary of TELNET steps are as follows:

1. Log on to a local host.

2. Invoke the TELNET program from the local host.

3. Identify the remote host by host name or host address.

4. Once connected to the remote host, log on with user name and password for the remote host system.

5. When finished working on the remote host, if the connection is not automatically terminated, break the connection.

b. TAC Access. A user can gain access to the network for a connection to a remote host computer through a TAC. The TAC access procedures are explained in DCAC 310-P70-74. The standard types of TAC access are as follows:

(1) Hard-Wired Terminal-to-TAC Connection. The standard direct physical connection for a terminal to a TAC is EIA RS-232-C (25 pin) connector.

(2) Dial-Up Terminal-to-TAC Connection. On MILNET, a dial-up terminal may also communicate with a TAC. Regardless of the kind of telephone line, a dial-up connection means that the TAC's attention is gained by dialing or specifying a telephone number and letting the TAC answer the telephone on the other end. A dial-up connection always requires a dial-up procedure to establish connection between the terminal and the TAC. There are two steps in connecting a terminal to a TAC using the telephone system. Further details can be obtained from DCA Circular 310-P70-74. Because the exact procedures required to "dial-up" the TAC vary from site to site, the user should consult with the NIC.

(a) The telephone number of the nearest TAC may be obtained directly from the network by using TACNEWS service or by calling the NIC. The telephone number of a specific TAC may be obtained from the NIC WHOIS server.

(b) The user should consult the manufacturer's instruction guide which comes with the modem, data set, or acoustic coupler for details on how to attach the device to the terminal, how to set it properly, and how to dial. Note that the transmission speed of the modem and terminal must match. In general, the user will dial the TAC number in the telephone and wait for the tone, switch the modem from "voice" to "data," and set the handset back on the telephone cradle. Note that some modems are "smart," i.e., the user can dial directly from the terminal.

c. Gateway Access. A terminal or computer connected to a LAN can communicate through the DDN if the LAN is connected to a gateway. The gateway is a computer whose software interfaces the protocols of both networks. The gateway is transparent to the user; no special commands or syntax are needed for communication through a gateway.

3. Network Naming and Addressing. Each host on the DDN has a unique host name and a host address associated with it as a means of identification. This address tells network programs the location of a host and on which subnetwork it resides. The host address includes four units of information, with each part separated by a decimal point. These units indicate the network address, the host port number on the PSN, a reserved section (usually zero), and the number of the PSN to which the host is connected, e.g., 26.3.0.45. A host name or address must be known to use network services such as TELNET or FTP, or to open a connection to a host via a TAC.

4. Common TAC Logon Problems.

a. If the logon sequence fails on a MILNET TAC, the user should examine the TAC access card carefully to be sure the User Identification (UID) and access code were correctly entered. Access codes never contain a zero (0), que (Q), one (1), or zee (Z), since each of these characters may be mistaken for another. If what appears to be one of the above characters is given on the access card, it is really the letter oh (O), gee (G), el (L), or the number two (2).

b. If the user continues to have difficulty logging on to the TAC after following the above procedures and being sure that the UID and access code were correctly entered, the user should call the NIC for additional help.

5. TAC Port Management. DCSDS is the central management authority for all TAC port assignments. Under no circumstances will site personnel (specifically the NSC) make changes or allow changes to be made to any TAC without specific DCA authorization.

CHAPTER 3. NETWORK SECURITY

1. General. Several safeguards are used on DDN to protect the security and privacy of subscriber traffic. These safeguards include separation of traffic with different classifications, separation of traffic to specific Communities of Interest (COI's), network access control, link encryption, and security violation reporting. Personal safeguards are also essential to network security.

2. Subnetwork Division.

a. DoD 5200.1-R, Information Security Program Regulation, requires division of traffic by security level and accreditation authority. As stated in Chapter 2, the DDN is an umbrella for several subnetworks which were derived by the level of classification needed for transiting traffic. More specifically, MILNET carries unclassified traffic, DSNET1 carries up to Secret traffic, DSNET2 carries up to Top Secret traffic, and DSNET3 carries up to Top Secret Sensitive Compartmented Information.

b. Implementation of BLACKER will allow integration of the DDN classified networks; e.g., DSNET1, DSNET2, and DSNET3 will integrate into one classified network, DISNET. The BLACKER system is a National Security Agency (NSA) developed COMSEC system certified as a Computer Security (COMPUSEC) system designed to support "multilevel" secure data communications for computer systems across packet-switched communications networks. Each COI within DISNET will be assigned to an administrative domain. Each domain will have the capability to have up to three Access Control Centers (ACC), two Key Distribution Center (KDC) pairs, and 1000 Blacker Front Ends (BFE).

(1) The ACC, the controlling element within a COI domain, mediates access permissions between BFE's fronting subscriber hosts and controls the KDC's. Access is in accordance to an access control database that defines the host pairs authorized to communicate and host pairs forbidden to communicate, and at which security level. The ACC is also the BLACKER System focal point for all security audit information in a domain.

(2) The KDC generates and distributes crypto-variable keys electronically over the network to BFE's in its domain authorized to communicate with each other by direction of the ACC. It maintains a database of all variables used within its domain and those used for inter-domain crypto-connections. The KDC is composed of a Key Variable Generator (KVG), a Key Management Interface Processor (KMIP) with associated peripherals, and it's own BFE.

(3) The BFE is a network interface device between an authorized host and a Packet Switch Node (PSN) and permits two hosts to exchange data with complete privacy and secure communications. By design it is transparent to both the network and the subscriber host. The PSN recognizes the BFE as a

host device while the host recognizes the BFE as a PSN. The BFE provides for black, plaintext (PT) at the Data Communications Equipment (DCE) interface to the host, and red, cyphertext (CT) at the Data Terminal Equipment (DTE) interface.

c. Within a given subnetwork, subscribers can be further subdivided into specific COI's. As explained above, separation of COI in DISNET will be by domain. COI separation is provided on the other DDN subnetworks by classmarking each subscriber of a known COI with a unique number identifying that COI. This capability is provided by a configurable parameter in the PSN software.

3. Network Access. Network access is based on subnetwork restrictions. For example, access to DSNET2 and DSNET3 is restricted to dedicated hosts. DSNET1 extends subscriber access to include limited use of TAC's and MTAC's, e.g., no dial-up connections, only limited use of dedicated TAC or MTAC terminals. MILNET has extensive use of host and TAC or MTAC terminal connections. In addition, MILNET has dial-up TAC and MTAC capability. TAC and MTAC access on MILNET is restricted by the TAC Access Control System (TACACS).

a. General Access Restrictions.

(1) Only subscribers engaged in U.S. Government business or research, or subscribers directly involved in providing operations and system support for Government-owned and/or sponsored computer communications equipment, may use the DDN. The network is not available for use by the general public, nor is it intended to compete with comparable commercial network services.

(2) Gateways and Local Area Networks.

(a) A DDN host system may include a gateway or a local area network (LAN). DCA is developing security standards for these. In the interim, host gateways and LAN's are required to meet the same standards of discretionary and mandatory security as other DDN elements.

(b) A DDN host system may include a gateway or LAN that attaches to a non-DDN subnetwork or ADP system. In this case, an authorized user might attempt access to DDN services or communications with other DDN users. DDN users would have no assurance that the non-DDN system met the security requirements necessary for interoperability. For this reason, DCA is preparing a security standard that addresses non-DDN attachments. In the interim, a DDN host must not allow a non-DDN user to gain access to services (such as FTP, SMTP, and TELNET) on a DDN subnetwork. If a non-DDN user has backside access to a DDN host, and if that user wishes to send data through a DDN subnetwork, the host must require the non-DDN user to first send the data to an authorized DDN user on the same host; then that DDN user may forward the information to other DDN hosts. The DDN host or user should use informal procedures to label such data to indicate to recipients that the data is possibly unreliable because of its source and the channel through which it passes. At a later date, DCA will establish formal labeling standards which will include the necessary support for standard protocols.

b. TAC Access Control System (TACACS). When a user attempts to access the network, the TACACS will intervene. TACACS requires terminal users to prove authenticity by providing a "user identification" (UID) with corresponding access code. Once this access code has been provided to and verified by TACACS, the authorized user is allowed access to the MILNET. The TACACS complies with CSC-STD-002-85, DoD Password Management Guidelines (otherwise known as the NSA Green Book); and the Federal Information Processing Standards Publication #112. (See Chapter 7 for TACACS registration procedures.)

(1) The TAC Access Audit Trail Analyzer (ATA) subsystem is the auditing and reporting facility of the TACACS. The ATA receives usage data from each TAC and records the UID (excluding the access code), the TAC host address and terminal port number, the destination host address, the number of packets passed through the network, and the approximate date and time of the session into the data base. MILNET TACACS automatically generates incident reports when certain unusual events occur. These reports are reviewed by the DDN Network Security Officer for indications of illegal or unauthorized network access attempts. TAC's used on the classified subnetworks have not yet implemented an audit trail and analysis capability. (See Chapter 7, paragraphs 3 and 4 for further definition of TACACS.)

(2) The NIC maintains a database for the MILNET TAC UID's that have been hot listed and for transmitting hot list updates to the appropriate MC's. The hot list is composed of the UID's of users who no longer have a need for network service, comprised UID's, and expired TACACS guest cards. Hot listed users cannot access the network through a TAC.

c. Host Access. Each host must also use a protective mechanism (e.g., subscriber identification and unique password log on) to authenticate a subscribers identity prior to accessing the host. This protective mechanism is host unique, therefore, is developed and maintained by the host administrator or other designated individual.

4. Circuit Encryption. All DDN IST's are encrypted to meet the security level required. For example, DSNET2 and DSNET3 use KG-34's and KG-84's to meet their security levels. DSNET1 uses KG-84's. MILNET is in the process of encrypting all IST's with KG-84's using unclassified key material. Subscriber access lines also comply with security levels, required for the assigned subnetwork.

5. Prohibited Acts. Subscribers of DDN must comply with all military, civilian and local regulations pertaining to data transmission systems.

a. Public Law 98-473, known as the "Counterfeit Access Device and Computer Fraud and Abuse Act of 1984," added Section 1030 to Title 18 United States Code on October 12, 1984. It was the first federal computer crime law to make unauthorized access to U.S. Government computers illegal. The law's definition of "computer" includes data storage or communications facilities directly related to or acting in conjunction with a computer. It prohibits anyone without authorization from knowingly accessing computer systems. Specifically, the code defense action as criminal of an individual:

(1) (1030(a)(1)) "...obtains information that has been determined by the U.S. Government...to require protection against unauthorized disclosure for reasons of national defense or foreign relations, or any restricted data as defined in...the Atomic Energy Act of 1964."

(2) (1030(a)(3)) "...uses, modifies, destroys, or discloses information in, or prevents authorized use of...(a) computer...operated for or on behalf of the government of the United States."

Individuals found guilty of unauthorized access or use of host computers over the DDN will be subject to prosecution under Title 18 of the Federal Criminal Code.

b. Transmission of information exceeding the classification level of the accessed subnetwork is strictly prohibited, per DoD 5200.1-R, Information Security Program Regulation. Military and civilian personnel of the DoD found guilty of compromising classified information are subject to administrative sanctions described in DoD 5200.1-R.

c. Subscribers must not use the network for advertising or recruiting purposes without written permission of DCA. The violators sponsoring O&M will be contacted for corrective action. Continued violation will lead to curtailment of subscriber access.

6. Security Violation Reporting.

a. Initial Notification. Any DDN user (person/department/agency) having knowledge of a suspected security violation must contact the appropriate Defense Communications Agency OC/ACOC MILNET Monitoring Center to report the violation. If possible, reporting should be via secure means. Secure and commercial telephone numbers to DCA Operations Centers are: WESTHEM/CONUS OC has KY3-2222; STU III (DSN312-222-2060; (COMM)202-692-5726-2268; or 1-800-451-7413. PACIFIC ACOC has STU III (DSN)315-456-2777; (COMM)808-656-2777. EUROPEAN ACOC has KY3-6429; STU III (DSN)314-430-5244; (COMM)49-0711-680-5244. The SCO or MC supervisor will request the following information:

(1) Identity of caller:
- Caller's name and phone number
- Where is caller calling from (organization)
- Where is caller calling from (city and state)
- What is the caller's DDN network address

(2) Details about the incident:
- When did the violation occur
- What happened
- How did the violation occur (if known)
- What damage was done
- What has the subscriber done about the violation
- What networks are they connected to
- What software is being used - Version
- How many subscribers are known to be affected
- How many subscribers are vulnerable (if known)
- Who else has been notified - names and phone numbers

- Does caller have any idea as to the identify of the intruder/violator

(3) Anything else the caller wishes to report

Once a suspected violation is reported and the above information collected, the PACIFIC and EUROPEAN OC's will immediately relay this information back to the DCAOC (WESTHEM/CONUS) for action.

b. Notification of the Defense Data Network Security Officer (NSO). The NSO will be contacted by the SCO or MC supervisor any time there is a reported network security problem. The NSO will authenticate the source of the report and will verify the reported information. Should the SCO or MC be unable to contact the NSO, the Headquarters, DCA MILNET or DSNET1 Manager, as appropriate, will be notified. Similarly, when an incident occurs on DISNET2 (WWMCCS) or DSNET3 (SCINET) and the NSO is not available, the WWMCCS ADP System Security Officer (WASSO) can be contacted via STU III at (DSN)312-227-2058 or (COMM)202-695-1944/0671; the SCINET Security Officer can be contacted via STU III at (COMM) 202-284-0846.

Points of Contact in DCA

DDN Network Security Officer (NSO)	(COMM) 202-692-7580/7581
MILNET Manager	(COMM) 202-692-7580/7581
DSNET1 Manager	(COMM) 202-692-7582-7583

c. Notification made by the NSO.

(1) Contact Management. The NSO will contact and periodically update appropriate DCA management on all security violations.

(2) Contact Investigation Agencies. The NSO will contact the FBI or appropriate Service investigative organization (AFOSI, NIS, ISC) if violation pertains to illegal activity.

(3) Contact Analysis Agencies. The NSO will contact the appropriate analysis agency and provide them a description of the problem and request immediate notification when a "fix" has been developed, tested, and independently verified. The following analysis agencies will be contacted:

(a) The Computer Emergency Reaction Team (CERT) provides support for VAX/SUN, UNIX, and VMS systems. These teams report security-related problems to vendors and assist in validating/verifying identified fixes.

(b) The National Security Agency (NSA) provides support for IBM and other non-UNIX and VMS systems. NSA works security-related problems through effected software vendors and assists in fix verification.

(4) Network Notification and Distribution. DCA provides distribution and coordination services through the Security Coordination Center (SCC). These services are limited to the MILNET only. The SCC identifies all subscribers who use the type(s) of hardware and/or software being affected, then notifies Host Administrators (HA's). Once the "fix" is identified, the SCC disseminates this information.

(5) Press Release. If the violation has the potential to be of high visibility (i.e., something that may appear in the press), the NSO will call the DCA Public Affairs Office to warn them about the event. The NSO will prepare the first draft press release if deemed necessary. The System Control Officer (SCO) and the MC Supervisor will not provide any information to the press, but will refer all calls to the NSO or the DCA Public Affairs Office.

7. Secure Subscriber Practices. The following subparagraphs are guidelines relating to secure subscriber practices. Implementation is optional but suggested.

a. Password Protection. Since use of the network is restricted, passwords, access codes, and TAC access cards should never be shared without express permission from the issuing authority. Users should follow these guidelines:

(1) Users should change their password regularly and at any time they feel their passwords may have been compromised. This includes passwords and access codes on local and remote hosts, as well as any other passwords the user encounters in network sessions. Users should contact their HA's to find out how to change passwords on their systems. Note that not all systems allow users to change passwords. Users who feel that their passwords have been compromised and cannot change them should contact their HA.

(2) Passwords should not be part of batch routines, macros, or comfiles. Users should have to type their password at each session.

(3) Users should report any unauthorized use of passwords and accounts to their HA.

(4) TAC access cards and records of host use identification and passwords should be kept in a secure place.

(5) Users should be familiar with and follow local security guidelines.

b. File Protection. Many operating systems have methods for protecting files from network read (copy) and write (save, change, delete) access. Users should set the default file protection for directories to "no read and no write to outside users." The users can still make files accessible to outside users over the network, but must knowingly set file and directory protection for this to happen. Users should consult with their host's system documentation or their HA for information about the default settings and how to change them.

c. Plagiarism. An unprotected file is not an invitation to copy or read it without first obtaining permission from the owner. It is as inappropriate to read on-line mail or peruse on-line files without permission as it would be to read colleagues' hardcopy mail or rummage around their desks.

(1) Electronic plagiarism is just as unethical as plagiarism by any other means. Users must observe and obey copyright laws.

(2) It is very easy and convenient to exchange programming code across the network. Most developers of such code are extremely generous in sharing their work. However, users should still obtain permission before copying or using someone else's code. Under no circumstances should programming code from anywhere on the network be used commercially (verbatim or edited) without the owner's explicit permission.

CHAPTER 4. NETWORK CONTROL

1. Objective. The objective of network control is to derive maximum usage from the DDN by making the most effective use of all available equipment and facilities.

2. Scope. Operational direction and control of the DDN is provided by the Defense Communications Agency Operations Center (DCAOC) and the Area Communications Operations Center (ACOC). Integral to each ACOC are network specific Monitoring Centers (MC's). The WESTHEM ACOC contains the CONUS MILNET, CONUS/European DSNET1, and Worldwide DSNET2 MC's. The European ACOC contains the European MILNET MC. The Pacific ACOC contains the Pacific MILNET and Pacific DSNET1 MC's. The DSNET3 MC is remoted within its Community of Interest (COI) and reports through the WESTHEM ACOC.

3. Monitoring Center Functions. Each MC performs five basic functions: (1) Network Monitoring; (2) Problem Resolution; (3) Data Base Configuration; (4) Installation, Test, and Acceptance; and (5) Network Status Administration. This section will briefly review each of these areas. A more detailed description of the operations and procedures of an MC will be contained in DCAC 310-P70-XX, Monitoring Center Operations.

a. Network Monitoring. In order to effectively control the networks, each MC must continuously monitor the network. Network Utilities (NU) is the software system employed to gather real time network information, which is displayed on the MC's netlog and lightbox. Figure 4-1, Monitoring Center Visibility, depicts the extent that MC's can monitor the network. In addition, each MC monitors projected outages through use of the Authorized Outage Log.

(1) The netlog displays real time event messages received by NU from the intelligent network entities (e.g., PSN's, TAC's, MTAC's, and MB's). Event messages consist of status, trap, and controller action messages. A status message is sent to NU when there is any change in the status of a PSN's IST connection, host interfaces, parameter values, or buffer counts. Trap messages are sent from PSN's, TAC's, and MTAC's to report on any unusual network behavior. NU generates controller action messages whenever NU control commands are used by the MC personnel. Information gathered from the event messages can be used to create additional displays and reports to suit the needs of Operations Management personnel. For example, there is a way of narrowing the scope of the netlog to focus on specified events (e.g., a specific kind of trap) or relating to specified network components (e.g., a specified PSN or IST).

(2) The lightbox gives the MC a graphic display of the status of network components. It can also include a textual listing of all components that are down.

(3) The Authorized Outage Log reflects all scheduled outages of backbone entities.

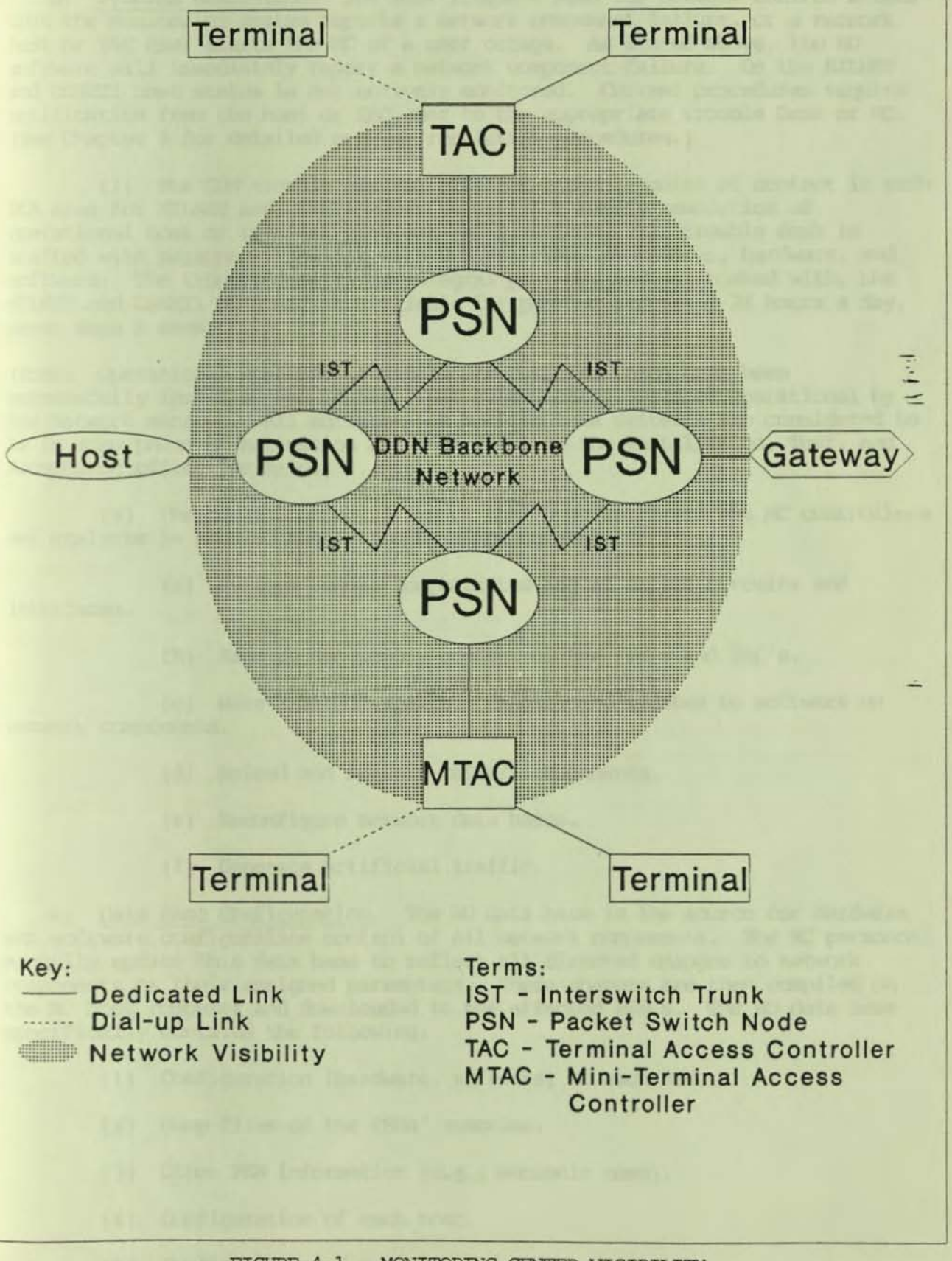


FIGURE 4-1. MONITORING CENTER VISIBILITY

b. Problem Resolution. The most frequent need for network control arises when the monitoring system reports a network component failure, or a network host or TAC user alerts the MC of a user outage. As stated above, the NU software will immediately report a network component failure. On the MILNET and DSNET1 host status is not actively monitored. Current procedures require notification from the host or TAC user to the appropriate Trouble Desk or MC. (See Chapter 9 for detailed problem resolution procedures.)

(1) The DDN trouble desk(s) provides a single point of contact in each DCA area for MILNET and DSNET1 users to call for timely resolution of operational host or terminal problems and questions. The trouble desk is staffed with personnel familiar with DDN policies, procedures, hardware, and software. The trouble desk is an integral part of, and collocated with, the MILNET and DSNET1 MC's and is available for problem reporting 24 hours a day, seven days a week.

(Note: Operational host and terminals are entities which have been successfully installed and tested, then subsequently declared operational by the network manager. All entities not meeting this criteria are considered to be in some phase of activation and must refer to the Installation, Test, and Acceptance office for help.)

(2) The control capabilities of the NU software aid the MC controllers and analysts in problem resolution by allowing them to:

(a) Perform remote loopback testing of access circuits and interfaces.

(b) Examine the memory content of the PSN's and TAC's.

(c) Make limited repairs, changes, and updates to software on network components.

(d) Reload and restart network components.

(e) Reconfigure network data bases.

(f) Generate artificial traffic.

c. Data Base Configuration. The NU data base is the source for hardware and software configuration control of all network components. The MC personnel manually update this data base to reflect all directed changes to network components or their assigned parameters. These changes are then compiled on the MC host computer and downloaded to the affected PSN's. The NU data base specifically contains the following:

(1) Configuration (hardware, software) of each PSN.

(2) Dump files of the PSNs' memories.

(3) Other PSN information (e.g., mnemonic name).

(4) Configuration of each host.

(5) Configuration of each IST.

(6) Description of each PSN's software type and version.

d. Installation, Test and Acceptance (IT&A). The purpose of IT&A is to ensure all new network components are correctly configured, connected, and tested. The MC controls all IT&A actions to ensure adverse impact to the operational network is minimized.

(1) Responsibilities and procedures for the conduct of network testing are contained in DCAC 370-P195-4, DDN Installation, Test, and Acceptance Procedures. Additionally, it sets standards for DDN acceptance testing. The acceptance tests to be performed depend upon the type of equipment and communications system being installed. Specific equipment and system test and acceptance checklists are included in the Circular. Acceptance testing is conducted for new site installations as well as operational sites being reconfigured.

(2) Follow-on Test and Evaluation (FOT&E) of the DDN is performed on a case-by-case basis to determine if previously identified deficiencies have been remedied, if any new deficiencies exist, and if performance has degraded.

e. Network Status Administration. NU is designed to collect and store real time information on network status, topology and throughput. This information is used to generate several periodic and special reports, used by DDN management to monitor and improve network efficiency, locate problem areas, and identify unfavorable trends.

(1) Status collection involves real-time tracking of which network components are up, down, or isolated. These conditions are reported in accordance with DCAC 310-55-1, Status Reporting for the DCS, and Chapter 8 of this Circular.

(2) The topology collection reflects the real time hardware and software configuration of the network components. The ultimate purpose of this collection is to detect discrepancies between the operational network and the NU data base. Advisories are generated whenever a discrepancy is detected.

(3) Optimal network design is highly dependent on the actual traffic distribution of the users. Also, in the DDN, neither the user population nor the network traffic distribution pattern remain constant. As a result, the traffic statistics collection and analysis capability is required for detection of trends, to permit adequate lead time, and to modify the network to accommodate changing patterns.

(a) The host-to-PSN and PSN-to-PSN traffic is recorded to determine host usage and to detect potential overloads. These figures are useful for deciding when and how the network topology should be changed, and for helping to isolate and resolve network problems.

(b) In addition to the usual traffic monitoring, there is occasionally the requirement for more extensive statistics and performance monitoring. This involves loading special software packages in the PSN that measure such things as host-host traffic or gather delay information. These measurements can also be used to determine the performance of specific network components, either as a design aid or as a means of fault isolation.

4. Continuity of Operations. The DCAOC Continuity of Operations Plan (COOP) provides the basic guide for contingency operations to be used if any of the MC's fail or has an extended outage. Each network component has a designated primary MC and one or more secondary MC(s). To ensure the secondary MC(s) have the full capabilities of monitoring and controlling the area(s) assumed during contingency, data base synchronization is necessary. Only the primary MC is allowed to edit its NU data base, but within minutes this change is automatically disseminated and the secondary MC's data bases are synchronized. Auxiliary files, such as the configuration files, are not automatically updated and are manually sent to the secondary MC's by the primary MC after a change is made. Since the data bases are synchronized, back-up to the secondary MC is achieved simply by administratively designating the new master MC. See Table 4-1 for the primary, secondary, and tertiary MC's.

5. Network Performance Parameters. Management Thresholds (MT's) and Performance Objectives (PO's) are established in DCAC 310-130-2, DCS Management Thresholds (MT) and Performance Objectives (PO). The MT's provide a level of measurement which, if not met, may require intensive management action by the responsible network manager. The PO's reflect the level of real performance that can be expected under optimum conditions. Network control uses the MT's and PO's as standards on which to base required actions.

6. Quality Assurance (QA). DCA Circular 310-70-57, DCS Quality Assurance Program, is being amended to include the DDN. Principal QA functions will include real-time and near real-time performance monitoring, data accumulation, quality control checks, problem tracking, and staff assistance. As shown in this chapter, many of these functions are already being accomplished through network control. Once fully developed, the DDN QA program will define the procedures to identify, evaluate, and maximize user service.

7. Network Configuration Management. Configuration management provides an orderly and accountable control over the network and its components as they exist and as they change. The DCA DCS Data System Directorate (DCSDS) (B600) has overall responsibility for all implementation activities worldwide. This includes ordering standard node hardware, configuration control of hardware and software, and tasking other elements of DCA and contractor support to install, test, and provide training on DDN equipment.

a. Network Engineering. Defense Communications Engineering Center (DCEC) assists the DCSDS by providing continual system engineering and technical support for operations throughout the life cycle of the DDN. Operational tasks include developing and enforcing testing requirements and procedures; engineering criteria and standards; and technical content of the deliverable data items.

TABLE 4-1. PRIMARY, ALTERNATE, AND TERTIARY MC'S FOR THE DDN SUBNETWORKS

SUBNETWORK	PRIMARY	ALTERNATE	TERTIARY
MILNET	CMMC, Arlington, VA	CMC, Cambridge, MA	PMMC, Wheeler AFB,HI EMMC, Vaihingen, GE
	EMMC, Vaihingen, GE	CMMC, Arlington, VA	PMMC, Wheeler AFB,HI
	PMMC, Wheeler AFB, HI	CMMC, Arlington, VA	EMMC, Vaihingen, GE
DSNET1	CDMC, Arlington, VA	PDMC, Wheeler AFB, HI	To be determined
	PDMC, Wheeler AFB, HI	CDMC, Arlington, VA	To be determined
DSNET2	WMC, Arlington, VA	AWMC, Ft. Ritchie, MD	OIMC, Reston, VA
DSNET3	SMC, Bolling AFB, DC	SSMC, ARLINGTON, VA	To be determined
ARPANET	AMC, Cambridge, MA	ANOC, Cambridge, MA	None

b. Hardware Installation. Installation changes to equipment that must be directed and coordinated by the DCSDS are:

(1) Installation and activation of node equipment.

(2) Installation and relocation of node equipment.

(3) Expansion or upgrading of existing node sites.

(4) Insuring all new or modified node installations conform with established DDN engineering standards.

c. DDN Circuit Routing Policy. The routing of DDN circuits presents complex issues which were compounded by the AT&T divestiture. Each case must be examined individually, however, there are two basic premises upon which routing policy can be based: (1) DDN circuits routed via DCS transmission facilities will be routed via corresponding DCS Technical Control Facilities (TCF's), and (2) Government TCF/Patch and Test Facilities (PTF's) should not be inserted in a circuit segment for which a single commercial carrier has end-to-end responsibility. In view of this, the following policies regarding the routing of DDN circuits apply:

(1) DDN circuits will be routed via Government TCF/PTF's when these facilities occur at the natural demarcation point between commercial carrier/Government or commercial carrier/commercial carrier responsibility.

(2) DDN circuits routed via Government-owned, on-base or in-house cable plants will be routed via the Government TCF/PTF when it is technically feasible, cost effective, and does not violate commercial tariffs.

(3) DDN circuits routed via Government TCF/PTF's will be configured to prevent inadvertent service interruption by either testing or patching, except at the direction of the appropriate network MC. Blocking plugs should be inserted in the line and equipment jacks to prevent inadvertent service interruptions.

(4) Unless specified in the TSR, the TSO issuing authority will route DDN circuits via DCS TCF/PTF's. If a DCS TCF/PTF is to be avoided, the rationale will be included in the TSR.

(5) Routing of circuits via local non-DCS TCF/PTF's will be negotiated on a case-by-case basis between DCA and the cognizant MILDEP representatives, normally during the site selection and survey process.

d. Network Changes. DDN Publication, DDN-P70-1, provides the procedures and delineates responsibility for making all operational changes to the DDN. Network changes are defined as software, hardware, circuit, or parameter changes to the operational networks. Formal procedures have been set up to accommodate network changes in a controlled and reasonable manner. These procedures are:

(1) Network Change Request (NCR). An E-Mail message, AUTODIN message, or letter issued by an activity to DCA (the appropriate network manager in DODM, e.g., MILNETMGR) is used to request a change to a backbone element. An NCR may be implemented by DODM, or forwarded to the appropriate DCA office for evaluation and recommendation.

(2) Subscriber Action Form (SAF). An E-Mail message, AUTODIN message, or letter issued by an activity to DCA (the appropriate network manager in DODM) is used to request a change to a host, terminal, or dedicated dial-up service. An SAF may be implemented by the network manager, or forwarded to the appropriate DCA office for evaluation and recommendation.

(2) Network Change Directive (NCD). An NCD is an E-Mail message issued by DCA (the appropriate network manager in DODM, e.g., MILNETMGR) to an MC and/or the NIC, to direct a required network change or to provide after-the-fact approval of an operational emergency change to the network.

(3) Network Change Action Notice (NCAN). An E-Mail message from the MC and/or the NIC. The NCAN is used to notify DCA (the appropriate DCA area network manager, e.g., MILNETMGR) that a direct change (referring to the NCD) has been completed. It is also used when an operational emergency change to the network, which is required to remain on a network element in excess of 48 hours, has been accomplished by the MC or NIC.

e. Configuration Control Group (CCG). The CCG is chaired by the DCSDS Technical Manager (DCA DDEP), or designated representative, and is responsible for reviewing and approving or disapproving new requirements and changes to the existing network hardware and software baselines. The CCG is also responsible for presenting and discussing security issues involving hardware, software, and procedures. The CCG monitors the Problem Reporting (PR) and Investigation Request (IR) process, monitors the disposition of the IR's and reserves the right to re-establish priorities or provide additional assessment, when required. The CCG membership consists of all the DCSDS Division Chiefs and the Deputy Program Manager for Logistics (Code B630).

CHAPTER 5. NETWORK MANAGEMENT

1. General. This chapter provides network management procedures for the DDN.

2. Points of Contact.

a. DDN Management and MC Points of Contact. These points of contact are contained in Table 5-1.

b. NSC and HA Points of Contact.

(1) The initial Point of Contact (POC) information is received by an NCD, and the data is entered for each individual POC into the NIC's WHOIS data base. This data base is updated on a daily basis. The host tables are then updated bi-weekly from the data base.

(2) Once a month, the NIC sends an E-Mail reminder to each NSC and HA that contains their name, electronic mailbox, postal address, phone number, and other pertinent data. The POC's are requested to verify the information and send any changes back to the NIC; correct data does not require a response. As responses are received the changes are entered into the WHOIS database.

(3) The NIC Host master sends monthly reports to each network manager that identify all database updates.

3. Message Distribution.

a. Electronic Mail (E-Mail).

(1) E-Mail is the information exchanged between individuals or organizations using the application of computer-to-computer data transfer technology, normally in the form of textual messages. It is widely used in the DDN environment for informal coordination, providing DDN operational direction, management control, configuration control, and as an informal means for integrating nodes and hosts into the DDN subnetworks. Additionally, it expedites these actions and reduces the administrative workload of formal correspondence preparation.

(2) E-Mail does not replace the formal record communications system, e.g., AUTODIN. Heads of organizations are not precluded from designating E-Mail as directive or formal in nature, however, E-Mail outside that chain of command will be considered informal information unless other prior arrangements are made between organizations.

(3) E-Mail service is provided by the sponsoring MILDEP/DoD Service. The sponsoring MILDEP/DoD also governs the access control and use of their E-Mail hosts.

TABLE 5-1. POINTS OF CONTACT

NAME/ADDRESS	COMM/AV	MAILBOX
ARMY		
US Army Information Systems Command/ATTN: AS-OPS-OI Fort Huachuca, AZ 85613-5000	602-538-8084 (DSN)879-8084	AS-OPS-OI@HUACHUCA-EMH.ARMY.MIL
NAVY		
Naval Telecommunications Command/ATTN: N51 4401 Massachusetts Avenue, NW Washington, DC 20390-5290	202-282-0381 (DSN)292-0381	NAVTELCOM@DDN-CONUS.DDN.MIL
AIR FORCE		
Air Force Communications Command/ATTN: DOOC Scott Air Force Base, IL 62225-6001	618-256-5422 (DSN)576-5422	AFDDN.OPS@GUNTER-ADAM.AF.MIL
MARINE CORPS		
United States Marine Corps ATTN: CCT Washington, DC 20380	202-694-3080 (DSN)224-3080	DDN-HQMC@DDN-CONUS.DDN.MIL
CONUS TROUBLE DESK (MILNET & DISNET)		
Trouble Desk Operator Defense Communications Agency ATTN: N211 Washington, DC 20305-2000	202-486-1982 (DSN)231-1787 800-451-7413 (EXCEPT INTL, ALASKA, WASHDC METRO)	
INSTALLATION TEST AND ACCEPTANCE (IT&A) DESK		
IT&A Operator Defense Communications Agency ATTN: N211 Washington, DC 20305-2000	202-746-2694/ 2695 (DSN)286-2694/2695 800-336-4862 (EXCEPT INTL, ALASKA, WASHDC METRO)	SERTH@CCT.BBN.COM
CONUS MILNET MC		
Controller on Duty Defense Communications Agency ATTN: N211 Washington, DC 20305-2000	202-692-2268/ 5726 (DSN)222-2268/5726	DCA-MMC@DCA-EMS.DCA.MIL

TABLE 5-1. POINTS OF CONTACT (con.)

EUROPEAN MILNET MC

Controller on Duty DCA European Area ATTN: E300 APO New York 09131-4103	CIV: 011-49-711-687-7766 011-49-680-5532/5534 ETS:430-5532/5534 MIL:2729-5532/5534 (DSN)314-430-5532/5534	STT-CONTROL@FRG.BBN.COM

PACIFIC MILNET MC

Controller on Duty DCA Pacific Area ATTN: P300 Wheeler AFB, HI 96854-5000	808-656-1472/ 1473/1474 808-624-3744 (DSN)315-456-1472/1473/1474	PMMC@DCA-PAC.DCA.MIL

SCINET MC (DSNET3)

Controller on Duty Defense Intelligence Agency ATTN: DSI-1D Washington, DC 20301-6111	202-373-4000 (DSN)243-4000	SMC-DIAC@DDN2.DCA.MIL

WINCS MC (DSNET2)

Controller on Duty Defense Communications Agency ATTN: N211 Washington, DC 20305-2000	202-692-2861 (DSN)222-2861	N211@DCA-EMS.DCA.MIL

CONUS DISNET MC (DSNET1)

Controller on Duty Defense Communications Agency ATTN: N211 Washington, DC 20305-2000	202-746-1849/ 1850 (DSN)851-3744	CDMC-DCAEMS@DCA-EMS.DCA.MIL

PACIFIC DISNET MC (DSNET1)

Controller on Duty DCA Pacific Area ATTN: P300 Wheeler AFB, HI 96854-5000	808-656-1472/ 1473/1474 808-624-3744 (DSN)315-456-1472/1473/1474	PDMC@DCA-PAC.DCA.MIL

TABLE 5-1. POINTS OF CONTACT (con.)

NETWORK INFORMATION CENTER		
DDN Network Information Center SRI International 333 Ravenswood Avenue Room EJ291 Menlo Park, CA 94025	800-235-3155 415-859-3695	NIC@NIC.DDN.MIL
DEFENSE DATA NETWORK MANAGERS		
MILNET	202-692-7580 (DSN)222-7580	MILNETMGR@DDN-CONUS.DDN.MIL
SCINET	202-692-7581 (DSN)222-7581	SCINETMGR@DDN-CONUS.DDN.MIL
WINCS	202-692-7581 (DSN)222-7581	WINCSMGR@DDN-CONUS.DDN.MIL
DISNET	202-692-7582 (DSN)222-7582	DISNETMGR@DDN-CONUS.DDN.MIL
EURMILNET	49-711-680-7222 (DSN)314-430-7222	EURMILMGR@DDN-EUR.DDN.MIL
EURDISMGR	49-711-680-7192	
PACMILNET	808-656-1124 (DSN)315-456-1124	PACMILMG@DDN-PAC.DDN.MIL
PACDISNET	808-656-1124 (DSN)315-456-1124	PACDISMG@DDN-PAC.DDN.MIL
DCA HEADQUARTERS		
DATA SYSTEMS MANAGEMENT DIVISION (DDO)	703-285-5226 (DSN)356-5226	DCADDO@IMO-UVAX.DCA.MIL
DATA OPERATIONS MANAGEMENT BRANCH (DDOM)	202-692-7582 (DSN)222-7582	DCADDOM@IMO-UVAX.DCA.MIL
DATA OPERATIONS SUPPORT BRANCH (DDOS)	703-285-5225 (DSN)356-5225	DCADDOS@IMO-UVAX.DCA.MIL

TABLE 5-1. POINTS OF CONTACT (con.)

EUROPEAN AREA		
DATA NETWORKS MANAGEMENT DIVISION (DED)	49-711-680-5703 (DSN)314-430-5703	E600@DCA-EUR.DCA.MIL
DATA NETWORKS MANAGEMENT BRANCH (DEDS)	49-711-680-7222 (DSN)314-430-7222	E610@DCA-EUR.DCA.MIL
PACIFIC AREA		
DCS DATA NETWORKS DIVISION (DPD)	808-656-1124 (DSN)315-456-1124	P600@DCA-PAC.DCA.MIL
DATA OPERATIONS BRANCH (DPDO)	808-656-1124 (DSN)315-456-1124	P650@DCA-PAC.DCA.MIL

b. General Messages.

(1) General Messages will be issued by Headquarters, DCA, DCA European Area, DCA Pacific Area, or the DCAOC to provide DCA-approved policy, standard procedures, instructions, guidance, and information for management control and operational direction of the appropriate DDN subnetwork. These messages are directive upon activities operating or deriving service from the DDN. The following general messages have been established:

General Messages	Routing Indicator	Cognizant Authority
ALLDISNETSTA	RUCRDNT	Hq DCA DDOM
ALLWINSTA	RUCRWIN	Hq DCA DDOM
CONUSMILNETSTA	RUCRMNC	Hq DCA DDOM
EURMILNETSTA	RUCRMNE	DCA-EUR E610
PACDISNETSTA	RUCRDNP	DCA-PAC P650
PACMILNETSTA	RUCRMNP	DCA-PAC P650

(2) General messages will be sequentially numbered by year; e.g., ALLWINSTA 01/83 or 02/83. General messages will remain in effect until cancelled by the message originator or cognizant authority for that general message series. The first message of each year will list all effective subnetwork general messages and include a recapitulation of the addressees and associated routing indicators. Node sites will maintain a complete file of all effective general messages for their respective subnetworks.

(3) General messages are distributed to addressees via AUTODIN by use of a collective routing indicator (CRI) to the collective address designator (CAD). Addressees of the CAD may include the JCS, Military Services, Unified and Specified Commands and their component commands, the operations and maintenance activities supporting each node site and their higher headquarters, and DCA areas.

(4) Changes to the addressee listing are distributed by message as modifications to the CAD; e.g., Modification 01/83 and 02/83. This is not to be confused with the general message sequential numbering system. Addressees should inform their serving telecommunications center/terminal to ensure appropriate CAD/CRI file distribution updates.

(5) Internal distribution will be accomplished by Telecommunications Centers to ensure that the office of primary responsibility and/or interest is aware of DDN procedures and policies. Of specific importance is the telecommunications operations office, patch and test or technical control facility, crypto facility, and Node Site Coordinator.

(6) DCAC 210-70-2, provides the policy and procedures, and delineates responsibility for the preparation and use of DCA general messages.

c. DDN Management Bulletins. DDN Management Bulletins are issued on-line by the NIC to a distribution list. These bulletins provide information on management, policy, and procedures related to operation of the DDN. Policy directives are also addressed in AUTODIN messages. NSC's and HA's that have an

E-Mail mailbox are automatically included as an addressee on bulletins, others can be added by sending a request to NIC@NIC.DDN.MIL.

d. DDN Newsletters. DDN Newsletters are issued on-line by the NIC to a distribution list. Newsletters provide general network news items that are of interest to network users. NSC's and HA's that have an E-Mail mailbox are automatically included as an addressee on newsletters, others can be added by sending a request to NIC@NIC.DDN.MIL.

4. DDN Publications. The documents referenced in this circular may be useful, depending upon the user's requirements.

5. Training.

a. DDN Course. This course provides the DDN user community with sufficient technical and program information to enable the users to obtain effective data communications service through the DDN and to meet DoD interoperability requirements.

(1) Video Tapes. Requisition procedures for DDN Course video tapes are as follows:

(a) Request the video tapes, which are identified by Product Identification Numbers (PIN) 505174 through 505177, directly from the local audio-visual center. The local audio-visual center will provide the necessary paperwork and funding.

(b) To fill out the forms, the requester will have to specify, in addition to the above PIN's, the tape titles, format(s) (VHS, Beta, and/or 3/4 inch), the respective quantities, and, of course, the shipping destination

(c) Tape titles by SAVPIN:

PIN	Title
505174	Section I - "Functional Requirements for Data Communications"
505175	Section II - "Computer Network Architectures"
505176	Section III - "The Defense Data Network and the DDN Protocol Suite"
505177	Section IV - "The DDN: Strategies for Subscribers".

(2) The printed document is available from the Defense Technical Information Center (DTIC). Identification of the document is a accession Number ADA 173472.

b. Node Site Coordinator. A video-tape and workbook are provided to each node site.

(1) The video-tape entitled, "The Node Site Coordinator-A Critical Role," provides an introduction to the DDN, an overview of the NSC's role, a typical transaction between an NSC and the MC and reviews node site equipment and its functions.

(2) The Node Site Coordinator's Workbook is to be used in conjunction with the video-tape. The workbook goes into more detail on the subjects covered in the video-tape.

c. Commercial Courses. Commercial courses are available. Contact DCA (Code B630) for course description, schedules and funding. Also, this information is published periodically in a DDN Newsletter.

6. Billing. The costs of developing, acquiring, implementing, operating, and maintaining the DDN are being shared among the Military Departments, the DCA, and other DoD agencies. Network operating and maintenance costs are funded through the Communications Services Industrial Fund (CSIF) and recovered through monthly billing of the Military Departments and DoD agencies based upon preestablished rates. These rates are currently based upon a pro-rata share of the network costs without regard to user population. However, a capability is under development enabling the collection of network usage data, connect time, and packet count as a basis for future allocation of cost recovery among the Military Departments and DoD agencies.

7. Logistics.

a. Logistic Support Plan (LSP). DCAC 270-P120-3, Logistic Support Plan for the DDN, provides logistical support information, instructions, guidance, and direction to DoD elements and other Government agencies concerned with command, operation, or support of the DDN. The United States Air Force (USAF), through the Sacramento Air Logistics Center (SM-ALC), has been designated as the Life Cycle Manager (LCM) for the life of the DDN. Supply support includes:

(1) Repair Parts. The DDN contractor provides contractor-owned repair parts and spares for on-site and off-site maintenance and repair. Storage of these repair parts and spares is the contractor's responsibility.

(2) Supply Accountability. The DDN contractor is responsible for maintaining records of repair parts and spares usage and for updating the Government's records of deployed equipment when maintenance changes the end item serial number and barcode date.

b. Preventive Maintenance. Periodically, the contractor provides the Government a written schedule stating the frequency and duration of the preventive maintenance required for each kind of equipment at the node sites and MC's. The Government specifies the schedule for the performance of the preventive maintenance. This schedule may require modification as needs arise or emergency situations occur. Scheduled preventive maintenance will be coordinated in advance with the appropriate network MC and NCS is normally performed on Monday through Friday, excluding holidays. Preventive maintenance may be performed on the same call for which corrective maintenance is requested, provided there is no additional charge associated with the preventive maintenance. Preventive maintenance may also be defined as on-call installation maintenance support, in the event of system expansion or deletion to ensure continual operation. Equipment preventive maintenance procedures are performed as follows:

(1) C/70. quarterly, 2-hour downtime.

(2) C/70, annual, 3-hour downtime.

(3) C/3 series, quarterly, 1/2-hour in-service.

(4) C/3 series, annual, 2-hour downtime.

c. On-call Corrective Maintenance. The DCA policy regarding maintenance response times for operational entities of the Defense Data Network is based on the existing DDN Hardware Maintenance Contract. Those times vary somewhat based on the "mission essentiality" of the subscriber community and has some constraints applied due to remote geographical locations. Cost is also a major factor. The existing response time requirements are:

(1) DSNET2 - Twenty-four hours for the entities located in Okinawa, Guam and the Philippines. Twelve hours for London, UK; Norfolk, VA; Langley AFB, VA; MacDill AFB, FL; Offutt AFB, NE; Atlanta, GA, Korea, and Japan. Two hours for all remaining sites.

(2) MILNET, DSNET1, and DSNET3 - Twenty-four hours for Guam, the Philippines, Okinawa, Turkey, Greece, Spain, and Alaska. Two hours for Oahu. Twelve hours for all other existing locations.

(3) ARPANET - Twelve hours all sites.

d. COMSEC Support. Support of DDN COMSEC material is provided through the relationship defined in a memorandum of agreement (MOA) between HQ USAF, the DCA DDN, and the Air Force Cryptographic Support Center (AFCSC). The MOA dated 3 April 1985 identifies the policies, responsibilities and procedures of the DCA and the USAF necessary to support COMSEC material requirements with a timely, systematic and organized implementation procedure for the DDN program. COMSEC material includes KG-84A encryption devices and associated manuals. Maintenance of COMSEC equipment is a Service or Agency responsibility, the same as any other COMSEC equipment.

(1) For issuing and shipment, DCA sends a message to the Air Force Cryptologic Support Center (AFCSC), Kelly Air Force Base, Texas; National Security Agency (NSA), Fort Meade, Maryland; and the COMSEC Account Custodians/Air Force Unit Commanders for the PSN end points of the circuit. This message includes the following actions: requests AFCSC to ship the KG-84A to the COMSEC Account Custodians/Air Force Unit Commanders responsible for supporting the PSN's at the end points of the circuit (note: KG's are shipped to the Army and Navy accounts by AFCSC per the DCA message, Air Force units must send an AF Form 601 to AFCSC to have KG's shipped); requests NSA to provide initial distribution of keying material to the COMSEC Account Custodians/Air Force Unit Commanders of the PSN end points of the circuit; provides the COMSEC Account Custodians/Air Force Unit Commanders of the PSN end points of the circuit with information as to which end point is the controlling authority of the keying material; and provides the strapping and switch settings for the KG-84A's. Subsequent keying/rekeying and resupply is a Service or Agency responsibility.

(2) To ensure users are not denied service due to excessive outages attributable to the performance of cryptographic key changes (crypto resets) it is necessary to schedule these resets. For MILNET and DSNET1, the Controlling Authority of the cryptographic key schedules the times with the distant-end and advises DCAOC, DCA-Europe, or DCA-Pacific, as appropriate. If there is a conflict in the scheduling of the crypto resets, DCAOC, DCA-Europe, or DCA-Pacific will resolve the issue and advise both PSN end points of the circuit. The DCAOC schedules the times for DSNET2. The Defense Intelligence Agency provides procedures for crypto resets for the DSNET3. It should be noted that cryptographic key resets are currently the main reason for IST outages.

(3) After PSN-PSN coordination, both sites will reset using the new key, check in-house back-to-back, and then place the crypto back on-line. Procedures for crypto reset are published by NSA and supplemented by the Services. For sites that may not be manned on a 24-hour, 7-days-a-week basis or other questions regarding crypto resets, check with your COMSEC Account Custodian for the procedures to be followed.

(a) If either site fails to see the other come on-line and synchronize within 10 minutes, they will contact the MC and coordinate a reset and/or correct the problem.

(b) No site will take more than one circuit out of service at a time for a crypto reset.

(c) It should be noted that crypto resets are one of the biggest contributors to downtimes for the DDN.

e. Availability of DDN Telecommunications Service Request (TSR) Numbers.

(1) DDN users, NSC's, major vendors, and local telephone companies have been experiencing coordination problems during installation or repair of equipment and circuits. This problem concerns vendors not having the TSR number with them when arriving on site.

(2) The DCSDS and DECCO have implemented a procedure to have the TSR number included on the vendors' work orders. The procedure adds certain elements of the TSR number into Item 131 of the TSR. An example using TSR DU15DEC860768 follows:

131A. Commander U.S. Army Information System Commands, ATTN: ASNA-HOP-PP, Bldg 13, Room 136, Ft Hood, TX 76544 (DU860768).

The above example shows the Telecommunications Certification Office (TCO), Fiscal Year and TSR number in parenthesis following the ZIP Code, e.g., (DU860768). The TSR Item 131A is normally on all TELCO work orders and as such, the abbreviated TSR number will also be reflected in the work order.

8. Survivability. The DDN system is a highly distributed network with adequate built-in features to ensure that it will survive the Joint Chiefs of Staff postulated threats at least commensurate with the headquarters, agencies, and activities it supports. Three network features enable the DDN to continue providing service even when it is partially damaged:

a. Site Hardening. Much of the DDN equipment is located on the same premises as the user equipment that it supports. Therefore, it is likely to survive as long as the subscriber equipment survives. DDN equipment is made survivable in three ways.

(1) If appropriate, it has High-Altitude Electro-Magnetic Pulse (HEMP) protection in the form of electro-magnetic shielding, line isolation circuits, and surge arresting components.

(2) Where necessary, uninterruptable power supplies are also provided so operation can continue during transient power failures.

(3) DDN circuit routing is selected for geographic dispersion and to avoid common facilities.

b. Redundancy. The backbone network is a dense trunking grid with many alternate routes, and critical users are dual-homed to ensure their access to the network. At critical sites the PSN's are installed with full backup capabilities. In addition, critical circuits are redundantly configured so a single failure does not isolate a node.

(1) Dual-homed Users. Critical users can be dual-homed to the network, and a dense trunking grid (backbone lines interconnecting the PSN's) will provide redundancy at all possible points in the network.

(2) On-call Circuits. On-call (H route) circuits have been established for certain PSN-to-PSN IST's to provide a minimum of uninterrupted service to the DDN, when the primary (A route) circuit fails or is degraded for an extended period of time.

(a) On-call circuits will be tested at least once every three months. Testing will normally be scheduled when minimum communications impact will occur to users of the network. The purpose of these tests is two-fold: (1) to ensure the circuit is capable of providing the desired service in a timely manner; and (2) to familiarize personnel with procedures for activation of an on-call circuit.

(b) The Circuit Control Office (CCO) of each on-call circuit is responsible for scheduling tests. The CCO will coordinate with the MC who will evaluate the network status and, based on this information, either approve or disapprove the test. Upon completion of the test, the CCO will report the results to DCA (DDO) and DCAOC (DOCOO), applicable Service Telecommunications Commands, and DCA-Europe (DEDS) and/or DCA-Pacific (DPDO), as appropriate.

(c) The DCAOC or ACOC will maintain a list of on-call circuits and the date and time each circuit has been tested. Further, the DCAOC or ACOC will maintain a Standing Operating Procedure (SOP) for each on-call circuit that provides information relative to the procedures, notifications, and other unique information necessary for activation of the circuit.

c. Dynamic Routing. The DDN adjusts itself to damage without disrupting service to surviving users. The distributed routing functions enable the PSN's to cooperate in automatically routing traffic around congested, damaged, or destroyed PSN's or IST's. The PSN routing algorithm also allows for the automatic update of their tables as new topologies are added. This high degree of adaptability, coupled with automatic monitoring of the PSN's, IST's, and access lines, enables the network to degrade gracefully when transmission paths, PSN's, or MC's are inoperative. The precedence and preemption handling capabilities of the network enable it to allocate the surviving network resources among critical subscribers.

CHAPTER 6. NETWORK INFORMATION CENTER

1. General. This chapter addresses the services the NIC provides. The Network Information Center (NIC) provides network registration, TAC access control, network auditing, and general reference services for the DDN. Databases and information servers containing pertinent network information are accessible on-line on a real-time basis for users.

2. Network Registration.

a. Each host on the DDN has a unique host name and 32-bit network address associated with it. The network address identifies the DDN subnetwork to which the host is connected, the host port number on the PSN, and the number of the PSN to which the host is connected. For example, network address 26.3.0.45 indicates the subnetwork MILNET, and port number 3 on PSN 45. The NIC registers the following information:

(1) Domains

(2) IP networks (names, numbers)

(3) Hosts (names, nicknames, network addresses, CPU types, operating systems, and protocols for MILNET, ARPANET, and internet hosts)

(4) Gateways (names, nicknames, network addresses, CPU types, operating systems, and protocols for MILNET, ARPANET, and internet hosts)

(5) Autonomous System Numbers used in the EGP protocol routing tables.

b. TAC access requires official authorization, and a unique user identification (UID) and access code (password).

(1) The person authorizing TAC access is the HA. HA's register all new users by completing a registration template for each user, then forwarding it to the NIC network mailbox (REGISTRAR @ NIC.DDN.MIL). (The template, plus instructions, are obtained either via FTP from the SRI-NIC host (26.0.0.73) using the pathname <USER-DRIVE>INSTRUCTIONS.TXT; via E-Mail (NIC.DDN.MIL); or via telephone query to the NIC. The HA's will continuously monitor the status of each user, and make changes as required.

(2) The NIC issues each authorized user a card identifying the user's unique UID and access code. These cards are automatically printed and sent in sealed mailers, so they are seen only by the specified users. (User cards are reissued annually as authorized by the HA.)

(3) If the user only requires TAC access for a limited time, the HA can issue a "guest card" which is good for a maximum of three months (these cards are reissued quarterly if the HA has requested them.)

(4) Authorization to use TAC's on one subnetwork does not provide access to TAC's on other subnetworks.

c. The WHOIS data base stores all DDN user registration information, MILNET TAC Access Card issuance and invalidation (HOTLIST) data, DDN host, TAC, gateway, network domain, and PSN data. The WHOIS database is the source of the individual and host information displayed to DDN users via the WHOIS/NICNAME server. (See paragraph 5a for use of the WHOIS/NICNAME server.)

3. TAC Access Control System (TACACS). To restrict network access for users connecting to the MILNET through a TAC, the TAC Access Control System (TACACS) has been implemented. TACACS uses the UID and access code to authenticate users and permit them access to the DDN.

a. After a successful TACACS log on, a terminal may communicate with any host in the community to which the terminal has been assigned. However, each host must also use a protection mechanism (e.g., an identifier and password log on) to authenticate the user's identity. Thus, a TAC user typically encounters two log-on requests, one at the TAC, which authorizes entry into the network, and a second at the destination host, which authorizes entry into the host.

b. The NIC maintains a database of the MILNET TAC UID's that have been hotlisted in order to transmit HOTLIST updates to the appropriate MC's. The HOTLIST is composed of the UID's of users who no longer have a need for network service, compromised UID's, and expired TACACS guest cards. Hotlisted users cannot access the network through a TAC.

4. Network Auditing. The NIC operates and maintains the Network Audit-Trail and Usage Reporting System (NAURS), specifically auditing MILNET.

a. The TAC Access Audit-Trail Analyzer (ATA) subsystem is the auditing and reporting facility of the (TACACS). The ATA receives audit-trail data from each TAC and records the UID (excluding the access code), the TAC network address and terminal port number, the destination host address, the number of bytes passed through the network, and the approximate date and time of the session into the data base. MILNET TACACS automatically generates incident reports when certain unusual events occur. These reports are reviewed by the DDN Network Security Officer for indications of illegal or unauthorized network access attempts. TAC's used on the classified subnetworks have not yet implemented an audit trail and analysis capability.

b. The Usage Data Collection and Processing subsystem (UDCP) collects, stores, and analyzes information received from the NADRS and the WHOIS database. The data collected in the UDCP database is the source of the monthly DDN Usage Summary Report, which supports the DDN billing program.

c. The NIC provides network audit trail reports to DCA on a periodic and on-demand basis. The reports are classified into three types: recurring reports, incident reports, and special reports. These reports are not available for common use and can only be obtained by approval of DCA.

(1) Recurring reports. The recurring reports are generated on a monthly basis.

(a) Number of Logins by Port. This report provide histograms of the distribution of TAC logins over all active ports on each TAC.

(b) Number of Individual Users by Port. This report provides histograms of the distribution of the name of unique individuals using any given TAC port over all active TAC ports.

(c) Average Login Time by Port. This report provides histograms of the distribution of the average of the connect times per port for all users of that port over all ports on each TAC.

(d) Percentage of Time in Use During Prime Time by Port. This report provides histograms which show the percentage of the actual use of each port during time over the total available prime time (i.e., 9:00 a.m. to 5:00 p.m. on weekdays, local time).

(e) Connect Time Summary. This report summarizes the connect times associated with each TAC by listing the total number of users, the total connect time of all of these users, and the average connection time per user.

(f) User Activity Report. This report summarizes the connection times of each individual user to all TAC ports that individual has used. It provides the user identification, the authorizing host, the total connection time for all TAC use by that individual during the month, the average connection, and the average daily connection time.

(2) Incident Reports. The incident reports are triggered by certain patterns of TAC usage. These reports are forwarded electronically to DCA for further examination. The NIC develops three reports as defined below:

(a) Multiple Login Reports - Type 1. This report is automatically generated whenever seven or more simultaneous logins occur with the same UID. The location of the TAC where the login occurs is also recorded, although the emphasis is on the number of logins, since that number of simultaneous logins probably indicates that the user is sharing the UID and password.

(b) Multiple Login Report - Type 2. This report is automatically generated whenever two or more simultaneous logins occur with the same UID, and the location of the TAC's from which the logins originate are geographically distinct.

(c) Multiple Login Report - Type 3. This report is automatically generated whenever a user accumulates a connection time exceeding 16 hours.

(3) Special Reports. Special reports are customized reports to investigate specific activities or events, and consequently are generated only upon request by DCA. Typical of these special reports are: an analysis of activities by individuals per port; a listing of the login activities of TAC's which are accessible by "800" telephone numbers; and a listing of all failed login attempts at one particular TAC.

5. General Reference Services. The NIC provides general reference services to DDN users via E-Mail, U.S. mail, and telephone. Examples of on-line services include WHOIS/NICNAME, NIC/QUERY, TACNEWS, and SERVICE.

a. WHOIS/NICNAME. WHOIS/NICNAME is a NIC program that provides information from a data base of network users. This database serves as an electronic "white pages." The information retrieved includes the user's name, handle (the unique string of characters in parentheses following the name in the database), network mailbox, U.S. mail address, telephone number, and AUTODIN address, if available. WHOIS/NICNAME provides the most up-to-date information available.

(1) Information can be retrieved via a WHOIS/NICNAME search when the user knows the individual's last name, partial name, full name, handle , directory name, or system program name.

(2) A listing of all the registered users on a particular host can be obtained by using the WHOIS/NICNAME command with the host name preceded by an asterisk (*). The response from the NIC will repeat the information for a host search, and will list the total number of individual members and their names, handles, username@hostname, and phone number.

(3) WHOIS/NICNAME responds to a query in one of three ways:

(a) If a single record matches the name given for the desired individual or organization, or if the NIC handle matches an existing record, the name, NIC handle, organization, U.S. mailing address, and network mailbox are displayed on the user's terminal.

(b) If several records match the name given, a brief list of the matching entries is displayed and the user is asked to choose the correct match by using the handle. A search by handle will produce the expanded entry for the individual or organization, as in paragraph (a) above.

(c) If no record matches the name or handle query, WHOIS/NICNAME will display the message "NO match for [user's name]" where [user's name] represents the name of the individual or organization being requested.

(4) Getting Help. The user can get help with the WHOIS/NICNAME system by typing the following command at the system prompt: whois help (return).

b. NIC/Query. NIC/Query is a browsing system containing general information about the DDN. Each list of topics included under the NIC/Query is presented to the user as a numbered menu. To access NIC/Query, the user must open a TELNET connection to the SRI-NIC host (host address = 26.0.0.73) and invoke NIC/Query by typing "nic" at the prompt. Topics available in Query include WHOIS, DDN HOSTS, PROTOCOLS, RFC's, and NETWORK DOCUMENTS.

c. TACNEWS. TACNEWS is a NIC on-line service that offers logon help to TAC users. It provides a mechanism for reading the DDN Newsletters and DDN Management Bulletins. Users should read these publications regularly to stay current on DDN policies, announcements, and network news items. Users can also have newsletters and management bulletins regularly delivered on-line to their network mailbox, by sending a request to NIC@NIC.DDN.MIL. The request should indicate that the user would like to be on the on-line distribution list and contain the user's name and address. TACNEWS can also be used to find the telephone number of the nearest TAC when the user provides the area code and prefix of his calling location.

d. User Assistance Service. The NIC provides user assistance services to DDN users via telephone, U.S. mail, and E-Mail.

(1) Telephone. Telephone service is available Monday through Friday, 7 am to 5 pm, Pacific time.

Toll-free: 800-235-3155
International: 415-859-3695

(2) U.S. Postal Address. Send U.S. postal mail correspondence to:

DDN Network Information Center
SRI International, Room EJ291
333 Ravenwood Avenue
Menlo Park, CA 94025

(3) Online mailboxes: To contact the NIC via E-Mail 24 hours a day, seven days a week, use these mailboxes:

NIC@NIC.DDN.MIL - General user assistance, document requests
REGISTRAR@NIC.DDN.MIL - User registration and WHOIS updates
HOSTMASTER@NIC.DDN.MIL - Host, domain, network changes and updates
ACTION@NIC.DDN.MIL - NIC computer operations
SUGGESTIONS@NIC.DDN.MIL - Comments on NIC publications and services
SERVICE@NIC.DDN.MIL - (see below)

e. SERVICE. Service is an automated document and information delivery service based on an electronic mail document retrieval mechanism. It provides some of the NIC services to DDN users who do not have access to the TELNET or FTP programs. It allows access to NIC documents and information via ordinary electronic mail. To use the mail service, send a mail message to SERVICE@NIC.DDN.MIL. In the SUBJECT field, request the type of service you wish followed by any needed arguments. The message body is normally ignored. The information you request wil be sent back to you as soon as possible.

Large files will be broken into parts and sent to the requestor in separate messages. Example subject lines:

```
WHOIS HOST NIC.DDN.MIL
NETINFO DOMAIN-TEMPLATE.TXT
SEND FRC INDEX
SEND RFC:ASSIGNED-NUMBERS.TXT
WHOIS LOTTOR, MARK
```

f. Domains. The Hostmaster at the NIC registers top-level and second-level domains. The NIC also administers several top level domains (including .MIL). For help or information about domain questions, contact Hostmaster@NIC.DDN.MIL.

g. Useful On-Line References. Several public files on the SRI-NIC host are useful to network users. The pathnames for some of the available titles are listed below. A complete listing of available files is found in NETINFO:INDEX.TXT. These files may be retrieved via FTP, using USERNAME = "anonymous," PASSWORD = "guess".

(1) NETINFO:MIL-NSC.TXT. Lists the NSC's for each PSN on the MILNET.

(2) NETINFO:MIL-HOST-ADMINISTRATORS-A-L.TXT. Lists the HA, alphabetically, for each MILNET host starting with the letter A through the letter L.

(3) NETINFO:MIL-HOST-ADMINISTRATORS-M-Z.TXT. Lists the HA, alphabetically, for each MILNET host starting with the letter M through the letter Z.

(4) NETINFO:HOSTS.TXT. This file contains the Official DoD Internet Host Table. It lists the names and network numbers of the different networks; and the names, network addresses, CPU types, operating systems, protocols of hosts, gateways, and TACS on the DoD Internet. It is designed to be machine-readable, whereas the previous lists are meant to be more user-friendly.

(5) NETINFO:DOMAIN.TXT. Lists all the top-level domains and their server machines.

(6) NETINFO:TAC-LOCATION.TXT. This file gives the geographic location for each TAC. It is very useful for locating the TAC closest to the user.

(7) NETINFO:TAC-PHONES.LIST. Lists the telephone numbers needed to dial up MILNET TAC's in the U.S.

(8) NETINFO:EUR-PAC-PHONE.LIST. Lists the telephone numbers needed to dial up MILNET TAC's outside the U.S.

(9) RFC:RFCnnn.TXT. Network technical notes, also known as Request for Comments (RFC's), are on-line in the directory RFC on the SRI-NIC host. New RFC's are announced to network users via an on-line distribution list maintained by the NIC. Individuals wishing to be added to the RFC notification list should send a message to NIC@NIC.DDN.MIL. In the title of this paragraph, "nnn" represents the RFC number.

(10) RFC:RFC-INDEX.TXT. Lists all RFC's in reverse numerical order. This index also includes: author, title, date of issue, number of pages, number of bytes, and information about which RFC's have been superseded or obsoleted.

(11) NETINFO:NIC-PUBS.TXT. An annotated list of NIC distributed documentation.

CHAPTER 7. OUTAGE PROCEDURES

1. General. This chapter provides a detailed overview of the procedures and reporting requirements for all DCS DDN outages. It applies only to DDN entities which have been declared operational by the applicable network manager.

2. Scheduled Service Interruptions. DCAC 310-70-1, Volume II, establishes the policy and procedures for scheduling DCS service interruptions. For DDN, all PSN interruptions are scheduled according to DCAC 310-70-1, Volume II, Chapter 4, paragraph 2c, Interruption of User Service (other than complete DCS station). All other DDN facilities are scheduled as directed in Chapter 4, paragraph 2h, Interruption of User Service (DCS Tail Station). DDN specific exceptions to DCAC 310-70-1, Volume II, Chapter 4 are contained in Chapter 8, paragraph 2r of that circular.

3. Unscheduled Service Interruptions. The following procedures will be followed to ensure priorities are established, resolutions are acted upon, documentation is accomplished, and the appropriate organizations are informed of all unscheduled outages and network deficiencies on MILNET and DSNET1, DSNET2, and DSNET3 unscheduled service interruptions are addressed. The resolution of an operational network problem basically goes through five phases: detection, categorization, resolution, review, and feedback. (See Figure 7-1, Problem Resolution Flow Chart.)

a. Problem Detection. The detection and reporting of a MILNET or DSNET1 related problem to the respective MC or associated MC Trouble Desk are the first steps in correcting an unscheduled service interruption. When reporting a problem, a trouble ticket or Problem Report (PR) number will be assigned to reference the outage during follow-up actions. In addition, a formal Problem Report (PR) will be initiated. (See Figure 7-2, Problem Report Format.)

(1) User Actions.

(a) Host subscribers should contact their respective HA to ensure the host is not experiencing problems. MTAC terminal, TAC terminal, MTAC dial-up, and TAC dial-up users should contact the applicable NSC to confirm that the MTAC, TAC, or PSN is not causing the problem. (In order for users to obtain the best possible results when reporting problems, the supporting organization should ensure the HA and NSC names and phone numbers are kept current in the Network Information Center (NIC) WHOIS data base.)

(b) HA's, MTAC terminal, and TAC terminal users should initially confirm the status of their access circuit from their equipment to the PSN, TAC, or MTAC to include the access circuit modems. This access circuit confirmation action should be accomplished through the local communications maintenance unit, Technical Control Facility (TCF), Circuit Control Office (CCO), or Communications Management Office (CMO), as prescribed in local instructions, in order to shorten lead time for access circuit restoration. MTAC and TAC dial-up users should contact the appropriate MC or associated Trouble Desk to confirm the status of the dial-up line.

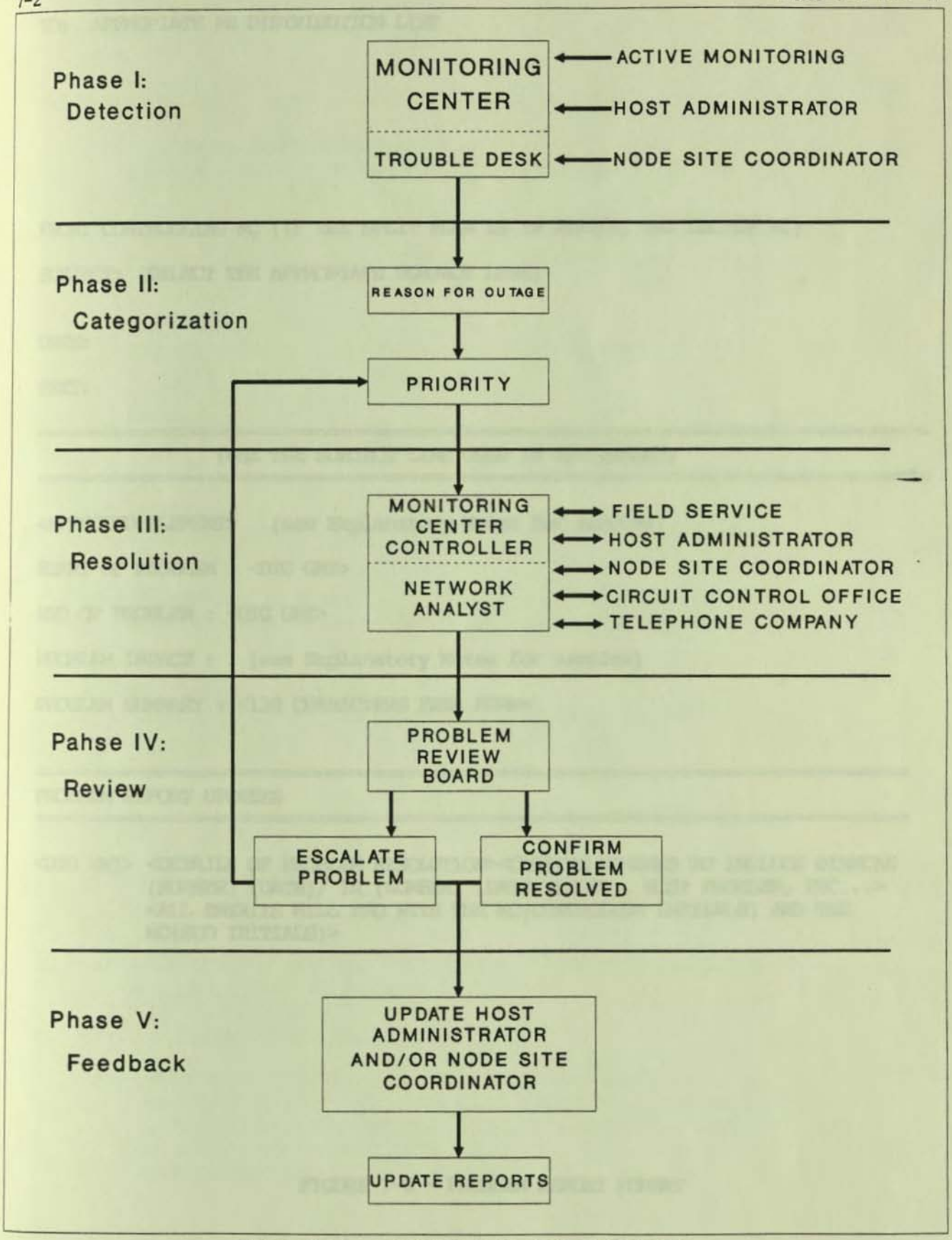


FIGURE 7-1. PROBLEM TRACKING FLOWCHART

TO: APPROPIATE PR DISTRIBUTION LIST

FROM: CONTROLLING MC (IF THE SPLIT PLAN IS IN EFFECT, THE BACKUP MC)

SUBJECT: (SELECT THE APPROPIATE SUBJECT LINE)

DATE:

TEXT:

(USE THE SUBJECT LINE USED IN THE HEADER)

<AFFECTED ELEMENT> (see Explanatory Notes for samples)

START OF PROBLEM : <DTG GMT>

END OF PROBLEM : <DTG GMT>

PROBLEM IMPACT : (see Explanatory Notes for samples)

PROBLEM SUMMARY : <138 CHARACTERS FREE FORM>

PROBLEM REPORT UPDATES

<DTG GMT> <DETAILS OF PROBLEM RESOLUTION><CLOSING REMARKS TO INCLUDE DISNCAN (NUMBER) (DATE)/ IR (NUMBER) (DATE ISSUED), HOST PROBLEM, ETC...> <ALL ENTRIES WILL END WITH THE MC(CONTROLLER INITIALS) AND THE MC(SCO INITIALS)>

FIGURE 7-2 - PROBLEM REPORT FORMAT

EXPLANATORY NOTES FOR FIGURE 7-2

Subject lines will comply with the following formats:

```
HOST/MC/EMH/MAILBRIDGE PROBLEMS:
    SUBJECT : PRX-Y : ZZ7-YYYYY : ?? : XX.XX.0.YYY-O&M TYPE :
              1   2   3   4      5    6          7

TAC TERMINAL (TAC-T) OR TAC DIAL-UP (TAC-D) PROBLEMS:
    SUBJECT : PRX-Y : ZZ7-YYYYY : ?? : TAC-(T/D)-O&M TYPE :
              1   2   3   4      5    6         7

PSN PROBLEMS:
    SUBJECT : PRX-Y : ZZ7-YYYYY : ?? : PSNXXX-O&M TYPE :
              1   2   3   4      5    6      7

TAC PROBLEMS:
    SUBJECT : PRX-Y : ZZ7-YYYYY : ?? : TACXXX-O&M TYPE :
              1   2   3   4      5    6      7

IST PROBLEMS:
    SUBJECT : PRX-Y : ZZ7-YYYYY : ?? : LNXXX--PSN-O&M-PSN-O&M :
              1   2   3   4      5    6       7a 7b  7c  7d

SYSTEM SOFTWARE PROBLEMS:
    SUBJECT : PRX-Y : ZZ7-YYYYY : SW : BRIEF DESCRIPTION :
              1   2   3   4      5    6

SYSTEM OPERATING PROBLEMS:
    SUBJECT : PRX-Y : ZZ7-YYYYY : OP : BRIEF DESCRIPTION :
              1   2   3   4      5    6
```

Key to Subject line terms:

1. PRX- : PR3, PR2, PR1

2. Y : O=OPEN, U=UPDATE, C=CLOSE

3. ZZ7 : ZZ=MILNET: MC:CONUS, ME:EUROPE, MP:PACIFIC, MX:BACKUP MC
   7 = YEAR (87=7, 88=8, 89=9, ETC...)

4. YYYYY : THE PR NUMBER FIVE DIGIT

5. ?? : HW = BBN MAINTAINED HARDWARE: C30, TAC, ECU's, etc.
   PW = SITE RELATED PROBLEMS: BASE POWER, AC, OTHER ENVIRONMENTAL
   LN = LINE PROBLEMS: MODEMS, FACILITY RELATED, CIRCIUT PATH, etc.
   SW = SOFTWARE RELATED PROBLEMS
   OP = OPERATIONAL RELATED PROBLEMS

EXPLANATORY NOTES FOR FIGURE 7-2 (continued)

6/7. MC/HOST/EMH/MAILBRIDGE: XX.XX.0.YYY—<O&M OF THE MC/HOST/EMH/MAILBRIDGE>
TAC USER: TAC-T—<THE O&M OF THE TERMINAL>
TAC-D—<THE O&M OF THE DIALUP>
PSN : PSNXXX—<THE O&M SPONSOR OF THE PSN>
TAC : TACXXX—<THE O&M SPONSOR OF THE TAC>
IST : LNXXX—<ENDPOINT PSN#,(HIGHER NUMBER)>—<O&M OF PSN>—
<ENDPOINT PSN#,(LOWER NUMBER)>—<O&M OF PSN>
SW : <SOFTWARE TYPE & VERSION>
OP : <12 CHARACTER - ONE WORD DESCRIPTION, E.G., PROCEDURES,
CONGESTION, ROUTING ETC...>

NOTE: O&M = THE SPONSORING MILDEP/DOD AGENCY FOR THAT ENTITY.
(USN, USA, USAF, DARPA, DMA, USMC, DNA, DOE)
XXX = THE NETWORK ASSIGNED NUMBER WHICH COULD BE UP TO 3 DIGITS.

Affected Element lines will comply with the following formats:

HOST/EMH/MAILBRIDGE PROBLEMS:
HOST NAME : <HOST,EMH,MC,MAILBRIDGE NAME>

TAC TERMINAL <TAC-T> OR TAC DIAL-UP <TAC-D> PROBLEMS:
TAC USER : <TAC NAME>

MC PROBLEMS:
<MC NAME : FACID : ENR CODE>

PSN PROBLEMS:
PSN : <PSN NAME : FACID : ENR CODE>

TAC PROBLEMS:
TAC : <TAC NAME : FACID : ENR CODE>

IST PROBLEMS:
LNXXX : <PSN#, PSN NAME TO PSN#, PSN NAME : CCSD>
<CKT ID# WILL BE USED IF CCSD IS NOT AVAILABLE>

SYSTEM SOFTWARE PROBLEMS:
DEFICIENCY : <SOFTWARE TYPE & VERSION>

SYSTEM OPERATING PROBLEMS:
DEFICIENCY : <ONE WORD DESCRIPTION OF OPERATIONAL PROBLEM, E.G.
TRAFFIC, PROCEDURES, ETC...>

EXPLANATORY NOTES FOR FIGURE 7-2 (continued)

Problem Impact lines will comply with the following formats:

```
MC/HOST/EMH/MAILBRIDGE PROBLEMS:
    <NETWORK AREA/SYSTEM AFFECTED>

TAC TERMINAL (TAC-T) OR TAC DIAL-UP (TAC-D) PROBLEMS:
    PORT<XX> DENIED SERVICE

PSN PROBLEMS:
    PSN : HOST(S) DENIED SERVICE :<XX>
          TAC PORT(S) DENIED SERVICE :<XX>
    ISOLATED PSN(S) : <PSN NAMES>
          HOST(S) DENIED SERVICE :<XX>
          TAC PORT(S) DENIED SERVICE :<XX>

TAC PROBLEMS:
    TAC PORT(S) DENIED SERVICE :<XX>

IST PROBLEMS:
    ISOLATED PSN(S) : <PSN NAMES>
          HOST(S) DENIED SERVICE :<XX>
          TAC PORT(S) DENIED SERVICE :<XX>

SYSTEM SOFTWARE PROBLEMS:
    SYSTEM(S) AFFECTED : <40 CHARACTER DESCRIPTION>

SYSTEM OPERATING PROBLEMS:
    SYSTEM(S) AFFECTED : <40 CHARACTER DESCRIPTION>
```

(c) When the host or TAC terminal equipment, and the associated access circuit are confirmed as operational by the local communications maintenance unit, a call should be made to the appropriate MC or associated Trouble Desk. Problems should be reported by the HA or host operator in order to begin immediate troubleshooting, but may be accomplished by the local communications maintenance unit on their behalf. As an initial step, the MC will conduct a remote loopback test to the host modem to verify the status of the access circuit. If the remote test is unsuccessful, the caller will be asked to recontact the appropriate CCO or CMO for resolution. If the remote loop is successful and the problem persists, the problem will be logged in, assigned a unique PR number, and additional fault isolation will be accomplished by the MC controller and/or analyst.

(2) Node Site Coordinator (NSC) Actions. The NSC does what the title implies: coordinates between the MC or Trouble Desk and the users. Each coordinator should report directly to the responsible MC or Trouble Desk any known PSN, MTAC, TAC, IST, or MB problems.

(3) MC Actions.

(a) The MC controllers monitor and control the subnetworks via the MC equipment. The controllers actively monitor and immediately react to all PSN, TAC, MTAC, MB, or IST outages. While user host "down" status is also reported by the PSN's, outages are processed and reacted to differently for each subnetwork. In the case of DSNET2 and DSNET3, the user hosts belong to a community of interest (COI) that is actively monitored by the respective COI operations centers in close coordination with the subnetwork MC. The MC controller or Trouble Desk operator works with the COI operations center to restore access area service.

(b) On MILNET and DSNET1, the MC's and MB's are the only hosts which are actively monitored. All other hosts are passively monitored because the HA's have complete discretion in taking their system out of service. User host outages and TAC user problems on these subnetworks are strictly determined by user notification. Once a user (host or TAC terminal) problem has been reported to the MC or the Trouble Desk, a PR number is assigned and the problem is entered into the problem resolution and feedback cycle for resolution.

b. Problem Categorization. Each problem will be categorized by Reason for Outage (RFO) code and priority level to further discern actions required for resolution. The definitions of RFO codes and priorities contained in this section will be used as a guide, with specific application being subnetwork unique.

(1) Reason for Outage (RFO) Codes.

(a) Currently, PR's use unique two position DDN RFO codes to identify the source of the outage. The codes are:

HW - DCA maintained hardware.
PW - Site environmental or power problems.
LW - Circuit, modem, circuit path problems.

SW - DCA maintained software.
OP - Operational or procedural deficiencies.
CR - Encryption.
HE - Host specific.

(b) Within the next two years, the RFO codes specified by DCAC 310-55-1, Status Reporting for the DCS, will replace the DDN unique codes. These RFO codes will be used to report the location and description of the outage.

1. An System Software Deficiency (SSD) is a deficiency which can be, with reasonable assurance, attributed to software, and in most cases can be created. An SSD also includes software which is not performing in accordance with current DDN specifications. The RFO cause or symptom code for software (S) will be the first position of the RFO code for SSD's. The RFO outage location code will identify the location of the software fault. If network wide, the location code for the DCAOC MC will be used.

2. An System Operating Deficiency (SOD) is a design deficiency which causes operating difficulties, e.g., topology. The RFO cause or symptom code for Human Error/Procedural Error (H) will be the first position code for SOD's. The RFO outage location code will identify the appropriate DOCC MC required to take action; for example, a rehome of an IST will identify the MC of the controlling theater DOCC element.

(c) A deficiency or error in DDN documentation is reported as a System Documentation Deficiency (SDD). In cases that involve DDN operations circulars, manuals, or procedures, an SDD is sent to the specified OPR, with information copies to HQ DCA Codes DODS, DDCI, and DOCCO (AUTODIN address: DCA WASHINGTON DC//DODS/DDCI/DOCCO//; E-Mail: B652@DDN1.DCA.MIL, B642@DDN.DCA.MIL, N211@DCA-EMS.DCA.MIL.

(2) Priority Levels. The following Priority levels are internal levels of reaction within the controlling theater DOCC element and are designed to give the associated MC general guidelines for deploying resources to solve operational problems. There are three levels of reaction based on the following criteria: (1) backbone or user elements, (2) seriousness of problem impact, and (3) amount of time elapsed in the problem duration.

(a) Priority One (PR-1). A priority one (PR-1) problem has met threshold criteria or has been escalated from a priority two (PR-2) level. It is a problem that warrants continual MC action, periodic Headquarters DCA review, and O&M sponsor awareness. Within PR-1 ranking and deployment of resources, the MC supervisor must consider whether the problem is backbone or user related, the operational impact, and the duration of the outage.

1. Host, MTAC, or TAC User. The outage exceeds 72 consecutive hours. A PR will be sent out at the 72 hour point and updated every 48 hours thereafter, or as significant developments occur. The MC Supervisor will determine if a development is considered significant. The MC controller will attempt a phone update to the user at least every 48 hours. The sponsoring O&M agency will be included on the opening, update, and closing PR messages. A summary of all open PR-1 user problems will be

appended to the Problem Review Board (PRB) minutes. Any PR-1's closed since the last PRB will also be addressed. (PRB defined in paragraph 3d(1).)

2. PSN, TAC, MTAC, IST, MB, or MC. The outage exceeds 12 consecutive hours, or there are five unscheduled outages of 10 minutes or more in one raday. All O&M's will be included on the opening, update, and closing PR messages. An E-Mail update will be released at a minimum of every 24 hours after opening, or as significant developments occur. The MC Supervisor will determine if a development is significant.

3. System Software or Operating Deficiency. An SSD is a problem that seriously impacts backbone software. An SOD is a problem that either denies or significantly degrades service to a widespread portion of the network (e.g., a multi-node congestion outage) or a problem which seriously impacts network operations. In the case of a multi-PSN congestion or outage, the appropriate network manager and ACOC staff must be alerted by phone contact immediately. The controlling CONUS MC will also be alerted to the problem and take immediate action to notify the appropriate DOCC element and network manager. If overlapping regions are affected, the DCAOC and appropriate network manager will be the controlling authority until resolved. A PR-1 report must be generated and sent by the controlling MC as soon as possible. An update will be issued every 24 hours after opening, or as significant developments occur. The DDN Investigation Request (IR) Manager will determine the validity and initiate corrective action on all SSD's. Specifically, the DDN IR Manager will either identify the SSD as not being a backbone software problem or categorize the SSD and open an IR.

(b) Priority Two (PR-2). A PR-2 problem has met threshold criteria to be escalated from the priority three (PR-3) level. It is a problem that warrants increasing MC action and initial Headquarters DCA awareness.

1. Host, MTAC, or TAC User. The outage exceeds 24 hours but is not over 72 hours. The MC will update the user as necessary but at a minimum of every 24 hours via phone. The MC will append all open PR-2 user problems to the PRB minutes. All PR-2's closed since the last PRB will also be addressed.

2. PSN, MTAC, TAC, IST, MB, or MC. The outage exceeds 4 hours but is not over 12 hours; or, if in the same raday there are four outages of 10 minutes or more, then the problem will be escalated to PR-2. A closing PR will be sent via E-Mail to the appropriate distribution list.

3. System Software or Operating Deficiency. A significant software or operating deficiency causing sporadic outages and degradation of service. If overlapping regions are affected, the DCAOC and respective HQ DCA Network Manager will be the controlling authority. E-Mail distribution will be made upon initiation of a SSD or SOD PR-2 using the format of an IR recommendation (see paragraph 5, Chapter 9). The DCSDS IR Manager will determine the validity and initiate corrective action on all SSD's. Specifically, the DCA IR Manager will have 96 hours to either identify the SSD as not being a problem or categorize the SSD and open an IR. In either case, all SSD PR's will be automatically closed at 96 hours, if not closed sooner. SOD's will be escalated or closed by the appropriate DDN Manager. No time restraint applies to SOD PR's.

(c) Priority Three (PR-3). A PR-3 problem has met initial reporting criteria and warrants initiating MC action and review. This level of concern remains at the MC level.

1. Host, MTAC, or TAC User. The outage is from the time of initial notification up to 24 hours. The PR will be logged in and given a unique PR number for referencing. The only documentation will be internal MC management logs and reports. Once resolved, these problems will be closed out with the entity's point of contact.

2. PSN, MTAC, TAC, IST, MB, or MC. The outage exceeds 10 minutes but is less than 4 hours. The outage will be reported and closed out via the Daily Outage Report. All backbone outages over 10 minutes will be assigned a PR number.

3. System Software or Operating Deficiency. Any software or operating problem that is minor in nature but whose correction will increase the operating efficiency of any element of DDN, will be opened as a PR-3. These problems will be area and/or subnetwork unique, and will not be governed by Government regulation or contract. If a problem affects more than one-area or is regulated by existing documentation, the problem will be-opened, at a minimum, as a PR-2 and controlled by the DCAOC and appropriate DCA DDN network manager. E-Mail distribution will be made upon initiation of a SSD or SOD PR-3. The DDN Software and IR Manager(s) will determine the validity and initiate corrective action on all SSD's. The network manager will determine the validity of all SOD's and take corrective action as necessary. As stated above, any SOD's requiring changes to current directives, policy, or network-wide procedures will be escalated to at least a PR-2 and resolved by the network manager.

c. Problem Resolution. All actions taken by the MC to restore or improve service are considered steps to problem resolution. The controllers will take immediate action to restore all known DDN related problems, in order of their receipt, by priority. Technical support personnel will be called in as needed to assist in resolution. Updating, tracking, and reporting the problem is an integral part of this action.

(1) Host, MTAC, or TAC User. If the DDN related problem is suspected to be trouble with the user access line, the MC will notify the applicable TELCO, DCA field service, or on-base agency to initiate corrective action. However, these telecommunications repair crews may need the assistance of the NSC or HA once on-site. The MC will maintain frequent contact with the user to gain additional information to solve the problem or to update the user with any significant changes in status. The MC will verify that the user is satisfied prior to closing out the problem. It will be incumbent upon the HA to apprise their connected users.

(2) PSN, TAC, MTAC, IST, MB, or MC. The MC will work directly with the prime contractor technical staff, TELCO, Government staff, and the NSC to resolve backbone problems. The resolution can be as simple as a software command to a given PSN or as complex as a dual dispatch of TELCO and prime contractor personnel, in coordination with the NSC.

(3) System Software or Operating Deficiency. These types of deficiencies may be transparent to the user, or the user may, as a result, be suffering frustrating problems of delay, error messages, or lack of connectivity. For SSD's, the prime contractor software experts will work with the DCA software managers to find the most suitable solution.

(4) NSC Assistance. Proper operation of the network requires NSC assistance be available to aid personnel in diagnosing and fixing problems related to nodes and IST's. Many outages are extended due to site assistance not being available in a timely manner, notably at night and on weekends and holidays. Likewise, field service personnel are sometimes denied access to the site. Also, site assistance is also required to assist the MC to restart equipment or loop the host and modem interfaces. Site access availability is required at all times for field service personnel; prior visit notification will be provided.

(a) Reloading a PSN. There are three methods for reloading a PSN: from a cassette, from a neighbor PSN, or from the NU. The choice of method depends on the circumstances in which the MC Controller finds the PSN and the network. The first method, loading from cassette, will be used only for the C/30 at the DCAOC or ACOC. The second method, reloading from a neighbor, will be used for the majority of the PSN's. The third method, loading from the NU, will be used when circumstances dictate that the master copy of the program be loaded directly into a PSN (e.g., for security reasons or for propagation of a special PSN version).

1. When the C/30 PSN to which the C/70 is homed fails, it cannot be reloaded from a neighbor PSN. In this event, reload will be accomplished using the cassette. The operational and backup C/30 PSN should each have an "IMPLOD" tape in their respective cassette readers at all times.

2. The backup PSN should be in its loader (passive standby with lights 6 and 2 illuminated) at all times. This can be accomplished only by having the "IMPLOD" tape in the tape reader.

3. The PSN "SYSLOAD" tape will not be used unless directed by the DCAOC. The NSC is responsible for the security and accessibility of the "SYSLOAD" tape.

4. NSC assistance will be required to place the proper tapes in the tape reader and aid in troubleshooting if problems arise during reloading.

(b) PSN Dumps. PSN memory dumps can be caused automatically by preset conditions within the program or be forced by operator command at the MC. These dump cassettes are important tools, used to analyze failures and sophisticated network problems. The following procedures will assist the NSC in processing a dump.

1. Ensure that a blank cassette tape with the write tabs enabled (the tabs located opposite to the cassette tape head should be closed over the holes to enable the write function on the cassette tapes) is mounted on the right hand cassette drive unit.

2. When a valid dump has been accomplished, the MC controller will notify the NSC to remove that dump cassette tape from the right hand drive unit.

3. The MC Controller will give the NSC a dump control number that the NSC will write onto the cassette dump tape that was removed. The operator will also add the Zulu time and date to this label.

4. The NSC will then mount another blank tape with a write enabled onto the right hand cassette drive unit from which the dump tape was removed.

5. The NSC will fill out a PR for the dump cassette, including the dump control number, Zulu time and date.

6. The cassette dump and PR will then be processed according to local site procedures and sent to DCA, ATTN: DOD, Washington, DC 20305-2000.

d. Problem Review. A DDN problem will be reviewed by the appropriate DDN PRB(s) for disposition (e.g., resolved, needing escalation, or requiring further investigation at the current priority level). Chronic or network-wide problems may be recommended to be opened as Investigation Reports (IR's). All other unresolved problems will continue to cycle through problem categorization, restoration, and review until formally closed.

(1) Problem Review Board (PRB). The PRB is chaired by the appropriate DDN network manager or assigned DCAOC/ACOC staff representative. The agenda and schedule are set by the chairperson. The PRB reviews all PR-1 reportsto ensure timely and correct resolution, and to determine if further action is required to preclude recurrence.

(a) Mandatory and Optional Members. The mandatory members of the PRB consist of, at a minimum, a DCAOC/ACOC representative, the appropriate DDN network manager, the MC manager, and the PR Administrator. dDesignated alternates may fill in, but the meeting must be chaired by a Government operations representative. Optional members may include: the DDN software manager, the DDN IR manager, statistical analyst(s), telecommunications contractors, field service representatives, network operations analyst(s), software support specialists (firefighters), and Service and Agency representatives.

(b) PRB Conduct of Business. The PR Administrator will distribute the agenda to the PRB members no later than 2 working days prior to the up-coming meeting. The time and method of delivery for the agenda is at the discretion of the PRB chairperson. As part of old business, the PRB will review all problems left unresolved from the last meeting. All problems occurring since the last PRB will then be discussed as part of the new business. The PRB chairperson will attempt to develop a consensus on the disposition of each problem. If a consensus is not possible, the PRB chairperson will determine what action(s) will be taken. All user nonconcurrence or escalation requests will be considered prior to making final disposition. The PRB minutes will reflect the board's decisions.

(c) PRB Tasking Authority. The PRB chairperson will have final authority to direct or request action be taken by the servicing and supporting contractors or Government organizations. This authority will comply with contractual and Government restraints. The PRB chairperson may also request escalation to, and opening of, an IR.

(d) PRB Minutes. The minutes are the after action report of the PRB, detailing the disposition of each problem discussed. Each entry will include the problem identification number, the date problem reporting was opened and closed, and a summary narrative of the problem, it's resolution, and any subsequent actions as determined by the PRB. The minutes will be distributed within 2 working days of the PRB meeting and will include the time and place of the next meeting.

(2) Problem Escalation.

(a) Circuit Restoration Priorities.

1. The National Communications System (NCS) Circuit Restoration Priority System applies to communications circuits of Federal Government departments and agencies, to include DCS circuits. The RP system is designed to identify the order in which order circuits should be restored in the event of a failure.

2. The RP's assigned to DDN circuits are based on the criteria established in NCS Memorandum Number 1-68, NCS Circuit Restoration Priority System, and DoD Directive C-4605.2, Restoration Priorities for Military Communications Channels.

3. The procedures for requesting assignment of an RP for a circuit and obtaining the necessary NCS certification are outlined in DCAC 310-130-1, Submission of Telecommunications Service Requests. The request for RP assignment is an integral part of the Telecommunications Service Request (TSR) for the circuit.

4. RP's are considered during problem resolution. Escalation to a higher MC priority corresponds directly with the assigned RP.

(b) High Interest Telecommunications (HIT) and Special Interest (SI) Items.

1. Critical circuits and facilities are identified in the DCAOC HIT and SI lists to ensure proper functioning of the network. These lists are developed and issued by the respective area DOCC elements.

2. The MC examines the HIT and SI lists upon initial identification of a network problem. Immediate escalation to a PR-1 is standard procedure for these entities.

(3) Problem Close Out. There are several ways a problem may be closed out. These are detailed below.

(a) MC Action. The MC will close the PR when the problem is resolved. All recommended closures will be reviewed and concurred with by the PRB. Any closures not receiving PRB concurrence will be reopened under the old PR number. The MC will close out the problem with the affected user or network entity and the appropriate TELCO, Field Service, or NSC.

(b) Discretionary Software Deployment. The MC may field a software patch to solve an immediate operational problem only if the problem has been reported as a PR-1 and a request for the opening of an IR-1 or IR-2 is sent to the DCSDS IR manager. The deployment will be documented in a discretionary network change action notice (DISNCAN) within 72 hours of deployment and must gain DCA approval within 96 hours to remain deployed on the subnetwork or network. Failure of the network manager to approve the patch by Network Change Directive (NCD) will result in immediate removal of the patch by the MC. A verbal extension may be given to the MC for the continued use of the patch, but an NCD must be issued to make the patch a permanent change. The MC must send an amended DISNCAN if the patch is removed.

(c) Opening of an IR. The IR procedures contained in Chapter 9, describe the MC and DCA requirements in initiating the IR process. Once an IR is opened, the PR will be closed cross-referencing the IR reporting number for follow-on action.

(d) DCAOC/ACOC/Network Manager Action. At any time the appropriate area network manager, in consultation with DCAOC/ACOC staff, may direct the close out of a PR. The DCAOC/ACOC staff representative, who has been delegated the PRB chairperson responsibility, may also act to close out a premature or incorrect PR. If such an action has been taken, then the final entry on the PR will detail who ordered the close out and the justification for this action.

e. Problem Feedback. All closing actions will be coordinated with the affected user(s) to verify problem resolution. Formal reporting will be on-going and is reviewed in paragraph 4, below.

4. Service Interruption Reporting. The following reports will be required for DDN outages:

a. Outages Reporting. All DDN backbone outages, either scheduled or unscheduled, are reported in accordance with DCAC 310-55-1. In addition, all MILNET and DSNET1 unscheduled outages will be documented in a Daily Outage Report, compiled and transmitted via E-Mail by the appropriate MC.

(1) The format with explanatory notes for the Daily Outage Report is shown in Figure 7-3.

(2) All DDN backbone entities will be reported on if they are identified as SI or HIT entities and reporting is deemed necessary by the appropriate DOCC element and respective theater network manager.

b. Problem Reporting. Each operational problems which is identified by or to the MC or Trouble Desk, is logged with a unique identification number and documented according to the procedures outlined in paragraph 3 of this chapter. The PR format is shown in Figure 7-2.

```
Subject:  <Theater-Network> Daily Outage Report for <day-month-year>

NOTE:     Line and Node outages of less than ten (10) minutes and Line outages
          that are the result of Node outages are not displayed, but are
          nevertheless counted in the statistical summaries (MTFB, MTTR, etc.)
          at the end of each section.

------ Lines ------

Line  <device>  (<name>),  <class>, serial #  <CCSD>:
  <day-month-year>^^<down time>^<up time>^^<duration>^^^<reason>
      $$<RFO>/RMKS<narrative>$$
_____________________________________________
=============================================

Summary:
  downs <total times down>, percent down <hours down/machine hours>
  MTBF <time>, MTTR <time>
  machine hours <number lines x 24 hours>, hours down <total down time>

------ Nodes ------

Node  <device>  (<name>),  <class>, serial #  <FACID>:
  <day-month-year>^^<down time>^<up time>^^^<duration>^^^<reason>
      $$<RFO>/RMKS<narrative>$$
_____________________________________________
=============================================

Summary:
  downs <total times down>, percent down <hours down/machine hours>
  MTBF <time>, MTTR <time>
  machine hours <number lines x 24 hours>, hours down <total down time>

------ TAC's ------

TAC  <device>  (<name>),  <class>, serial #  <FACID>:
  <day-month-year>^^<down time>^<up time>^^^<duration>^^^<reason>
      $$<RFO>/RMKS<narrative>$$
_____________________________________________
=============================================

Summary:
  downs <total times down>, percent down <hours down/machine hours>
  MTBF <time>, MTTR <time>
  machine hours <number lines x 24 hours>, hours down <total down time>
```

FIGURE 7-3. DDN DAILY OUTAGE REPORT FORMAT

```
——— MC's ———

MC  (<name>),  <class>, serial #  <FACID>:
  <day-month-year>^^<down time>^<up time>^^^<duration>^^^<reason>
      $$<RFO>/RMKS<narrative>$$
_____________________________________________
=============================================

Summary:
  downs <total times down>, percent down <hours down/machine hours>
  MTBF <time>, MTTR <time>
  machine hours <number lines x 24 hours>, hours down <total down time>

=============================================
Note:  REASON FOR OUTAGE (RFO) CODES TAKEN FROM DCAC 310-55-1.
=============================================

End of <Theater-Network> Daily Outage Report for <day-month-year>
.<end of report>
```

FIGURE 7-3. DDN DAILY OUTAGE REPORT FORMAT (continued)

KEY TO TERMS IN FIGURE 7-3

<device>	=	line, node, or TAC number: "1" for line 1, "39" for node 39, "7" for TAC 7.
<name>	=	For a line, enter the Facility ID (FACID) codes for the termination/end points, e.g., M05-M65. For a node and TAC, use the geographic location. For an MC, give the name of the MC.
<class>	=	For a line, indicate line speed. For a node, TAC or MC, enter the type of equipment (e.g., C/30,LSI11, C/70).
<CCSD>	=	For a line, enter the complete 8-digit CCSD assigned to the line. For lines that do not have an assigned CCSD, use the format LINE*###. (where * = network, e.g., MILNET; ### = Line number). For example, LINEM018.
<FACID>	=	FACID for the node, TAC, MC.
<date>	=	9 character field of the form dd-mmm-yy; for example: 15-Jan-87.
<down time>	=	Time in form hh:mm; for example: 12:30.
<up time>	=	Time in the form hh:mm.
<duration>	=	In hours, of the form hh:mm.
<reason>	=	One of the following reasons: CableCut, CarrierProblem, ClearedSelf, ClearedTest, Environment, FacilityProblem, Isolation, H-Testing, Hardware, MicrowaveFading, ModemProblem, NodeDown, Operations, PM, PowerFail, Repairs, ReleasedToTELCO, Retrofit, S-Hardware, S-Software, S-Testing, SitePower, Software, SystemReloc, Unknown, and Version Change.
$$	=	Denotes start of the Reason For Outage (RFO) code and remarks.
<RFO>	=	Enter the 4-digit RFO code that reports the location and description of the outage. (See DCA Circular 310-55-1, Chapter 3).
<RMKS>	=	Unclassified clarifying narrative. (69 characters per line, unlimited number of lines.)
$$	=	End of 55-1 idication.

c. Leased Circuit Outage Reporting. DCAC 350-135-1, Defense Commercial Communications Acquisition Procedures, Chapter 8, provides procedures for processing and submitting DD Form 1368 (Modified Use of Leased Communications Facilities). DCAC 350-135-1 procedures are modified as follows:

(1) The responsible MC will submit a DD Form 1368 to DECCO to document interruptions of more than 30 minutes of service on the commercially leased IST's.

(2) The MC located in the same geographic area as the CCO or CMO, will submit a DD Form 1368 to document extended (minimum of 2 hours) or frequent interruptions to leased host or terminal access circuit service. The appropriate network manager will determine which user access circuits will be reported. By 1 October 1989, all access circuit management responsibilities, to include reporting interruptions of leased service, will transfer to the O&M Service Organizations and DoD Agencies.

d. Communications Status and Spot (COMSTAT & COMSPOT) Reporting. The purpose of the COMSTAT and COMSPOT reports are to provide the Joint Chiefs of Staff, Unified and Specified commands, the Services, and other addressees, with essential information on the global communications situation within the DCS. COMSTAT reports are required in accordance with DCA Instruction (DCAI) 310-85-1.

(1) COMSPOT reports are required on MILNET and DSNET1 failures that meet the established reporting criteria. The appropriate ACOC MC's are responsible for providing the information required by DCAI 310-85-1.

(2) COMSPOT reports are not required for failures on DSNET2 or DSNET3, however, the controlling MC is required to provide the same information to the DCAOC Systems Control Officer (SCO) as soon as a failure meets the COMSTAT criteria.

(3) COMSTAT reports are required on MILNET, DSNET1, DSNET2, and DSNET3 failures that meet the established reporting criteria.

(4) The DCAOC, ACOC Europe, and ACOC Pacific are responsible for preparation and submission of COMSTAT and COMSPOT reports for their respective areas of responsibility.

e. Classified Reporting. For those problems that are considered to contain classified information, reporting will be accomplished by AUTODIN, cross-referencing the assigned PR number. The unclassified E-Mail will only cross-reference the DTG of the AUTODIN message in the SUMMARY OF PROBLEM Section of the PR. Under no circumstance will the MC release classified information in an unclassified E-Mail PR message. The SCO will coordinate the AUTODIN problem report message.

CHAPTER 8. INVESTIGATION REQUEST PROCEDURES

1. General. This chapter briefly reviews and supplements the Investigation Request (IR) process outlined in the Configuration Management (CM) Plan for the DDN.

2. Investigation Requests. IR's are documented investigations of escalated operational problems, requiring additional technical and/or managerial resources to resolve or which need subnetwork-wide implementation.

3. Investigation Request Types. IR types are classifications of problems which consist of the following:

SW - System Software Deficiency
HW - Hardware Problems
SY - System Problems (hardware, software, or firmware)
OP - System Operational Deficiency

a. The first three categories (SW, HW, and SY) will be the responsibility of the contractor to determine if the problem resides in the software, hardware, or a combination supplied by that contractor.

b. The last category (OP) is the responsibility of DCSDS to formulate a resolution and amend appropriate DCA publications, if necessary.

4. Investigation Request Priority Levels. IR Priority Levels are established levels of operational impact. IR priority levels and their associated reporting intervals are presented in Table 8-1. The Contractor IR Manager aids the submitter of the IR recommendation in setting an appropriate priority level. The DCSDS IR Manager retains final authority for initially establishing and/or subsequently changing the priority level of each IR within these guidelines.

5. Investigation Request Procedures. The following steps provide the IR processing procedures from IR recommendation through IR closure. Figure 8-1 provides an IR procedural flow chart.

a. Any outage or occurrence reported in a PR which results in a patch or like modification to the operating network (not including such changes as configuration or parameter changes) or which requires further investigation, will be forwarded to the contractor IR Manager as an IR recommendation. In addition, the Contractor IR Manager receives IR recommendations from the DCSDS IR Manager, the MC's, the contractor technical staff, and the DCA operational staff.

TABLE 8-1. PRIORITIES FOR INVESTIGATION REQUESTS

Priority Level	Definition	Response	Reporting
1	URGENT Severe and widespread impact on operations is occurring.	24hr/7day wk; preempts lower priorities.	Daily (working days) and monthly by E-Mail.
2	CRITICAL Highly probable that impact on operations will occur.	24hr/7day wk; preempts lower priorities.	Weekly and monthly by E-Mail.
3	VERY IMPORTANT Somewhat probable that a severe impact on operations will occur.	Normal work week (Monday through Friday).	Monthly by E-Mail.
4	IMPORTANT Highly probable that reduced performance is or will be experienced by a significant group of users.	Normal work week. Preempts lower priorities.	Monthly by E-Mail.
5	INCONVENIENT Somewhat probable that reduced performance is or will be experienced by a group of users.	Normal work week. Preempts lower priorities.	Monthly by E-Mail.
6	INTERESTING Changes that impact reliability, efficiency testing, etc. Minor corrections without functional impact.	Normal work week. Background tasks.	Monthly by E-Mail.

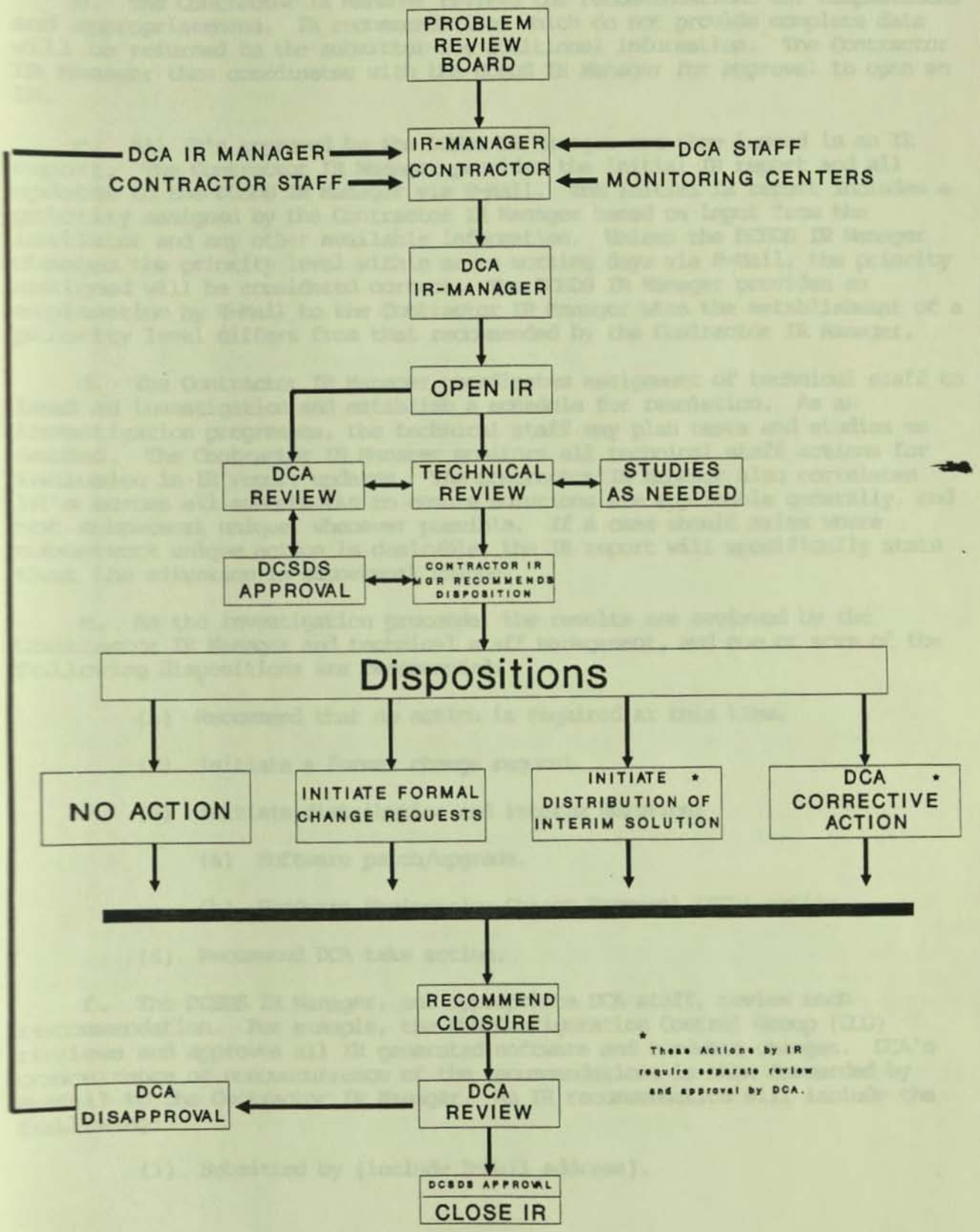


FIGURE 8-1. TRACKING FLOWCHART

b. The Contractor IR Manager reviews the recommendations for completeness and appropriateness. IR recommendations which do not provide complete data will be returned to the submitter for additional information. The Contractor IR Manager then coordinates with the DCSDS IR Manager for approval to open an IR.

c. All IR's approved by the DCSDS IR Manager are then issued in an IR report. The Contractor IR Manager provides the initial IR report and all updates to the DCSDS IR Manager via E-Mail. The initial IR report includes a priority assigned by the Contractor IR Manager based on input from the initiator and any other available information. Unless the DCSDS IR Manager changes the priority level within seven working days via E-Mail, the priority assigned will be considered correct. The DCSDS IR Manager provides an explanation by E-Mail to the Contractor IR Manager when the establishment of a priority level differs from that recommended by the Contractor IR Manager.

d. The Contractor IR Manager coordinates assignment of technical staff to lead an investigation and establish a schedule for resolution. As an investigation progresses, the technical staff may plan tests and studies as needed. The Contractor IR Manager monitors all technical staff actions for inclusion in IR report updates. The Contractor IR Manager also correlates IR's across all subnetworks to ensure solutions are applicable generally, and not subnetwork unique, whenever possible. If a case should arise where subnetwork unique action is desirable, the IR report will specifically state that the situation is subnetwork unique.

e. As the investigation proceeds, the results are reviewed by the Contractor IR Manager and technical staff management, and one or more of the following dispositions are recommended:

(1) Recommend that no action is required at this time.

(2) Initiate a formal change request.

(3) Initiate distribution and interim solution:

(a) Software patch/upgrade.

(b) Hardware Engineering Change Proposal (ECP) action.

(4) Recommend DCA take action.

f. The DCSDS IR Manager, and appropriate DCA staff, review each recommendation. For example, the DDN Configuration Control Group (CCG) reviews and approves all IR generated software and hardware changes. DCA's concurrence or nonconcurrence of the recommendations is then forwarded by E-Mail to the Contractor IR Manager. An IR recommendation will include the following:

(1) Submitted by (include E-Mail address).

(2) DDN network and site.

(3) Suspected IR type (SW, HW, SY, OP).

(4) Suggested IR priority level.

(5) Points of contact to receive all IR correspondence.

(6) A detailed explanation of the problem, including past history and current status.

(7) Description of a workaround if available.

(8) Description of how this problem can be reproduced, if known.

(9) Software version involved, if known.

(10) References (e.g., PR's).

(11) An appended set of any back-up data available (e.g., netlog printout, dumps), if mailed. If IR recommendation is transmitted via AUTODIN or E-Mail, forward this information via mail.

g. The Contractor IR Manager then closes out or revises the IR report according to received DCA direction.

6. Investigation Request Reporting. The Contractor IR Manager is responsible for the following IR reporting:

a. There are three periodic reporting cycles for individual IR reports. They are: (1) daily (working day) reports for priority level 1, (2) weekly reports for priority level 2, and (3) monthly reports for levels 3 through 6. (See Figure 8-2 for example of an IR Report.)

b. In addition to periodic reporting, individual IR reports are sent via E-Mail any time an IR is resolved (recommended closed or closed) or a change occurs.

c. Each quarter, a summary list is sent via E-Mail of all IR's open at the applicable priority level except as follows: (1) If no IR's at that level are open, no report is sent. (2) In the event that there are fewer than five IR's open at the priority 1 or 2 level and all those IR's will be represented by a full report, a summary will not be sent. (See Figure 8-3 for an example of an IR Summary Report.)

d. The Contractor IR Manager is also responsible for providing status in the contractor's monthly project status report. All IR summaries and reports generated during the month are included in this report.

Report on Investigation Request #: IR86-0055-MILNET-SW Report #: 1
Date of Report: 10/23/86 Priority: 3

Reporting: open

IR Title: TAC crashes due to lost data blocks

Summary of Problem:

Euro-MILNET MC has reported that several European TAC's (FKTTC, HDLTC, BRMTC, and VNZTC) have crashed periodically. PAC-MILNET MC has also reported recent TAC crashes.

BBNCC Cambridge Software Support has isolated the TAC crashes to be a result of the TAC running out of PDB's (Protocol Data Blocks) or MBLK's (Message Data Blocks). When a TAC receives a TCP Reset message from hosts for a port which is in a Closing state or Sync-Received state, it does not return to the PDB associated with the message to the free PDB queue. A PDB is lost each time this occurs. The TAC eventually crashes when there are no more PDB's on the free PDB queue. The PDB's remain lost until the TAC is reloaded.

The problem has been corrected in a patch to TAC 113 which properly returns PDB's to the free PDB queue.

Current Status:

10/12/86 report (#1):

TAC 113 (S011-001) corrects the problem of the TAC crashing due to this data block management problem.

Pending Actions:

BBNCC will submit this Patch, TAC 113 (S001-001), to the DDN CCG for approval/disapproval for inclusion on the DDN shelf.

Date Opened: 10/23/86

Reason for Opening: (PR or other): PR86-0188-EMMC-SW

Relevant Problem Area(s): SOFTWARE (TAC 113)
(SOFTWARE, HARDWARE, SYSTEM, PROCEDURAL)

Additional Points of Contact: (other than standard list)

All correspondence about this IR should be copied to all addressees of this message. Additional information is available on request.

FIGURE 8-2. EXAMPLE INVESTIGATION REQUEST REPORT

EXPLANATORY NOTES FOR FIGURE 8-2

The IR identification number is logged by the Contractor IR Manager and is of the form IR (year) - (#) - (network) - (type). The year and sequential number together provide a unique identifier. The type and network information are used for sorting and reference.

The report number is incremented by one each time an IR report is issued by the Contract IR Manager.

In the case of the closed IR Report, if an action is required to re-open the report, the heading will show "RE-OPENED" and the report numbering will continue successively from the last entry.

Priority levels are defined in Chapter 7 of this document.

The reporting entry indicates whether an IR is a new investigation to be opened, an update of a previously opened IR, a closing recommendation, closed, or re-opened.

The IR title is a brief description, particularly useful for summary reports.

Summary of the problem is a concise description of the problem that usually stays the same while the IR is open.

The current status field contains a series of dated entries, latest first. These status entries accujulate so that each report essentially subsumes the lats. This field contains information about the status of an investigation including Solution Numbers and Patch Numbers.

The pending actions field identifies what next steps need to be taken and who is responsible. The emphasis is on immediate action items.

Additional points of contact are those who wish to receive reports on the particular IR. The standard list consists of those authorities and functional representatives who wish to receive all IR reports. In some cases, a person on the standard list may also be called out as a POC to document a special interest in an IR.

The remaining fields are self-explanatory.

OPEN IR's

Date of Report: 11/24/86

PRIORITY 3

IR Number:	IR86-0055-MILNET-SW
IR Priority:	3
IR Title:	TAC crashes due to lost data blocks
MC Recommending IR	CMMC
Date Opened:	10/23/86
Date of Last Report:	10/31/86
Last Report Number:	2
Status:	no change, TAC 113 (S001-001) sub
IR Action Group:	Contractor

IR Number:	IR86-0050-MILNET-SW
IR Priority:	3
IR Title:	IOP PSN drops packets
MC Recommending IR	CMMC
Date Opened:	08/29/86
Date of Last Report:	09/25/86
Last Report Number:	2
Status:	no change, PSN 6.0 P54
IR Action Group:	DCA

PRIORITY 4

IR Number:	IR86-0011-MILNET-SW
IR Priority:	4
IR Title:	NU 6.0 vermolist - all in global dumps core
MC Recommending IR:	CMMC
Date Opened:	03/13/86
Date of Last Report:	10/31/86
Last Report Number:	3
Status:	no change, NU 6.0 P26 (vermolist)
IR Action Group:	DCA

FIGURE 8-3. EXAMPLE INVESTIGATION REQUEST SUMMARY REPORT

EXPLANATORY NOTES FOR FIGURE 8-3

The IR number

The IR priority

The IR title

MC recommending IR

Date the IR was opened

Date of the last IR report (and, therefore, the last status change)

The last report number

The IR status, which includes two entries:
(Open, update, closing recommendation, closed, or re-opened)

A short text field describing the current status (i.e., waiting for next PSR release, patch into test, etc.)

IR action group

CHAPTER 9. SOFTWARE CONFIGURATION MANAGEMENT

1. General. This chapter provides procedures and guidance, and defines the control responsibilities for DDN software configuration management.

2. Scope.

a. DCA is not responsible for any software associated with user equipment. Software for such equipment is the sole responsibility of the sponsoring MILDEP or agency. Therefore, unless otherwise specified, the use of the word software in this chapter is referring to DDN backbone software.

b. All software used in the DDN backbone is the responsibility of DCA. Requests by MILDEP's or agencies for changes to the software are forwarded to DCA for review and approval.

c. Distribution of the documentation pertinent to the software is limited to those Government organizations with direct support responsibilities. Requests from other organizations shall be directed to DCA, ATTN: DDRA, Washington DC 20305-2000.

3. Defense Communications Agency (DCA) Responsibilities.

a. Provides the overall development, implementation, maintenance, and management of DDN software.

b. Ensures Independent Verification, Validation, and Test (IVV&T) of all revisions, enhancements and changes to the software.

c. Provides quality assurance on all assumed or acquired software.

d. Directs the applicable MC's to install and deploy software.

e. Reviews for approval all discretionary software changes made by the MC's.

f. Provides a focal point for software recommendations and requirements.

g. Provides advance notification to DoD activities and other appropriate agencies of any software actions which would impact systems connected to the DDN.

h. Defines and provides the MILDEP's and agencies with a listing of X.25 certified interface devices. In addition, DCA provides for X.25 certification testing.

i. Conducts audits and reviews of the configuration management records to ensure that the required software configuration is maintained in the network.

4. Monitoring Center (MC) Responsibilities.

a. Ensures software deficiencies are properly reported as PR's or IR's.

b. Maintains network configuration control data.

c. Requests deployment of software changes and MC data base changes from DCA via an NCR.

d. Obtains, installs, and deploys software as directed by DCA. The DCA direction will be via an NCD.

e. Notifies DCA of installation and deployment completion, via an NCAN.

f. Deploys emergency patches and diagnostic software. Advises DCA within the defined time limits via a Discretionary NCAN.

g. Performs software audits and reviews as directed by DCA.

h. Acts as the central coordinating authority with the NSC's and appropriate Service and/or Agencies on the installation of software.

5. Prime Software Contractor Responsibilities. The prime software contractor, as directed by DCA, is responsible for the design, development, testing, implementation, configuration management, and routine administration of the DDN software. Specific responsibilities include, but are not limited to, the following:

a. Develops and maintains software configuration management documentation.

b. Develops and maintains software inventory, inventory accounting, and update reporting, in coordination with DCA.

c. Prepares and maintains a DDN software component library of approved items available for distribution and installation.

d. Develops and documents DCA approved changes to operational software.

e. Exercises daily configuration management over all software development activities, in conjunction with DCA.

f. Develops, executes, and evaluates emergency corrections to reported deficiencies in the software.

6. Configuration Management. Configuration Management (CM) for the DDN provides orderly and accountable control over the network and its components as they exist and as they change. CM for DDN software is divided into two areas: (1) Network Component Configuration Management, (2) Operational Network Configuration Management. Figure 9-1 depicts the DDN CM overview. The software management structure is shown in Figure 9-2.

a. Network Component Configuration Management. Network component CM is basically developmental. In this area, the prime software contractor works with the members of the DDN CCG to review, approve, and document all new baseline software releases, and subsequent patches to these releases.

(1) Configuration Control Group (CCG). DCA's formal review and approval or disapproval of changes to the software baseline is accomplished by the CCG. The CCG performs the following functions:

(a) Reviews and approves changes to the existing software baselines, ensures that the changes are properly implemented and tested, and ensures documentation changes are accomplished.

(b) Reviews changes to software to check for security impact.

(c) Manages formal records of all changes to the system.

(d) Ensures that all software releases and revisions are rigorously tested.

(e) Convenes requirements review and design review panels for technical review of software design changes.

(f) Reviews software Release Overviews and approves or disapproves the technical design approach.

(g) Approves or disapproves software program releases and patches.

(2) Computer Software Configuration Items. Each DDN hardware and software component is identified as a configuration management item (CMI). Software components are specifically identified as computer software configuration items (CSCI's). DDN CSCI's consist of all documentation and identification associated with CCG approved PSN program packages and microcode, TAC program and microcode, and any additions or modifications to NU.

(3) Software Patches. Software patches are used to correct deficiencies or incorporate minor enhancements into existing software. Patches are normally a result of software problems identified on the operational network and documented in a PR and/or IR. Other problems are identified by the contractor during development, testing, or operations.

(a) Patches are developed by the DDN software contractor and are submitted via a Patch Release Note to the DCSDS. Upon acceptance, the Patch is processed through the CCG for approval/disapproval for placement on the operational shelf.

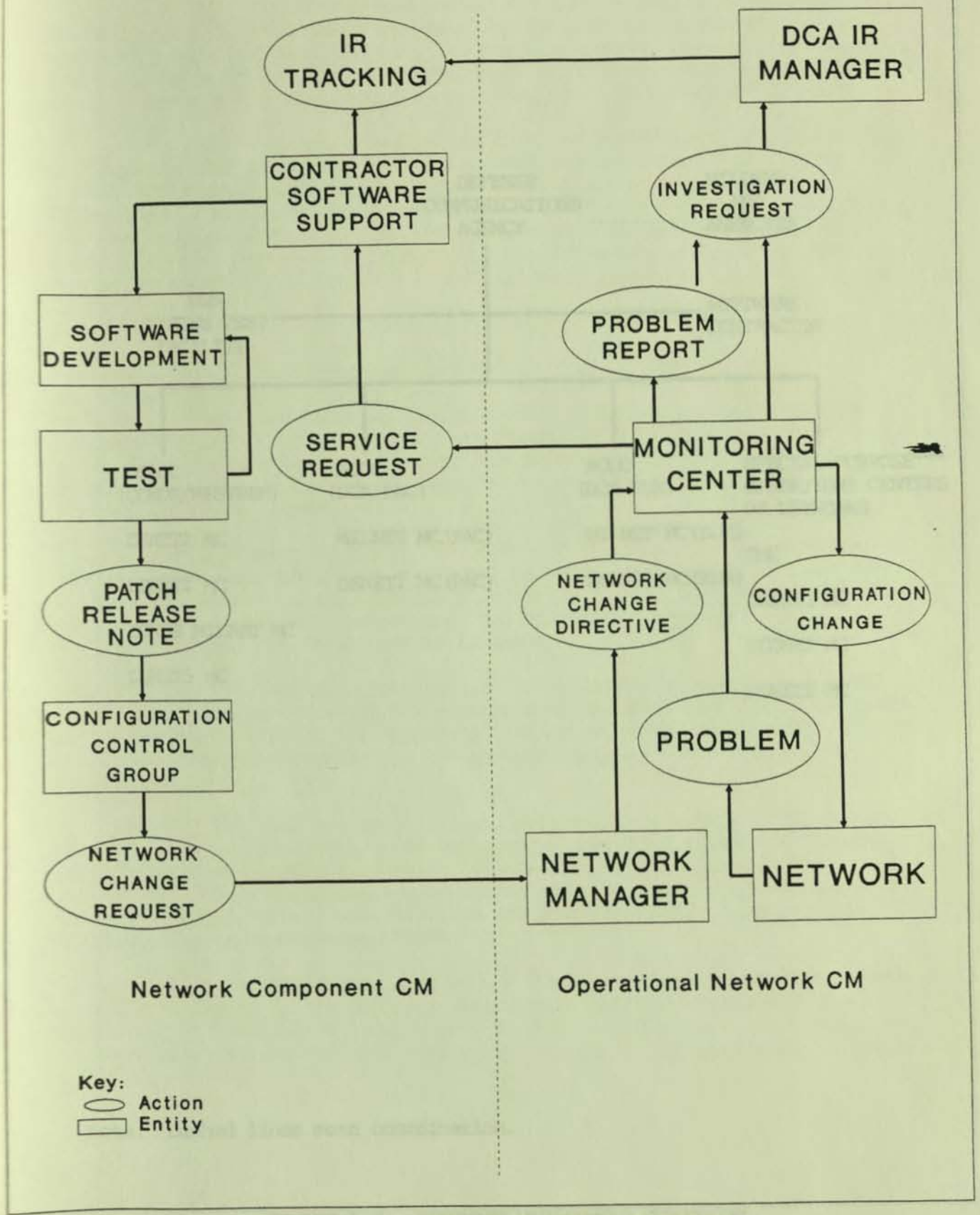
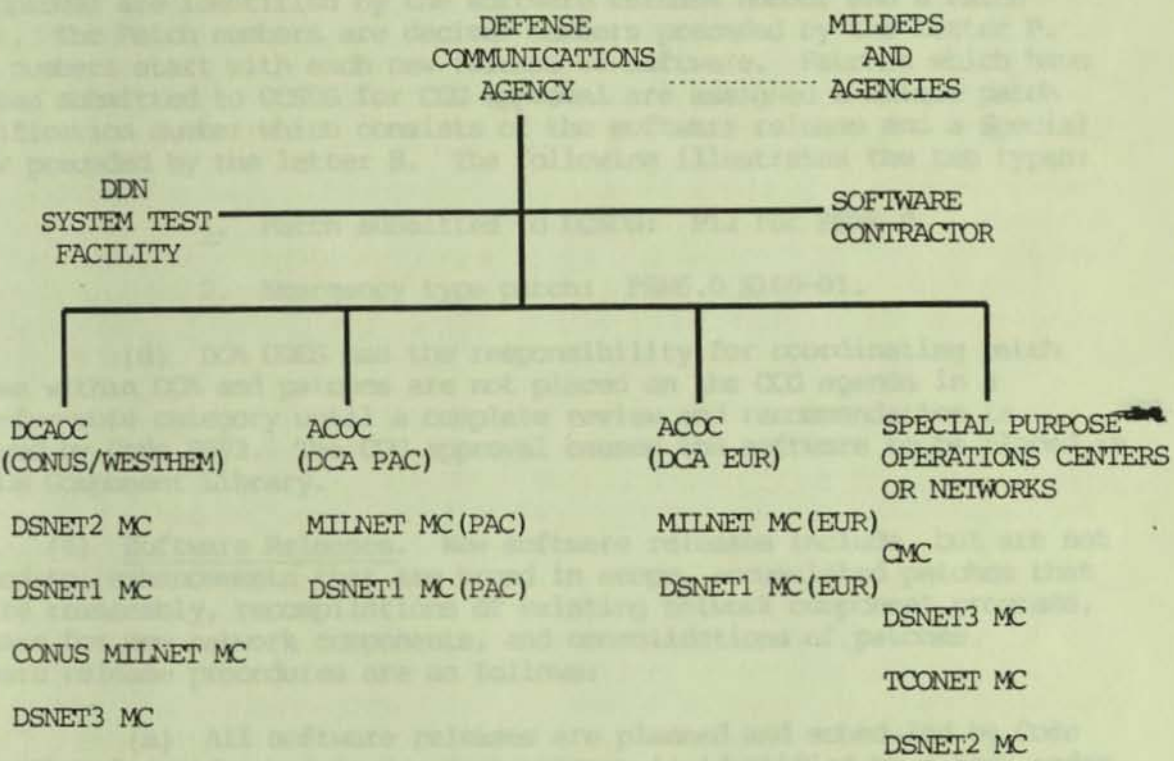


FIGURE 9-1. SOFTWARE CONFIGURATION MANAGEMENT



Note: Dashed lines mean coordination.

FIGURE 9-2. SOFTWARE MANAGEMENT STRUCTURE

(b) DCSDS does not conduct formal testing of the patches. Each proposed software patch is tested by the software development contractor at their test facility. These test results are used by DCA in the evaluation of the patch for acceptance. The contractor then generates a Patch Release Note containing a section entitled, "Testing Performed."

(c) Patches submitted to DCSDS by the software contractor for CCG approval are identified by the software release number and a Patch number. The Patch numbers are decimal numbers preceded by the letter P. These numbers start with each new release of software. Patches which have not been submitted to DCSDS for CCG approval are assigned a unique patch identification number which consists of the software release and a Special number preceded by the letter S. The following illustrates the two types:

1. Patch submitted to DCSDS: P12 for PSN6.0.

2. Emergency type patch: PSN6.0 S100-01.

(d) DCA DDES has the responsibility for coordinating patch reviews within DCA and patches are not placed on the CCG agenda in a ready-for-vote category until a complete review and recommendation is received by Code B602. The CCG approval causes the software to be placed in the DDN Component Library.

(4) Software Releases. New software releases include, but are not limited to, enhancements that are broad in scope, accumulated patches that require reassembly, recompilations of existing network component programs, software for new network components, and consolidations of patches. Software release procedures are as follows:

(a) All software releases are planned and scheduled by Code B612. The plan and schedule for each release is identified by a task order and reviewed by the CCG for approval; once approved for development, the task order is incorporated into the software support contract for development.

(b) New software releases affecting the network access protocols may require subscriber software or operating procedure changes. DCA provides advanced notification of such releases to all affected subscribers to allow software programming or operating procedure changes to be made. The length of time allotted for such changes is by necessity, determined on a case-by-case basis.

(c) DCSDS does not conduct formal testing of releases. Each release is tested by the software development contractor at their test facility. A test report is generated to document the results. DCSDS reviews the test results when reviewing the release for approval.

(d) The Software Release Request (SRR) is submitted to the Contracting Officers Representative (COR), Code DDRA, and to Code B602, by the development contractor. Code B602 assigns a CCG tracking action number to the SRR and the COR passes it to the Action Office, Code DDES, for solicitation of comments from other DCSDS elements and to provide an acceptance or rejection recommendation back to the COR. If accepted, the SRR will be considered for approval or disapproval by the CCG. If approved, the software will be placed on the DDN Component Library (Operational Shelf) at the contractor's facility. If rejected, the contractor will be directed to correct the problem preventing its approval. Software is conditionally approved for operational use in cases where documentation is not totally accepted, but a requirement exists for the software to be made operational.

7. Operational Network Configuration Management. Operational network CM applies to the CM for the installed software. In this area, DCA works with the prime software contractor to distribute and deploy approved changes to the network components, control the investigation of software problems, deploy emergency patches, and conduct audits and reviews of the operational network software.

a. Distribution. The DCSDS Software Manager, Code B652, establishes the schedule for implementation of a patch release and directs the distribution of the software via NCD. This NCD authorizes the designated MC's to obtain the software from the DDN Component Library, to install the software on the MC,
and to deploy the software.

(1) A collection of all CCG approved software patches is distributed on a DDN Software Update (DSU) tape. The tape contains a collection of individual patches for all software releases. When installed, the net result is the same as if these patches had been installed individually. The tape is identified as DSU yy.i where "yy" equals the year in which the tape was distributed and "i" equals the number of tapes issued so far that year. For example, DSU86.3 would be the third tape issued in 1986.

(2) The first Tuesday of February, April, June, August, October, and December is the cut-off date for adding patches to the DSU. If no patches have been approved since the last tape was generated, a new DSU will not be generated. When a new tape is generated, it will be tested and shipped to the monitoring centers on the third Tuesday of the above months. DCSDS, Code B652, will direct the deployment of appropriate patches from the tape following its distribution.

b. Deployment. DCSDS, Code DDOS, directs the deployment of each patch via an NCD. If the patch was not to resolve an emergency situation, an NCD will be issued to deploy all required patches from the DSU tape distribution for that period. For emergency situations, an NCD will be issued immediately. This NCD will authorize the designated MC(s) to obtain the patch(es) from the DDN Component Library, will authorize the software

contractor to honor the software request, and will direct the patch(es) to be deployed. When a software patch is deployed by the MC, an NCAN is issued to confirm that the software implementation action has been completed.

c. Software Deficiency Reporting. DDN software component deficiencies which cause operational problems are to be reported as an IR. (See Chapter 9.)

d. Emergency Program Actions. Emergency program actions are sometimes required for the resolution of program deficiencies which deny service to a significant number of users. The MC's are authorized to initiate a temporary program change under these conditions.

(1) Conditions for Emergency Action. Emergency action may be taken if the program deficiency is in one of the following categories:

(a) The problem is classified as being urgent and will cause severe and widespread impact on operations. This is considered a Priority 1 problem when reported as an IR. An IR must be opened within 24 hours after deployment of the software.

(b) The problem is critical and it is highly probable that a severe and widespread impact will occur soon. This is considered a Priority 2 problem when reported as an IR. An IR must be opened within 24 hours of deployment of the software.

(c) The problem is very important and it is possible that a severe impact on operations will occur. This is considered a Priority 3 problem when reported as an IR. In this case an IR must be opened before the software can be deployed.

(2) MC Actions.

(a) The MC will obtain and deploy the software to resolve the problem.

(b) As soon as possible, but not later than within 72 hours, the MC will forward a Discretionary NCAN to the DCSDS Software Manager. This Discretionary NCAN will describe the software deployed, the problem that occurred, and specify all PR's and IR's opened as a result of the problem.

(c) If, at the end of 96 hours, DCSDS has not responded with an NCD acknowledging the NCAN, the software must be removed from the system.

(3) DCSDS Actions.

(a) DCSDS will evaluate the problem, its resolution, and issue an NCD if the software is to remain on the system.

(b) If it is determined that the software should not remain on the system, an NCD will be sent to the MC requesting that the software be removed.

8. Requests for System Modification. DCSDS, Code DDES, is responsible for all DDN backbone component software development actions.

a. Software Enhancement. A software enhancement is defined as a new backbone operational capability that has potential for implementation by software programming. Code DDES has the overall responsibility for review of software requirements and enhancements regardless of their origin. The CCG has the responsibility for final approval of these requirements and enhancements for development and implementation.

b. System Change Proposal (SCP). An SCP serves as the vehicle for requesting a change to the DDN backbone component software. An SCP may be generated by any Host Administrator but must be formally submitted to their respective Communications and/or Information Systems O&M Command for validation. Validated SCP's shall be forwarded via letter endorsement, to DCA, ATTN: Code DDES, Washington, DC 20305-2000.

c. Format for SCP Submittal. An SCP shall be submitted in the following format and contain the information described for each field:

(1) Submitted By: Name of the person submitting the change. (Principal point of contact most familiar with the requirement.)

(2) Date: Date that the SCP is submitted.

(3) Organization: Organization of the submitter.

(4) Type of Proposal: Software.

(5) Change Description: A detailed description of the software change desired.

(6) Justification for the Change: Reason why the change is desired and the extent to which the change is applicable to other DDN subscribers' host system.

(7) Impact if not Approved: The impact on the system if the change is not approved.

(8) Priority of Request: The urgency of the change.

(9) Test Information: Any special consideration for testing the change if approved.

d. System Change Proposal Processing. All SCP's are processed as follows:

(1) The HA submits, via cover letter, the SCP to the respective O&M Command or Agency.

(2) The O&M Command or Agency shall evaluate the proposal for its network-wide application, and forward validated requirements, via letter endorsement with comments, to DCA. Proposals which are not validated by the O&M Command or Agency shall be returned to the originating HA with no further action required.

(3) Validated proposals received from the O&M Command or Agency shall be evaluated by DCA on a case-by-case basis and notification provided as to its approval or disapproval.

(4) Approved proposals shall be assigned a DCA control number and identified for inclusion in a future software release.

2831-91

Draft Report - February 1991

Descriptions of NIC Tables and Lists

Prepared by:
SRI International
Network Information Systems Center
333 Ravenswood Avenue
Menlo Park, California 94025

Mary K. Stahl
Douglas MacGowan

Prepared for:

Defense Communications Agency
DDN Defense Communications System Organization
Code B622
Washington, DC 20305

Attention: Mr. Tyrone Smallwood

cc: Defense Communications Agency (D712/RPDA)
Defense Commercial Communications Office
Scott Air Force Base, Illinois 62225-8300

Attention: Ms. Deborah Wellen

Contract DCA200-90-C-0027
SRI Project ECU 1050
CDRL No. 027

Approved by:

Franklin F. Kuo, Acting Director
Network Information Systems Center

REPORTS

UNCLASSIFIED
SECURITY CLASSIFICATION OF THIS PAGE

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1a. REPORT SECURITY CLASSIFICATION Unclassified	1b. RESTRICTIVE MARKINGS
2a. SECURITY CLASSIFICATION AUTHORITY	3. DISTRIBUTION / AVAILABILITY OF REPORT
2b. DECLASSIFICATION / DOWNGRADING SCHEDULE	
4. PERFORMING ORGANIZATION REPORT NUMBER(S) DID DI-E-30105B, SRI Project 1050	5. MONITORING ORGANIZATION REPORT NUMBER(S)
6a. NAME OF PERFORMING ORGANIZATION SRI International Network Information Sys Center 6b. OFFICE SYMBOL (If applicable) EJ201	7a. NAME OF MONITORING ORGANIZATION Defense Commercial Communications Office
6c. ADDRESS (City, State, and Zip Code) 333 Ravenswood Avenue Menlo Park, California 94025	7b. ADDRESS (City, State, and Zip Code) Defense Communications Agency Scott Air Force Base, Illinois 62225-8300
8a. NAME OF FUNDING / SPONSORING ORGANIZATION Defense Communications Agency 8b. OFFICE SYMBOL (If applicable) B622	9. PROCUREMENT INSTRUMENT IDENTIFICATION NUMBER DCA200-90-C-0027
8c. ADDRESS (City, State, and Zip Code) Code B622 Washington, D.C. 20305-2000	10. SOURCE OF FUNDING NUMBERS PROGRAM ELEMENT NO. / PROJECT NO. / TASK NO. / WORK UNIT ACCESSION NO.
11. TITLE (Include Security Classification) Descriptions of NIC Tables and Lists	
12. PERSONAL AUTHOR(S) Mary K. Stahl, Douglas MacGowan	
13a. TYPE OF REPORT Draft 13b. TIME COVERED FROM _____ TO _____	14. DATE OF REPORT (Year, Month, Day) 91-02-25 15. PAGE COUNT
16. SUPPLEMENTARY NOTATION	

17. COSATI CODES			18. SUBJECT TERMS (Continue on reverse if necessary and identify by block number)
FIELD	GROUP	SUB-GROUP	TACs, gateways, hosts, autonomous systems, domains

19. ABSTRACT (Continue on reverse if necessary and identify by block number)

The DDN Network Information Center (NIC), under contract to the Defense Communications Agency, provides naming and addressing registration services for the Defense Data Network (DDN). Named and numbered entities registered under this contract, include hosts (including Terminal Access Controllers (TACs) and gateways), networks, autonomous gateway systems, and domains. The NIC maintains and administers a number of tables and files containing data as a result of this registration service.

20. DISTRIBUTION / AVAILABILITY OF ABSTRACT ☐ UNCLASSIFIED/UNLIMITED ☐ SAME AS RPT. ☐ DTIC USERS	21. ABSTRACT SECURITY CLASSIFICATION
22a. NAME OF RESPONSIBLE INDIVIDUAL Franklin F. Kuo	22b. TELEPHONE (Include Area Code) (415) 859-4116 22c. OFFICE SYMBOL EL290

DD Form 1473, JUN 1986 *Previous editions are obsolete* SECURITY CLASSIFICATION OF THIS PAGE

ABSTRACT

This document describes all online tables, files, and distribution lists maintained by the DDN Network Information Center (NIC) under contract to the Defense Communications Agency. This document fulfills the requirements of CDRL 027, under contract DCA200-90-C-0027.

TABLE OF CONTENTS

List of Figures

SECTION 1. INTRODUCTION

The DDN Network Information Center (NIC), under contract to the Defense Communications Agency, provides naming and addressing registration services for the Defense Data Network (DDN). Named and numbered entities registered under this contract comprise hosts (including Terminal Access Controllers (TACs) and gateways), networks, autonomous gateway systems, and domains. The NIC maintains and administers a number of tables and files containing data as a result of this registration service.

All of the tables and files described in this document may be obtained from the NIC.DDN.MIL host via FTP or by sending an email request to the SERVICE@NIC.DDN.MIL mailbox. Each file is described in a separate subsection of this document. Online file names are specified either in the heading of the subsection that describes the file or in the subsection text describing its purpose.

Descriptions of the files are provided in three main sections. Section 2 includes machine-readable online files; these are referred to as "tables." Files described in Section 3 are human-readable files that exist for informational reasons and are more user-friendly than those in Section 2. Section 4 includes descriptions of online mailing lists associated with the files and tables. All files and tables include a version number and/or the date of last update at the top of the file.

Examples of the tables and lists described in this document can be found in the Appendix.

SECTION 2. TABLES

2.1 NETINFO:HOSTS.TXT

2.2 Purpose

Type = Machine Readable.

This table is the Official DoD Internet Host Table in ASCII text. It provides name-to-address translation and is used by hosts in the DDN Internet to interoperate with one another. The table is available via FTP as NETINFO:HOSTS.TXT. It is also available via the NIC Hostname Server on port 101 of the NIC.DDN.MIL host. Host data in the table are obtained from several sources: from Network Change Directives (NCDs) issued by the network managers; from administrators of DDN and internet hosts; and from data obtained through network registration performed as part of the NIC Hostmaster function. The host table specification has been described in RFC-952, "DoD Internet Host Table Specification."

2.2.1 Format

HOSTS.TXT comprises three types of entries, divided into groups. The groupings for entries are NET, GATEWAY, and HOST, with the network entries being the first group listed. Each group contains a variable number of individual entries. (See Appendix, Figure A-1.)

MILNET (network 26) hosts are sorted according to their PSN number (the fourth octet of the internet address) and by PSN port number (the second octet of the internet address.) All other entries are sorted numerically by network address within each group.

2.2.2 Description of Elements

Each host table entry is an ASCII text string and is composed of six data fields: keyword, internet address, name/nickname, machine type, operating system, protocol list. The fields are separated by colons, and each entry ends with a colon.

Field 1	KEYWORD indicating whether this entry pertains to a NET, GATEWAY, or HOST. NET entries are fixed and cannot have alternate addresses or nicknames.
Field 2	Internet Address of Network, Gateway, or Host, followed by alternate addresses.
Field 3	Official Name of Network, Gateway, or Host (with optional nicknames, where permitted.)
Field 4	Machine Type
Field 5	Operating System
Field 6	Protocol List

Fields 4, 5, and 6 are optional, but strongly encouraged.

Fields 3 through 6, if included, pertain to the first address in Field 2.

"Blanks" (spaces and tabs) are ignored between data elements or fields, but are disallowed within a data element.

A semicolon starts a comment; the remainder of the line is ignored.

Each entry ends with a colon.

2.2.3 Method of Generation

The host table is generated twice weekly using the NIC program TABLE.EXE. The program extracts the data from the NIC WHOIS data base, compiles it in table form, inserts introductory commentary information at the beginning of the table, and increments the version number by one digit based on the version number of the previously generated table.

2.3 NETINFO:HOSTS.TXT-Z

2.3.1 Purpose

Type = Machine Readable

This is a UNIX 4.3BSD compressed version of the information in HOSTS.TXT. Its format, method of generation, and function are the same as for the HOSTS.TXT description above.

2.4 NETINFO:MIL-HOSTS.TXT

2.4.1 Purpose

Type = Machine Readable

This Table contains HOSTS.TXT entries of MILNET machines. Its format and function is the same as for the HOSTS.TXT description above.

2.4.2 Method of Generation

This file is generated simultaneously with the HOSTS.TXT table by using the program STABLE.EXE.

2.5 NETINFO:NETWORKS.TXT

2.5.1 Purpose

Type - Machine readable

This table contains one entry for each registered network and is used by UNIX systems on the DDN and Internet to map network names to numbers prior to establishing network connections.

2.5.2 Description of Elements

The individual entries in the group NET consist of three fields:

Field 1	Keyword NET
Field 2	Internet network numbers
Field 3	Official name of network.

2.5.3 Method of Generation

This table is generated by the NIC program TABLE.EXE at the same time HOSTS.TXT is generated.

2.6 NETINFO:DOMAINS.TXT

2.6.1 Purpose

Type = Machine readable

This table is an ASCII text file of all the official registered top-level domains. Data included in the table are obtained from information provided by the Domain Administrator and are stored in the NIC WHOIS database. The table is updated on an as-needed basis each time a new top-level domain is registered or when any of the data change. The domains table may be obtained via FTP from host NIC.DDN.MIL as NETINFO:DOMAINS.TXT, or by using the NIC Hostname Server on port 101 of the NIC host.

2.6.2 Format

The format of this table is based on that of the Official DoD Internet Host Table. There is only one group of entries, DOMAIN. (See Appendix, Figure A-2.)

2.6.3 Description of Elements

The individual entries in the group DOMAIN consist of three fields:

Field 1	Keyword DOMAIN
Field 2	Internet addresses of name servers for the domain, each one separated by a comma.
Field 3	Official name of top-level domain.

"Blanks" (spaces and tabs) are ignored between data elements or fields, but are disallowed within a data element.

Each entry ends with a colon.

2.6.4 Method of Generation

The domain table is updated via running the NIC program DOMTXT.EXE.

2.7 Zone Files for DDN Domain Name System

2.7.1 Purpose

Type = Machine readable

These are the master files for the DDN Domain Name System. They provide a standard representation to be converted by individual domain name software systems. (See Appendix, Figure A-3.) Filenames are in the form *.ZONE, with "*" being the name of a top-level domain. A separate data file exists for each zone or top-level domain. The zone files, which are available in ASCII text format, contain information on all top-level and second-level domains registered in the NIC WHOIS database. The various domain name servers and resolvers in use on the DDN and Internet convert these files into a format suitable to their purposes. The TOPS20 operating system that is run on the root server A.ISI.EDU relies upon the domain binary file equivalents that are described below. Each file contains information about the name servers for the zone. This information includes the name servers' internet addresses. The files may also hold information on delegated subdomains and hosts for that particular domain. Historically, however, hosts have not been permitted to register in top-level domains; therefore, the zone files for top-level domains do not currently contain host information.

The files also indicate the length of time that the data are considered to be valid. Information included in these files is obtained primarily from domain registration applications processed by NIC Hostmaster, and from corrections submitted to NIC Hostmaster by Domain Administrators. Other information is obtained through the host registration process via NCDs, and by correspondence with Host Administrators and coordinators of Internet hosts or networks.

2.7.2 Format

Each zone file contains some introductory commentary information at the beginning of the file. Entries follow, in the form of Resource Records (RRs) with a standard format, as shown below.

<name> [<ttl>] [<class>] <type> <data>

The record is divided into fields which are separated by white space. A blank field defaults to the previously specified field in a previously defined resource record.

2.7.3 Description of Elements

The individual elements of each entry follow the format specified in RFC-1033, "Domain Administrators Operations Guide," and in RFC-1034, "Domain Names - Concepts and Facilities."

<name>	The name field defines what domain name applies to the given RR.
<ttl>	TTL stands for Time To Live. It specifies how long a domain resolver should cache the RR before it discards the data and asks a domain server again. If the TTL field is blank, the resolver will default to the minimum time specified in the record that denotes the start of the zone.
<class>	The class field specifies the protocol group. Currently, two types are defined: Internet (IN) and CSNET (CS).
<type>	The type field specifies what type of data is in the RR. The currently defined types are Name Server (NS), Internet Address (A), Canonical Name or Alias (CNAME), Well Known Service (WKS), Host Information (HINFO), and Mail Exchanger (MX).
<data>	The data field is defined differently for each type and class of data.

A semicolon starts a comment; the remainder of the line is ignored.

The asterisk ("*") is used for wildcarding.

The at-sign ("@") denotes the current default domain name.

2.7.4 Method of Generation

The zone files are generated twice weekly with the NIC program MAKEZ.EXE. If no errors are found, these files are transferred to the root server ns.nic.ddn.mil, and to the other root server sites in the domain name system. Binary equivalents of the zone files are then generated for the root server at A.ISI.EDU using the program MAKEDB.EXE.

2.8 Binary Files for DDN Domain Name System

2.8.1 Purpose

Type = Machine readable

These files are the binary equivalent of the zone files described above. The files, stored in the domain name server and domain name resolver, are used by root servers that run the TOPS20 operating system. At this time, the only active TOPS20 root server is located at A.ISI.EDU.

2.8.2 Method of Generation

The files are generated twice weekly by running the NIC program MAKEDB.EXE. This program reads the domain zone files and compiles a binary version of the data in the online file DOMAIN:FLIP.DD. This file is then renamed to the <DOMAIN.VERSION5> directory.

SECTION 3. INFORMATIONAL FILES

3.1 NETINFO:MIL-HOST-ADMINISTRATORS-A-L.TXT

(NETINFO:MIL-HOST-ADMINISTRATORS-M-Z.TXT)

3.1.1 Purpose

Type = ASCII text

These files list the Host Administrator (HA) for each host on MILNET (network 26). All data in the file are extracted from the NIC WHOIS database. Initially the data are collected from NCDs, then are kept current by monthly online solicitations for corrections to HAs by NIC Hostmaster. (See Appendix, Figure A-4.)

3.1.2 Format

The entries in the HA file are sorted by hostname and consist of the name of the host; the host network address; and the name, mailbox, postal address, and phone number of the Host Administrator. Also included in each entry is the sponsoring agency for the host, and the type of communications interface between the host and the network. In addition, each entry contains the text line pertaining to the host from the Official DoD Internet Host Table. It also shows the host configuration. (See Appendix, Figure A-4.)

3.1.3 Method of Generation

The HA file is generated using the NIC program TABLE.EXE. The file is updated weekly.

3.2 NETINFO:MIL-NSC.TXT

3.2.1 Purpose

Type = ASCII text

This file lists the Node Site Coordinator (NSC) for each host on MILNET (network 26). Information contained in the file is obtained from several sources. The initial information is taken from NCDs. Changes, deletions, or additions are obtained from responses to NIC Hostmaster's monthly request for updates sent to all NSCs. Information is also received from individual NSCs on a voluntary basis. All data for this file are stored in the NIC WHOIS database. (See Appendix, Figure A-5.)

3.2.2 Format

The entries in the file are sorted according to PSN number. Each entry contains the PSN number and name; name of the network; name, mailbox, address, and phone number of the NSC; and phone numbers for emergencies, after hours, and the NSC's home. In addition, the file contains the network address and hostname of any TAC or gateway attached to the PSN. (See Appendix, Figure A-5.)

3.2.3 Method of Generation

The MILNET NSC file is generated weekly using the NIC program TABLE.EXE.

3.3 NETINFO:MIL-CONFIG.TXT

3.3.1 Purpose

Type = ASCII text

This file lists the host configuration for each host on MILNET. The information for this file is obtained from NCDs, correspondence with HAs, and the results of the monthly request for updates sent to each HA by NIC Hostmaster. The data are stored in the NIC WHOIS database. (See Appendix, Figure A-6.)

3.3.2 Format

Entries in the file contain of the PSN number, PSN name, "O&M," PSN port number, hostname, host configuration, and type of communications interface connecting the host to the network. The entries are sorted in numerical order according to PSN number; each host connected to the PSN is sorted in numerical order by PSN port number. The host configuration information consists of the machine type and operating system used by the host. (See Appendix, Figure A-6.)

3.3.3 Method of Generation

The host configuration file is generated using the NIC program TABLE.EXE. An updated version of the file is generated weekly.

3.4 NETINFO:HOST-LOCATION.TXT

3.4.1 Purpose

Type = ASCII text

This file lists all MILNET hosts sorted according to their geographical location.

3.4.2 Format

Each entry in the file is comoosed of hostname, host network address, and postal address of the host site. The entries are sorted alphabetically according to state or country. (See Appendix, Figure A-7.)

3.4.3 Method of Generation

The host location file is generated using the NIC program TABLE.EXE. The file is generated weekly.

3.5 NETINFO:TAC-LOCATION.TXT

3.5.1 Purpose

Type = ASCII text

This file contains a list of all the MILNET TACs. Data are obtained from NCDs and from communication with NSCs on a regular basis and are subsequently stored in the NIC WHOIS database.

3.5.2 Format

Entries in the file comprise the hostname, network address, and postal address of the TAC site; and the name, mailbox, and phone number of the NSC for the TAC. (See Appendix, Figure A-8.)

3.5.3 Method of Generation

The file is generated weekly using the NIC program TABLE.EXE.

3.6 NETINFO:MIL-PSN-COORD.TXT

3.6.1 Purpose

Type = ASCII text

This file lists the contacts for every PSN and attached host on MILNET (network 26).

3.6.2 Format

Each entry in the file is composed of several layers of information. The entries are sorted according to their PSN number. The beginning line of the entry contains the PSN number and PSN name. The second line of information gives the name and network mailbox of the NSC. The following line of the entry shows the host, gateway, or TAC attached to the PSN; these entities are listed according to their network address. The fourth line of the entry shows the name and network mailbox of the HA or NSC for each of these attached entities. (See Appendix, Figure A-9.)

3.6.3 Method of Generation

This file is generated weekly using the NIC program TABLE.EXE.

3.7 NETINFO:HADMINBYADDR.TXT

3.7.1 Purpose

Type = ASCII text

This file lists all and MILNET hosts, gateways, and TACs with the name and mailbox of the contact for each. All data in the file are extracted from the NIC WHOIS database. Initially the data are collected from NCDs, and then are kept current by monthly online solicitations by NIC Hostmaster to each Host Administrator for corrections to the data.

3.7.2 Format

Each entry in the file consists of a hostname, host network address, and name, mailbox, and phone number of the HA. Entries are sorted according to their network addresses so that all hosts situated on a PSN are adjacent to one another in the list. TAC entries are handled in a different manner; because TACs have NSCs, not HAs, a referral to the NSC file is inserted in TAC entries. (See Appendix, Figure A-10.)

3.7.3 Method of Generation

The file is generated weekly using the NIC program TABLE.EXE.

3.8 NETINFO:DOMAIN-CONTACTS.TXT

3.8.1 Purpose

Type = ASCII text

This file contains the name and address of contacts for each registered domain in the DDN domain naming system. Information included in this file is obtained from domain registration applications processed by NIC Hostmaster, and from corrections submitted to NIC Hostmaster by Domain Administrators. The raw data are stored in the NIC WHOIS database.

3.8.2 Format

Each entry in the file consists of the name of the domain followed by the name, mailbox, and phone number of the administrative, technical, and zone contacts for the domain. The file is organized by top-level domain name. The contacts for any existing second-level domains are listed under the information for each top-level domain. (See Appendix, Figure A-11.)

3.8.3 Method of Generation

This file is generated weekly using the NIC program DOMFKS.EXE.

3.9 NETINFO:DOMAIN-INFO.TXT

3.9.1 Purpose

Type = ASCII text

This file provides a summary list of all top-level domains and any second-level domains currently registered in the NIC WHOIS database. Information included in this file is obtained from domain registration applications processed by NIC Hostmaster, and from corrections submitted to NIC Hostmaster by Domain Administrators. The raw data are stored in the NIC WHOIS database.

3.9.2 Format

Each entry in the file consists of the name of the top-level domain and subdomains registered at the second-level. In the case where there are no second-level domains registered under a top-level domain, a statement to that effect is inserted in the file. (See Appendix, Figure A-12.)

3.9.3 Method of Generation

This file is generated weekly using the NIC program DOMFKS.EXE.

3.10 NETINFO:NETWORK-CONTACTS.TXT

3.10.1 Purpose

Type = ASCII text

This file contains the information on contacts for every registered 32-bit Internet number. Information included in this file is obtained from Internet number registration applications processed by the NIC Hostmaster, and from corrections submitted to NIC Hostmaster by network coordinators. The raw data are stored in the NIC WHOIS database.

3.10.2 Format

Each entry in the file consists of the Internet number and name of the network, followed by the name, NIC WHOIS database handle, mailbox, and phone number of contact for the network. The file is organized according to network number and is dividied into sections for Class A, B, an C network numbers. (See Appendix, Figure A-14.)

3.10.3 Method of Generation

This file is generated weekly using the NIC program INTNUM.EXE.

3.11 NETINFO:ASN.TXT

3.11.1 Purpose

Type = ASCII text

This file contains the information on contacts for every registered 16-bit autonomous system number (ASN). Information included in this file is obtained from ASN registration applications processed by NIC Hostmaster, and from corrections submitted to NIC Hostmaster by ASN administrators. The raw data are stored in the NIC WHOIS database.

3.11.2 Format

Each entry in the file consists of the ASN number and name, followed by the name, NIC WHOIS database handle, mailbox, and phone number of contact for the ASN. The file is organized according to autonomous system number. (See Appendix, Figure A-13.)

3.11.3 Method of Generation

This file is generated weekly using the NIC program INTNUM.EXE.

SECTION 4. ONLINE DISTRIBUTION LISTS

4.1 HADMIN

4.1.1 Purpose

Type = ASCII text

This file contains the online network mailbox of every Host Administrator who has a network mailbox. The file contains entries for MILNET HAs and is used when network messages must be sent to all HAs as a group. Updates to the information included in the file are obtained from NCDs, from responses to the monthly request-for-updates sent by NIC Hostmaster, or voluntarily from the HAs themselves. The data from which the file is generated are stored in the NIC WHOIS data base. The HA distribution list is kept online in PS:<MAIL.DISTRIBUTION>HOST-ADMIN.DIST, and the current version contains 576 entries.

4.1.2 Format

Entries in the file follow the format of a standard TOPS20 online distribution list. The distribution list contains a beginning text line that ends with a colon. When the distribution list online filename is specified at the "TO" prompt by a user who is preparing to send a message, that initial text line is automatically inserted by the message handling system as the "To" field of the message header. Each subsequent line in the file contains a text string consisting of a single online mailbox; each entry line ends with a comma. (See Appendix, Figure A-15.)

4.1.3 Method of Generation

This distribution list is generated weekly using the NIC program DSTLST.EXE.

4.2 NSC

4.2.1 Purpose

Type = ASCII text

This file contains the online network mailbox of every Node Site Coordinator (NSC) who has a network mailbox. The file contains mailboxes for MILNET NSCs and is used when network messages must be sent to all NSCs as a group. The format and method of generation for this list is the same as that of the HA distribution list described above. (See Appendix, Figure A-15.) The NSC distribution list is kept online in PS:<MAIL.DISTRIBUTION>NSC.DIST, and the current version of the list contains 268 entries.

4.3 SECURITY1

4.3.1 Purpose

Type = ASCII text

This file contains the online network mailbox of DCA designated primary points of contact for security related issues. The format and method of generation for this list is the same as that of the HA distribution list described above. (See Appendix, Figure A-15.) The SECURITY1 distribution list is kept online in PS:<MAIL.DISTRIBUTION>SECURITY1.DIST, and the current version of the list contains 13 entries.

4.4 SECURITY2

4.4.1 Purpose

Type = ASCII text

This file contains the online network mailbox of every Host Administrator, Node Site Coordinator, and DDN user interested in receiving security information and who has a network mailbox. DDN Security Bulletins are sent to the members of this list. The format and method of generation for this list is the same as that of the HA distribution list

described above. (See Appendix, Figure A-15.) The SECURITY2 distribution list is kept online in PS:<MAIL.DISTRIBUTION>SECURITY2.DIST, and the current version of the list contains 1,198 entries.

4.5 MGT

4.5.1 Purpose

Type = ASCII text

This distribution list contains the network mailboxes of all HAs and NSCs who have mailboxes, and other selected individuals. The list is used to send notifications of newly issued DDN Management Bulletins. Data included in the list are obtained from NCDs, from responses to monthly request-for-updates sent by NIC Hostmaster, or from individuals who request to be added to the list. The data included in the file are stored in the NIC WHOIS database. The format and method of generation for this list are the same as that of the HA distribution list described above. (See Appendix, Figure A-15.) The MGT distribution list is kept online in PS:<MAIL.DISTRIBUTION>MGT.DIST, and currently contains 1,168 entries.

4.6 DDN-NEWS

4.6.1 Purpose

Type = ASCII text

This file contains the network mailboxes of all HAs, NSCs, and other individuals interested in receiving online copies of the DDN Newsletters. Its format and method of generation are the same as that of the HA distribution list described above. (See Appendix, Figure A-15.) The DDN-NEWS distribution list is kept online in PS:<MAIL.DISTRIBUTION>DDN-NEWS.DIST, and the current version of the list contains 1,265 entries.

4.7 HOST-UPDATES

4.7.1 Purpose

Type = ASCII text

Network mailboxes of all HAs and NSCs are automatically included in this distribution list unless NIC Hostmaster is specifically requested not to do so by the individual. The list includes mailboxes for Internet site representatives as well. Other mailboxes included in the list are those of site technical personnel who have been delegated responsibility for updating local host tables by their HAs. The list is used by NIC Hostmaster to announce the existence of updated host tables. Mailboxes included in the list are obtained from NCDs, from responses to monthly request-for-updates sent by NIC Hostmaster, or from individuals who request to be added to the list. The data included in the file are stored in the NIC WHOIS database. The HOST-UPDATES distribution list is kept online in PS:<HOSTMASTER>HOST-UPDATES.DIST, and the current version contains 829 entries. Its format and method of generation are the same as that of the HA distribution list described above. (See Appendix, Figure A-15.)

4.8 RFC

4.8.1 Purpose

Type = ASCII text

This distribution list is used to send online announcements of newly released Requests for Comments (RFCs) to the internet community. The format of this file is the same as that of the HA distribution list described above. (See Appendix, Figure A-15.) The RFC distribution list is kept online as PS:<MAIL.DISTRIBUTION>RFC.DIST, and the current version of the list contains 637 entries.

4.8.2 Method of Generation

The distribution list is updated manually using a text editor. Additions or deletions to the list are made in response to requests from individuals in the network community.

4.9 TCP/IP

4.9.1 Purpose

Type = ASCII text

This distribution list may be addressed by any person in the internet community who wishes to send pertinent information relating to TCP, IP, and other internet protocols. The list contains the online mailboxes of any person interested in being on the list. It differs from the other NIC-maintained distribution lists in that network users send mail to the entire list of mailboxes by addressing their electronic mail messages to one specific online mailbox, TCP-IP@NIC.DDN.MIL.

The format of this file is the same as that of the HA distribution list described above. (See Appendix, Figure A-15.) The TCP/IP distribution list is kept online as PS:<MAIL.DISTRIBUTION>TCP-IP.DIST. At the time of this writing, the TCP/IP distribution list contains 427 entries.

4.9.2 Method of Generation

The distribution list is updated manually using a text editor. Additions or deletions to the list are made in response to requests from individuals in the network community.

4.10 NAMEDROPPERS

4.10.1 Purpose

Type = ASCII text

This distribution list may also be addressed by any person in the internet community to discuss ideas and issues relevant to the DDN domain naming system. The list contains the online mailboxes of any person interested in being on the list and participating in discussions. Network users send mail to the entire list of mailboxes by addressing their electronic mail messages to one specific online mailbox NAMEDROPPERS@NIC.DDN.MIL.

The format of this file is the same as that of the HA distribution list described above. (See Appendix, Figure A-15.) The NAMEDROPPERS distribution list is kept online as PS:<MAIL.DISTRIBUTION>NAMEDROPPERS.DIST. At the time of this writing, the NAMEDROPPERS distribution list contains 231 entries.

4.10.2 Method of Generation

The NAMEDROPPERS list is manually updated using an online text editor. Additions or deletions to the list are made in response to requests from individuals in the network community.

4.11 ISODE

4.11.1 Purpose

Type = ASCII text

This distribution list may also be addressed by any person in the internet community to discuss ideas and issues relevant to the ISO Development Environment. The list contains the online mailboxes of any person interested in being on the list and participating in discussions. Network users send mail to the entire list of mailboxes by addressing their electronic mail messages to one specific online mailbox ISODE@NIC.DDN.MIL.

The format of this file is the same as that of the HA distribution list described above. (See Appendix, Figure A-15.) The ISODE distribution list is kept online as PS:<MAIL.DISTRIBUTION>ISODE.DIST. At the time of this writing, the ISODE distribution list contains 499 entries.

4.11.2 Method of Generation

The distribution list is updated manually using a text editor. Additions or deletions to the list are made in response to requests from individuals in the network community.

4.12 Protocol Releases and OSD Network Directives

4.12.1 Purpose

Type = ASCII text

There are no standing online distribution lists for the purpose of announcing new protocol specifications, protocol changes, or OSD network directives. Distribution lists for those purposes are compiled as the need arises. The format of the distribution lists, when compiled, would be the same as that of the HA distribution list described above. (See Appendix, Figure A-15.)

4.12.2 Method of Generation

The distribution lists are generated either manually or by program, depending on whose mailboxes are to be included in the lists. If the mailboxes are of users identified in the NIC WHOIS database as members of a group, the list can be generated using the NIC program DSTLST.EXE. If the entries on the list were not identified with a particular group in the NIC database, the distribution list would be compiled manually.

APPENDIX A. EXAMPLES

```
NET : 26.0.0.0 : MILNET :
NET : 128.10.0.0 : PURDUE-CS-EN :
GATEWAY : 26.16.0.3, 192.42.2.2 : GW-GRUNION.NOSC.MIL : VAX-11/750 :
          UNIX : IP/GW,EGP :
HOST : 26.21.0.17 : DDN-CONUS.DDN.MIL,DDN1.DCA.MIL,DDN.DCA.MIL : C/70 :
       UNIX : TCP/TELNET,TCP/FTP,TCP/SMTP,TCP/TIME :
HOST : 192.67.67.20 : NIC.DDN.MIL,SRI-NIC.ARPA : DEC-2060 : TOPS20 :
       TCP/TELNET,TCP/FTP,TCP/SMTP,TCP/TIME,TCP/ECHO,ICMP,UDP/TIME,
       UDP/DOMAIN,TCP/FINGER :
```

Figure A-1: Example of Host Table Entries

```
DOMAIN: 192.67.67.53, 26.3.0.103, 128.9.0.107, 192.33.4.12, 128.8.10.90,
   26.1.0.13, 128.102.16.10, 192.52.195.10, 128.20.1.2, 192.5.25.82 : MIL :
```

Figure A-2: Example of Entries in Domains Table

```
.       IN      SOA     NS.NIC.DDN.MIL. HOSTMASTER.NIC.DDN.MIL. (
                                900423  ;serial
                                1800    ;refresh every 30 minutes
                                300     ;retry every 5 minutes
                                604800  ;expire after a week
                                86400   ;minimum of a day
                                )
                        518400      NS    NS.NIC.DDN.MIL.
NS.NIC.DDN.MIL.         518400      A     192.67.67.53
.                       518400      NS    AOS.BRL.MIL.
AOS.BRL.MIL.            518400      A     128.20.1.2
                        518400      A     192.5.25.82
.                       518400      NS    A.ISI.EDU.
A.ISI.EDU.              518400      A     26.3.0.103
                        518400      A     128.9.0.107
.                       518400      NS    GUNTER-ADAM.AF.MIL.
GUNTER-ADAM.AF.MIL.     518400      A     26.1.0.13
.                       518400      NS    C.NYSER.NET.
C.NYSER.NET.            518400      A     192.33.4.12
.                       518400      NS    TERP.UMD.EDU.
TERP.UMD.EDU.           518400      A     128.8.10.90
.                       518400      NS    NS.NASA.GOV.
NS.NASA.GOV.            518400      A     128.102.16.10
                        518400      A     192.52.195.10
```

Figure A-3: Example of Domain Zone File Entry

```
  HOST NAME                HOST ADDRESS          HOST ADMINSTRATOR

ABERDEEN-IGNET.ARMY.MIL    26.13.0.29            Cogdell, Ervin
   SPONSOR: ARMY       X.25                      (No Mailbox Given)
                                                 Aberdeen Proving Grounds
                                                 Army Ordnance Center and School
                                                 Attn: ATSL-IG
                                                 Aberdeen, MD 21005-5001
                                                 (703) 301-278-2066
                                                 (DSN) 298-2066
HOST : 26.13.0.29 : ABERDEEN-IGNET.ARMY.MIL : CONVERGENT-TECH-CN1000 : CTOS ::

Configuration:      CONVERGENT-TECH-CN1000(CTOS)
```

Figure A-4: Example of Host Administrator File Entry

```
IMPNUMBER/NAME                NET NAME        24 HOUR POC
   NSC NAME                                   [E] = Emergency phone
   ADDRESS                                    [A] = After hours phone
   PHONE                                      [H] = Home phone

      TAC NUMBER              TAC NAME
                              GATEWAY

3  SANDIEGO-NOSC              MIL             (619) 553-2293
   Broersma, Ronald L.  (ron@NOSC.MIL)
   Naval Ocean Systems Center
   Code: 914
   San Diego, CA 92152-5000
   (619) 553-2293 (DSN) 312-553-2293

      26.0.0.3                                SANDIEGO.MT.DDN.MIL
      26.1.0.3, 128.49.16.7                   NOSC-GW.NOSC.MIL
      26.3.0.3, 192.5.65.1                    NPRDC-GW.NAVY.MIL
      26.5.0.3, 128.54.20.1                   SDCSVAX-GW.UCSD.EDU
      26.12.0.3, 192.12.7.1                   SSSD-GW.SSSD.NAVY.MIL
      26.15.0.3, 192.31.63.10                 SCUBED-GW.SCUBED.COM
      26.16.0.3, 192.42.2.2                   GW-GRUNION.NOSC.MIL
```

Figure A-5: Example of NSC File Entry

```
PSN   PSN NAME      O&M          PORT    HOST NAME                  CONNECT TYPE
                                         HOST CONFIGURATION

-------------------------------------------------------------------------------
1     OBERURSEL     ARMY         1       OBERURSEL.MT.DDN.MIL       DH
                                          C/30
                                 3       RHE-EDS.AF.MIL             X.25
                                          PLEXUS-P/60(UNIX SYSTEM V)
                                 6       PCC-OBERSL.ARMY.MIL        X.25
                                          GEAC-8215/PAD(ZOPAL)
                                 7       OBERURSEL-EMH1.ARMY.MIL    X.25
                                          SPERRY-5000/80(UNIX SYSTEM V)
                                 17      OBL-LINK-GW.EUCOM.MIL      X.25
                                          CMC/DRN-3200
```

Figure A-6: Example of Host Configuration File Entry

```
STATE/COUNTRY
   HOST NAME                    HOST ADDRESS       SITE ADDRESS
ALABAMA
   ANNISTON-ASIMS.ARMY.MIL      26.11.0.204        Fort McClellan
                                                   Building 144, Computer Room
                                                   Anniston, AL 36205-5120
```

Figure A-7: Example of Host Location File Entry

```
STATE/COUNTRY
   HOST NAME                    HOST ADDRESS       SITE ADDRESS
                                                   SITE CONTACT
ALABAMA
   ANNISTON.MT.DDN.MIL          26.2.0.113         Anniston Army Depot
                                                   USACC
                                                   Network Control Center
                                                   Building 363
                                                   Anniston, AL 36201
                                                   Cranmer, Ray
                                                   (rcranmer@ANNISTON-EMH1.ARMY.MIL)
                                                   (205) 235-6938 or 235-4195
                                                   (DSN) 571-6938 or 571-4195
```

Figure A-8: Example of TAC Location File Entry

```
  IMPNUMBER NAME
     Coordinator Name          (Network Mailbox)

        Net Address    TAC/HOST/GW Name
                  HostAdmin/Coord Name      (Network Mailbox)

1   OBERURSEL
    Wright, Chief             (nsc-oberursel@EUR.DCA.MIL)

    26.1.0.1      OBERURSEL.MT.DDN.MIL
                  Wright, Chief             (nsc-oberursel@EUR.DCA.MIL)
    26.6.0.1      PCC-OBERSL.ARMY.MIL
                  Burski, Ann               [No Mailbox]
    26.7.0.1      OBERURSEL-EMH1.ARMY.MIL
                  Welch, Richard A          (ASQEXLDOMD01@OBERURSEL-EMH1.ARMY.MIL)
    26.8.0.187, 26.3.0.1      RHE-EDS.AF.MIL
                  Phillips, Richard         [No Mailbox]
    26.17.0.1, 192.42.244.1      OBL-LINK-GW.EUCOM.MIL
                  Steck, Harry H.           (LINKHELP@OBL-LINK.EUCOM.MIL)
```

Figure A-9: Example of PSN-COORD File Entries

```
  HOST NAME              HOST ADDRESS        HOST ADMINSTRATOR
EMMC.DCA.MIL               26.0.0.2             Moore, Richard
                                                (rmoore@FRG.BBN.COM)


PATCH.MT.DDN.MIL           26.1.0.2             See NETINFO:MIL-NSC.TXT
```

Figure A-10: Example of HADMINBYADDR File Entries

```
DOMAIN NAME
  CONTACT:  NAME                MAILBOX                          PHONE

EDU

 Admin: NIC Hostmaster          Hostmaster@NIC.DDN.MIL
                                          (800) 235-3155 (415) 859-3695
 Tech : NIC Hostmaster          Hostmaster@NIC.DDN.MIL
                                          (800) 235-3155 (415) 859-3695
 Zone : NIC Hostmaster          Hostmaster@NIC.DDN.MIL
                                          (800) 235-3155 (415) 859-3695

Berkeley.EDU

 Admin: Henry, Robert W.    rwh@UCBVAX.BERKELEY.EDU     (415) 642-8493
 Tech : Karels, Mike        karels@UCBARPA.BERKELEY.EDU (415) 642-4948
 Zone : Karels, Mike        karels@UCBARPA.BERKELEY.EDU (415) 642-4948
```

Figure A-11: Example of Entries in Domain Contacts File

```
(Top-level domain with no registered subdomains:)

AR
No known domains under this top level domain.

(Top-level domain with numerous registered subdomains:)

  EDU
ACUSD.EDU       ADELPHI.EDU     ALASKA.EDU      ALBANY.EDU      ALFRED.EDU
ALLEG.EDU       AMHERST.EDU     ANDREWS.EDU     APPSTATE.EDU    ARIZONA.EDU
ASC.EDU         ASU.EDU         AUBURN.EDU      AUVM.EDU        BATES.EDU
BAYLOR.EDU      BELOIT.EDU      Berkeley.EDU    BETHEL.EDU      BETHELKS.EDU
BGSU.EDU        BINGHAMTON.EDU  BOWDOIN.EDU     BRADLEY.EDU     BRANDEIS.EDU
  ...(remainder of entry)...
```

Figure A-12: Example of Entries in Domain Information File

```
------------------------------------------------------------------
FILE FORMAT:

ASN Number                          ASN Name
 Contact Name (NIC-identifier)      Contact's Mailbox
  Contact's Phone Number
------------------------------------------------------------------

1                                   The BBN Core Gateways
 Brescia, Michael (MB)              BRESCIA@BBN.COM
   (617) 873-3662

2                                   DCN-AS
 Mills, Dave (DLM1)                 MILLS@HUEY.UDEL.EDU
   (302) 451-8247 (302) 737-9212
```

Figure A-13: Example of ASN File Entries

```
------------------------------------------------------------------
FILE FORMAT:

  Network Number                        Network Name
   Contact Name (NIC-identifier)      Contact's Mailbox
     Contact's Phone Number

------------------------------------------------------------------
Class A Networks
------------------------------------------------------------------

3.rrr.rrr.rrr                       GE-INTERNET
 Bradt, James E. (JEB50)            bradt@CRD.GE.COM
   (518) 387-7170

4.rrr.rrr.rrr                       SATNET
 Blumenthal, Steven H. (SHB)        BLUMENTHAL@BBN.COM
   (617) 873-3197
```

Figure A-14: Example of NETWORK-CONTACTS File Entries

```
Host Administrator distribution:
ACTION@GUNTER-ADAM.AF.MIL,
adamec@BRL.MIL,
Adkins@DOCKMASTER.NCSC.MIL,
adm@ANKARA.AF.MIL,
adm@RAMSTEIN2-EMH.AF.MIL,
...(other entries)...
```

Figure A-15: Sample Format of Distribution Lists