AD-A262 860

REPORT DOCUMENTATION PAGE

Form Approved
OMB No 0704-0188

2. REPORT DATE	3. REPORT TYPE AND DATES COVERED
4-5-93	Draft - Through February, 1993

DDN NEW USER GUIDE - Final Draft Third Edition

5. FUNDING NUMBERS

C-DCA-200-91-D-0014

6. AUTHOR(S)

Barbara Varallo - Editor

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

DDN Network Information Center
Government Systems Incorporated
14200 Park Meadow Drive
Chantilly, VA 22021-2219

8. PERFORMING ORGANIZATION REPORT NUMBER

NIC 60001, February 1993

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)

Defense Technical Information Center
(DTIC) Cameron Station
Alexandria, VA 22314

10. SPONSORING/MONITORING AGENCY REPORT NUMBER

Not Known

11. SUPPLEMENTARY NOTES

First Edition Produced December 1985, Revised November 1987
Second Edition Produced February 1991, Third Edition DRAFT, October 1991
Revised DRAFT, October 1992 Approved February 1993

12a. DISTRIBUTION/AVAILABILITY STATEMENT

Available to DDN Users in hardcopy or online in file NETINFOINUG.DOC

DISTRIBUTION STATEMENT A
Approved for public release
Distribution Unlimited

12b. DISTRIBUTION CODE

13. ABSTRACT (Maximum 200 words)

This document focuses on the MILNET. This DDN New User Guide explains the policies, concepts, and conventions of the DDN, with major emphasis on the MILNET. This guide contains an overview of and a tutorial introduction to the DDN, along with descriptions of its more interesting network programs and services. It is not intended to be a highly technical document, and it does not cover the procedures for attaching hardware, terminals, or other equipment to the network. The DDN New User Guide provides the procedures and guidelines necessary for the beginning user to proficiently use the DDN computer network. Background information includes Network Concepts and terms such as Domain Name System (DNS) and Government Open Systems Interconnection Profile (GOSIP), and gateway concentrators.

93 4 12 002

93-07561

14. SUBJECT TERMS

NIC, TAC, WHOIS, DDN, MILNET, DNS, GOSIP, TELNET, FTP, UNIX, NICNAME, IP NETWORK, POC, RFC.

15. NUMBER OF PAGES

16. PRICE CODE (NTIS ONLY)

17. SECURITY CLASSIFICATION OF REPORT	18. SECURITY CLASSIFICATION OF THIS PAGE	19. SECURITY CLASSIFICATION OF ABSTRACT	20. LIMITATION OF ABSTRACT
UNCLASSIFIED	UNCLASSIFIED	UNCLASSIFIED	SAR

NSN 7540-01-280-5500

Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Std. Z39-18

DDN NEW USER GUIDE

February 1993

Third Edition

Editor:
Barbara Varallo

Prepared by the DDN Network Information Center, Government Systems Incorporated, 14200 Park Meadow Drive, Chantilly, VA 22021-2219. Hardcopies may be obtained from the Defense Technical Information Center (DTIC), Cameron Station, Alexandria, VA 22314.

It is the intent of the DDN Network Information Center (NIC) to make the *DDN New User Guide* widely available to DDN users at minimal cost. It may be obtained in hardcopy or machine-readable form from several sources. Military users may obtain hardcopy from the Defense Technical Information Center (DTIC); DTIC can provide the ordering number. For non-military users—such as contractors, systems personnel, and researchers—who have access to File Transfer Protocol (FTP), copies are available online. The file NETINFO/NUG.DOC contains an ASCII sequential text version. Also, the NIC will make every effort to assist key military DDN Points of Contact (POCs) in providing copies of this Guide to their user communities.

DDN New User Guide. Printed and bound in the United States of America. Published by the DDN Network Information Center, Government Systems Incorporated, 14200 Park Meadow Drive, Chantilly, VA 22021-2219.

First Edition: December 1985

Revised: November 1987

Second Edition: February 1991

Third Edition: DRAFT, October 1991
Revised: DRAFT, October 1992
Approved: February 1993

ACKNOWLEDGEMENTS

The current edition of the *DDN New User Guide* was prepared by the DDN Network Information Center for the Defense Information Systems Agency, Defense Network Systems Organization (DISA DNSO) under contract number DCA 200-91-D-0014.

The NIC wishes to acknowledge the valuable services that the Host Administrators and Node Site Coordinators have provided to the network community and to the development of this guide.

TABLE OF CONTENTS

LIST OF FIGURES

SECTION 1. INTRODUCTION

1.1 Welcome

Welcome to the Defense Data Network, or the DDN, as it is more commonly called. The DDN is a powerful operational military network. It might be thought of as an "umbrella" network composed of several large segments or subnetworks. The unclassified portion of the DDN is a subnetwork known as the MILNET. The MILNET connects the DDN to an even larger network that includes military contractors, universities, and research centers; this entire collection of interconnected networks is called the Internet. Its users number in the millions. It is the MILNET on which this document focuses.

The *DDN New User Guide* explains the policies, concepts, and conventions of the DDN, with major emphasis on the MILNET. The *Guide* contains an overview of and a tutorial introduction to the DDN, along with descriptions of its more interesting network programs and services. It is not intended to be a highly technical document, and it does not cover the procedures for attaching hardware, terminals, or other equipment to the network. This information is provided in other documents [1,2].

Originally, the MILNET was an integral part of the research network known as the ARPANET (after the Advanced Research Projects Agency, which was the sponsor). In 1984, the MILNET and the ARPANET were physically separated, and gateways[1] were installed to allow traffic to be interchanged between the MILNET and the research networks sponsored by DARPA (the Defense Advanced Research Projects Agency). By 1990, the original ARPANET technology had become obsolete, and the ARPANET was discontinued in June of that year.

The DDN affords its users a wealth of services and resources. Many of your colleagues already work on the network, and you will be able to communicate with them quickly and easily even though they may be hundreds of miles away. The DDN also allows you to participate in discussions about topics of interest to you and gives you the opportunity to use network programs and tools to enhance your own capabilities.

Using a computer network is not difficult. However, as with any new tool, using it proficiently requires learning some procedures and guidelines and practicing your new skills. The *DDN New User Guide* will provide the background information necessary to get you started. We hope you find it a useful introduction to the DDN.

1.2 Using This Guide

The *DDN New User Guide* is written for the beginning user and should be supplemented with reading from other sources. Network-specific terms are defined both in context and in the Glossary (Section 11). Throughout the text, references appear in the form "[n]". The bracketed numbers refer to citations in the Bibliography (Section 10), which lists documents containing additional explanatory or background information. Also, check online help systems and the documentation that usually accompanies the network programs you use. (Watch for pointers to online help files when you first access a program or service.) We encourage you to expand your knowledge of the network by consulting these and other information sources whenever you can.

---

[1] Gateways are special computers with the capability of interconnecting networks. Gateways are necessary when routing messages through more than one network.

The *Guide* is divided into sections and subsections, each covering topics of interest to a new user. A summary of the contents of each section follows.

- Section 1 (this section) is a brief introduction to the *Guide*.
- Section 2, The Defense Data Network, describes the structure of the DDN and its administration. It also describes the MILNET and the role of the Defense Network System Organization (DNSO). It provides a brief historical sketch of the evolution of the DDN from the original ARPANET.
- Section 3, Network Connection, describes the ways in which various machines access the network.
- Section 4, DDN TAC Access, describes the procedures for obtaining and using a TAC Access Card and provides detailed procedures for accessing the network through a Terminal Access Controller (TAC) or a Mini-TAC. Also included is background information that will be helpful to TAC and Mini-TAC users, such as common error messages, TAC commands, and instructions for performing file transfers.
- Section 5, Network Use, provides "how-to" instructions for some of the DDN's most useful services, such as electronic mail programs, FTP, and TELNET.
- Section 6, The DDN Network Information Center (NIC), describes in detail the databases, programs, files, documents, and services offered by the NIC.
- Section 7, Security Considerations and Network Conduct, explains the legal and courtesy standards of the network. The importance of host and network security is discussed, and in Section 7.1, the requirements for legitimate access to the DDN are defined. Be sure to read the etiquette section (Section 7.3). Adhering to the guidelines given there will decrease your chances of unwittingly offending other users during your first days on the net.
- Section 8, Network Concepts Overview, provides some background information on terms and concepts that a new user might hear but not understand. This section includes discussions on topics such as the Domain Name System (DNS), network addressing, Government Open Systems Interconnection Profile (GOSIP), and gateway concentrators.
- Section 9, Network Service Centers and Contacts, describes network service providers and how to reach them. The DDN Network Information Center (NIC) is logically the first place to look for information unavailable at the local level. The NIC can help you solve network use problems, locate documents and resources, or identify appropriate points of contact (POCs) for further assistance.
- Sections 10 and 11 are a Bibliography and a Glossary of terms used in this guide.
- The appendices contain information about resources available to network users and answers to some of the questions most often asked by new users.
- A feedback form is located at the back of the *Guide*. We encourage our readers to use the form to make suggestions or point out errors. We value your comments and suggestions and will consider them for future versions of the *DDN New User Guide*. You may also send suggestions online to NIC@NIC.DDN.MIL.

1.3 Document Conventions

This document uses several printing conventions to identify the difference between characters you type (input) and those that a computer prints to your screen (output). These conventions are described below.

Unless otherwise indicated, all user input is terminated by pressing the carriage return or Enter key on your keyboard. (Pressing this key does not cause a visible character to be printed.) In this document, the carriage return or Enter key (↵) is represented as <Return>. Both input and output are characterized by a typewriter-like font to further differentiate them from the surrounding text.

1.3.1 User Input Display

Your input (i.e., the characters you type) is represented in bold typeface:

```
Your input looks like this.
```

1.3.2 Machine Output Display

A non-bold, non-proportional font represents machine prompts, messages, and other output.

```
Machine text looks like this.
```

1.3.3 Comment Display

In examples or instructions, Italics indicate comments we have inserted for further clarification.

Our comments look like this.

1.3.4 Typing Control Characters

In using the network, it may sometimes be necessary for you to type special characters known as control characters. These characters are often represented in documentation by a letter prefixed with the circumflex character "^"—e.g., ^y. When entering these control characters, you must press the control key simultaneously with the desired letter. For example, if you see a "^y" in input instructions, this indicates a control-y, and it means that you should press the control key while you type the letter "y". Throughout this *Guide*, the control key is represented by the circumflex, unless otherwise stated.

This page is left blank intentionally.

SECTION 2. THE DEFENSE DATA NETWORK

2.1 Network Overview

When you access a local computer, you are largely unaware of what kind of link connects your terminal to the computer you wish to use. The terminal seems to be the computer, since it prints or displays what is happening. As you progress in your work, you may need to move data from your local computer onto another computer, or you may wish to send a message to a colleague working on a computer at a distant location. At this point, the usefulness of a communication network becomes apparent.

A communication network is a group of computers joined by data-carrying links. A network may be as small as two or three personal computers tied together by local telephone lines and located in the same building, or it may be a vast complex of computers spread over the world, whose data links include long-haul telephone lines, satellite relays, fiber-optic cables, or radio links. It is also possible for several different networks to be interconnected to form an "internetwork" or "internet."

Everyone is familiar with telephones. Phone sets inside the house connect to outside lines that lead into nearby local or regional telephone exchanges. These exchanges are connected to make up one or more national telephone systems. The national telephone systems communicate with each other to make up an international telephone network. There are also private telephone systems that have their own equipment and are totally separate from the public telephone system.

Computer networks follow a similar pattern. Local area networks (called LANs) may connect computers within a building or in different buildings. A LAN may remain separate, or it may interconnect to regional, national, or worldwide commercial or government networks. Many of these large and small networks are gradually interconnecting through gateways to form a worldwide system of data networks similar to the telephone system. Indeed, since many computer networks use telephone communication lines to carry data from one computer to the next, the two systems are closely interwoven.

You do not need detailed knowledge of this technology to use a network, but you do need to understand the concept of going through layers of equipment and interconnections. Effective network use also requires knowing the online addresses of people or machines with which you wish to communicate and knowing your own network address as well.

The DDN is a special kind of data network known as a packet-switched network. On this network, a terminal or a source host computer (generally just called a host) passes a message along with its destination address to the local Packet Switching Node (PSN)[2] computer. The PSN breaks the message into packets, or smaller chunks of data. Each of these packets has the same destination address and source address as the original message, plus a sequence number indicating which piece of the original message it represents. The packets are passed from PSN to PSN until they reach the destination PSN, where they are reassembled in their original order and delivered to the destination host.

A packet switched network differs from a circuit-switched network in that no predetermined dedicated path exists for delivery of the data. Each packet takes the best route that it can find at the time, and all the packets in a

[2]PSNs were originally known as Interface Message Processors, or IMPs.

message do not necessarily take the same route. Once the packets arrive at the destination PSN, they are reassembled in the correct sequence and delivered to the destination host as a complete message.

2.2 Network Access Methods

The Defense Data Network (DDN) is made up of a variety of equipment. Its users provide terminals, modems, leased circuits to the PSN, and host computers. The DDN supplies node computers, encryption equipment, and some support services. You can reach the network from your terminal in several ways by using different combinations of hardware in conjunction with different network programs. These network connection methods are shown in Figure 2-1.

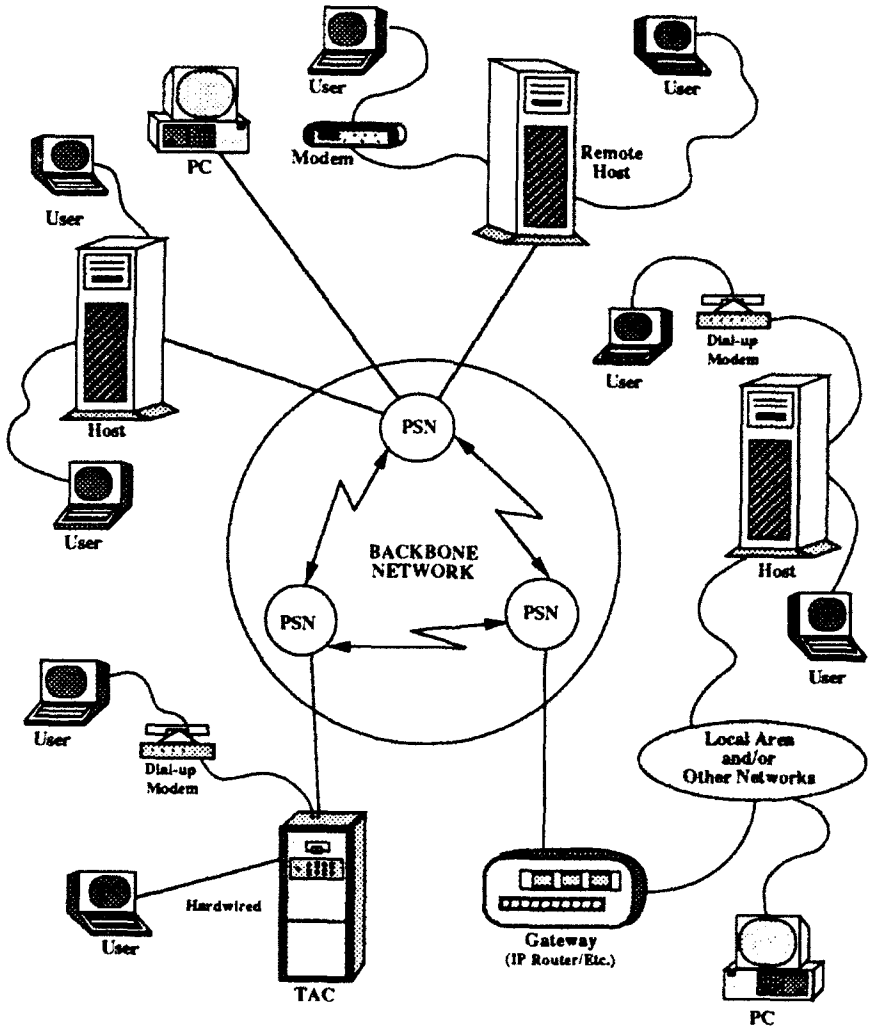


Figure 2-1. Methods of Accessing the Network

A terminal may reach a host in several ways.

- A wire or cable may run directly from the terminal to the computer; this is called a hard-wired terminal.

- A terminal may communicate with a computer via a telephone connected to the terminal through a modem or acoustic coupler; this is called a dial-up terminal.

Dial-up terminals can connect to the network at speeds of from 300 to 9600 bits per second (bps). A speed of 1200 bps is common in the continental United States, while 1200 bps is more common in Europe.

> [NOTE: The speed setting of both your terminal and your modem must be the same to enable the two devices to communicate properly with one another.]

With the appropriate equipment, personal computers may also be used as terminals. In this case, the personal computer emulates (or acts like) a terminal when it is used in terminal mode.

A terminal may be directly attached to a local area network (LAN) or to a local switch (similar to a telephone switch). The user of such a terminal can reach any computer on the LAN or any computer connected to the switch. The LAN may also be connected to the DDN through a gateway, which is a computer whose software can direct traffic from the LAN onto the larger long-haul network and vice versa.

2.3 Organization of the DDN

The Defense Data Network is a large military common-user data communications internetwork operated for the Department of Defense (DoD) by the Defense Network Systems Organization (DNSO) of the Defense Information Systems Agency (DISA).[3] The DDN is made up of several networks. The MILNET is the DDN network that is connected to the Internet.

2.4 Development of the DDN

As mentioned previously, the MILNET is an unclassified military network that is part of the DDN. It was built using technology developed as part of the ARPANET, which was the prototype packet-switched network.

The ARPANET was built by the Defense Advanced Research Projects Agency (DARPA) in 1969 as an experiment to determine the viability of a store-and-forward, host-to-host, packet-switched network. The network designers wanted to demonstrate that computers made by different manufacturers, of different sizes, and running different operating systems, could communicate with one another across a network. It was envisioned that users of such a network could share programs and communicate via the network with other users at distant locations. The experiment was successful, and today many data networks are modeled after the ARPANET.

In 1979, the Department of Defense decided to interconnect several DoD long-haul computer networks through a set of internet protocols so that these networks could share the same backbone of node computers linked by high-speed telephone lines. Protocols are rules or standards by which computers communicate on a network. The ARPANET protocols were developed by researchers known as the Internet Working Group (IWG), under the sponsorship of the DARPA Information Processing Techniques Office (IPTO). The protocols were tested for

[3]Formerly, the Defense Communications System Organization (DCSO) and the Defense Communications Agency (DCA), respectively.

several years on the ARPANET, and they proved useful for creating the networking environment that the DoD wanted.

In 1982, the DoD issued a directive [3] adopting a single set of communications protocols based on the ARPANET protocols. This was followed later in 1982 by a directive [4] to create the DDN as a parent, or umbrella, operational military network made up of several existing or planned DoD computer networks.

By 1983, the ARPANET, which was still considered an experimental network, had grown to over 300 computers, many used for day-to-day operational military purposes as well as for research. Other military users were seeking networking services. To meet this growing need for an operational military network, the DoD evaluated several network architectures and finally chose the DARPA Internet architecture as the model for its common-user communications network, the DDN.

In September 1984, the original ARPANET was split into two separate unclassified networks—a military research and development network (ARPANET) and a military operational communications network (MILNET). The split returned to DARPA a network for experimentation and established an unclassified military network able to accommodate the DoD's growing operational needs.

In June 1990, the ARPANET was officially dissolved. Many sites that were formerly part of the ARPANET are now connected to the National Science Foundation Network, NSFnet. The MILNET remains under the administration of DISA. Plans for upgrading and expanding the current network are now underway. A Defense Research Internet (DRI) will meet defense needs, while the National Research and Education Network (NREN) will provide a national forum for research and education.

2.5 The Defense Information Systems Agency, Defense Network Systems Organization (DISA DNSO)

DISA's Defense Network Systems Organization (DNSO) evolved from the Defense Communications System Organization in 1991 (the same year in which DISA evolved from the Defense Communications Agency). The DNSO handles overall management and operations. It also sets policy guidelines and assists new military subscribers in bringing their computers and related equipment onto the DDN.

The DNSO provides many services to network users and potential network subscribers. It is responsible for

- Keeping the network "up and running,"
- Providing user assistance,
- Setting policies and guidelines,
- Anticipating growth and expansion,
- Assisting new subscribers.

Among its other duties, the DNSO also

- Manages access control and security for the network backbone,
- Designates host and node contacts,
- Coordinates military sponsors,
- Provides technical management of contracts for services, equipment, and software obtained from outside vendors.

To provide operational management support for the DDN, the DISA DNSO has designated a person to act as the primary Point of Contact (POC) for operations for each of the DDN networks. For example, the MILNET Manager is responsible for MILNET operations. One of his/her duties is to approve all host connections to the

MILNET and all changes to such connections. For information about how to contact the current MILNET Manager or any of the other DDN network managers, you may call the DDN Network Information Center. (See Section 6.1.1.)

This page is left blank intentionally.

SECTION 3. NETWORK CONNECTION

3.1 Host Access

To open a connection through the network from one host to another, you must first log in to one of the hosts from a terminal. After logging in, you may open a connection across the network to a second host. Once this connection is established, you may log in to the remote host computer and work there. When you finish and log out of the remote computer, the network connection is closed and you are back where you began—still logged in to the first host. In this way, it is easy to use the resources of more than one computer (assuming that you have a valid account on each system).

The direct host-to-host connection just described is called a TELNET connection. TELNET is a valuable network tool because it lets you use programs and utilities on remote machines that may not be available locally. You may also open a specialized host-to-host link called a file transfer or FTP connection. (FTP is the acronym for File Transfer Protocol.) FTP allows you to copy or transfer files from one host to another. Sections 5.1.2 and 5.1.3 provide specific details for executing host-to-host FTP and TELNET connections.

3.2 TAC Access

Military users can access the DDN by connecting to a Terminal Access Controller, or TAC, and then logging into the TAC by entering a valid Userid and Access Code (password). A TAC allows a wide variety of terminals to communicate directly with any host on the network without going through an intervening host. There are three types of TAC-to-terminal connection:

1. When a wire or cable runs directly from a terminal to a TAC, it is called a *hard-wired* or direct-connect terminal.

2. A terminal may also connect to a TAC through a telephone and modem; this is called a *dial-up* connection.

3. Some terminals are referred to as *dedicated* terminals. These terminals use a point-to-point modem to connect to the network; they are not considered "dial-up" terminals.

After logging into a TAC, you can reach a network host by specifying its host address. You may also establish this type of connection on a Mini-TAC (see Section 4.2.6).

> [NOTE: You must be a registered, authorized user to obtain a TAC Userid and Access Code. See details in Section 4.1.1.]

3.3 Gateway Access

If a computer is attached to a LAN or a non-DDN network, a gateway or concentrator manages communication between the local network and the DDN. The gateway is transparent—that is, you should be unaware that it is there. Some sites do not allow traffic to flow from the DDN to their internal network. In such cases, the gateway exists and is functional, but you must use the gateway host itself to perform any tasks that require access to the DDN (e.g., to establish a TELNET or FTP connection to a DDN host). Electronic mail can travel

over this type of gateway transparently. Ordinarily, you need no special commands or syntax to communicate through a gateway. Figure 2-1 illustrates a gateway connection from a LAN to the DDN, as well as the other connection strategies discussed in this Section.

[NOTE: Because of software limitations, figures are not visible in the ASCII format of the online version of this document.]

3.4 A Word About Personal Computers

Although Personal Computers (PCs) can be attached to the DDN in several ways (including as hosts), at present, *most* personal computers on the DDN are not hosts—that is, they have not implemented the network protocols and are not attached directly to a PSN. Functioning simply as terminals, they have no other capabilities so far as the network is concerned.

Like a terminal, a PC can be connected to a host, Terminal Access Controller (TAC), or Mini-TAC through either a dedicated or a dial-up line. In these cases, the PC needs special software that allows it to imitate a terminal.

Once you have assembled the proper equipment, you must configure the software for your particular system. You will often need to set the following parameters:

speed	The baud rate (in bits per second) at which data is sent and received; usually 1200 baud if your connection is through a dial-up modem. However, 9600 baud dial-up service is currently being introduced. For direct lines, check with your Node Site Coordinator.
data bits	Usually set at 8 (or 7 when accessing the network via a TAC)
stop bits	Usually set at 1
parity	Usually set to "even" or "none"

If these settings do not work, ask local user representatives or host personnel what your system requires. Consult the documentation that accompanies your personal computer, software, and/or modem for details of operation.

Local site representatives should be the first point of contact for PC-related problems. If you have no such representative, contact the Host Administrator for the host you are trying to reach. The NIC may also be able to help with some of the problems you encounter. Check to see if your organization has a PC users group, as other users can be a valuable source of advice. In addition, the network has several general and machine-specific PC interest groups that can provide a broad range of information and answers. (See Appendix A for information on these groups, and see Section 4.2.5 for a discussion of transferring files through a TAC or Mini-TAC to a PC.)

SECTION 4. DDN TAC ACCESS

This section provides information about TAC cards and explains how to use a TAC or Mini-TAC to log on to the network and set it to transfer files. It also provides information on special settings that may be required to allow the TAC/Mini-TAC to transfer files and function more efficiently.

4.1 TAC Card Information

The following paragraphs explain how users are registered to receive TAC cards, what items are printed on a TAC card, and how to get a *TAC Users' Guide*.

4.1.1 TAC User Registration

If you are unable to connect directly to your host computer, you will be issued a TAC Access Card that allows you to access your host via a TAC or Mini-TAC. Whether you are located hundreds or thousands of miles away from the host or right next door, you will need a TAC card only if you cannot access your host directly.

TAC access requires official authorization from a MILNET Host Administrator, as well as the assignment of a unique TAC Userid and Access Code (Password).

After obtaining official authorization, the NIC issues each MILNET TAC user a TAC Access Card containing a Userid and Access Code. The NIC cannot issue a card until it has received approval from the Host Administrator for the user's primary MILNET host (or from the Host Administrator of the gateway to which his primary host is attached).

> [NOTE: If you need a TAC card for a limited time, your Host Administrator can probably issue you a TAC guest card, which is good for up to three months. If you need such temporary access, contact your Host Administrator.]

Regardless of whether you normally use a direct connection to your host, you may need a TAC Access Card if you travel extensively. Because TACs and Mini-TACs are located all over the world, an Access Card allows you to log in when you are out of town without incurring long distance phone charges.

The TAC Access Card contains a Userid and Access Code. This Userid and Access Code are to be used *only* by the person to whom the card is issued. While there is a strict policy of limiting TAC cards to one per person, you may have many DDN host 'ogin accounts, and one TAC card can be used to access any of these accounts. You do not need a TAC card from each host on which you have an account. Any TAC card works on all TACs.

Note that TAC cards are issued to users by individual name only. They are not issued to groups of users or entire offices. This policy applies even when many users share a single login account. Not only is this a security measure, but it also prevents multiple users from losing DDN access when a single card is invalidated.

If you are using a card issued to another DDN user, please notify the person listed as the CONTACT on the card. This is probably your Host Administrator. Inform him/her that you are using an account on his/her host and that you wish to have a TAC card issued in your own name.

4.1.1.1 Users Behind Concentrators

DDN Management Bulletin 76 [5] states that only administrators of hosts that are directly connected to the MILNET can authorize TAC or Mini-TAC Access Cards for their users. Administrators of hosts that are behind concentrators or gateways cannot directly authorize their users for TAC access unless they are delegated that authority by their gateway Host Administrator. Such administrators will need either to transfer jurisdiction over their users to their gateway administrator or to obtain authority from him/her to request TAC access directly. If you are a user or Host Administrator who has questions about this policy, please send a message to

REGISTRAR@NIC.DDN.MIL

or call 1-800-365-DNIC for assistance.

If you access the MILNET via a concentrator/gateway, the name of that concentrator, its address, and its administrator may appear on the HOST, NETADDRESS, and CONTACT lines of your TAC card. You may still use your card to access your primary login account, even if it is on another host; however, you must know the network address of your primary host. The administrator of your primary host can tell you its address. You must know this address when you log into a TAC and when you request help with a TAC login problem.

4.1.2 TAC Card Example

Figure 4-1 is a sample of the left portion of a DDN TAC Access Card. To help you understand the information on the TAC card, we have identified what each information item represents.

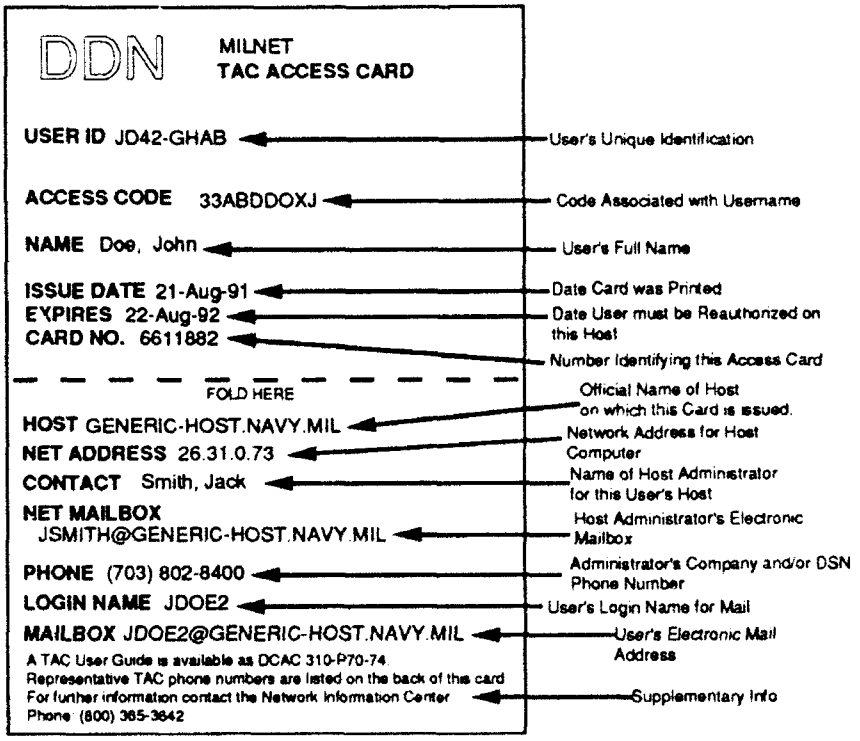


Figure 4-1. TAC Card Example

TAC cards are perforated and include instructions to "detach here" and "fold here," allowing you to reduce the size of the card so that you may insert it in a wallet or credit card case.

> **WARNING!!** Do not laminate your TAC Card. Because of NIC printing requirements, blank cards are enclosed within carbon-coated envelopes. This carbon material fades very quickly when placed in plastic envelopes or when permanently laminated. This phenomenon also extends to the placement of transparent tape over the print. If you wish to preserve or darken the information printed on your card, we recommend that you use a ballpoint pen to rewrite it just above or below the appropriate item.

The most important information on the right-hand portion of your TAC card is your mailing address. However, the NIC includes its toll-free User Assistance Hotline number on this section of the card in case you lose the left half. In addition to the hotline number, the top of the card contains a brief set of user guidelines. As an authorized TAC or Mini-TAC user, you are expected to comply with these guidelines. If you find yourself in the position of sharing a TAC Access Card with other users, please notify your Host Administrator and request a TAC card for each individual.

4.1.2.1 Common TAC Card Userid/Access-Code Input Errors

Just below the guidelines section is a key that shows how each printed character appears on a TAC card. The statement, "Access codes never contain a one, zero, 'Q' or 'Z'" follows. Remember that these characters are invalid *only* in Access Codes and *not* in Userids. If you find that the TAC or Mini-TAC is returning a "Bad Login" error message during your first attempts to log in, check to see if you are typing one of these invalid characters. For example, if you're typing a zero, try the letter O (oscar). If you're typing a Q (quebec), try the letter G (golf) instead. Use the key to compare the printed characters. Be aware that other character can also be similar. For instance, the 8 (eight) sometimes looks like a B (bravo), and the S (sierra) sometimes looks like a 5 (five). TAC card Userids and Access Codes are not case-sensitive, i.e., you can enter them in either uppercase or lowercase letters.

If you have any questions about reading or using your TAC access card, call the NIC for assistance at 1-800-365-DNIC.

4.1.3 Obtaining the *TAC Users' Guide*

The paragraph in fine print at the bottom of your TAC card alerts you that further, more comprehensive information is available to you. Upon written request, you can obtain the *TAC Users' Guide* from the Defense Information Systems Agency (DISA). This document is geared toward users who are interested in learning some of the finer points of TAC usage.

To order the *TAC Users' Guide*, send a note specifying its title and DCAC 310-P70-74 to the following address:

> Defense Information Systems Agency
> Attn: Code BIAR
> 701 S. Courthouse Road
> Arlington, VA 22204-2199

4.2 TAC Login Procedures

This section discusses how to use a TAC or Mini-TAC to log in to the DDN. It also describes how to connect to a TAC or Mini-TAC, lists some common TAC/Mini-TAC error messages, and presents information about transferring files through a TAC to a PC.

4.2.1 Connecting to a TAC or Mini-TAC

The following paragraphs explain the various ways in which you can connect to a TAC or a Mini-TAC.

4.2.1.1 Dial-up TACs

To connect to a TAC/Mini-TAC using the telephone system, follow the general procedures described here. Because the exact steps required to dial the TAC/Mini-TAC depend on your local hardware setup, check with local site representatives for details.

You may obtain the number of the nearest TAC/Mini-TAC directly from the network by using the TACNEWS service (see Section 6.3.3) or by calling the NIC at 1-800-365-DNIC. You can look up the phone number of a specific TAC/Mini-TAC via the NIC WHOIS service (see Section 6.3.1). In addition, many TAC/Mini-TAC phone numbers are listed on the back of your TAC Access Card.

4.2.1.2 Using a Terminal with an Acoustic Coupler

To use an acoustic coupler, first dial the TAC/Mini-TAC number on a telephone and listen for the dial tone. When you hear the tone, put the telephone handset into the indicated position on the coupler cuffs.

4.2.1.3 Using a Dial-up Modem

A dial-up modem will be wired to your telephone and to your terminal. (Consult the instructions that come with the modem to attach it to your terminal and set it properly.) Begin by dialling the TAC/Mini-TAC number on the telephone. Then, wait for the tone, switch the modem from "voice" to "data," and set the handset back on the telephone cradle. Note that the speed of the terminal must match the speed of the modem. Also note that some modems are "smart"—that is, you will not have to use the telephone to dial the number. Instead, you will type some instructions to your terminal, such as "DIAL5551212" or "ATDT9,18003682227." The modem will then dial the number as instructed and make the connection for you. See your modem instruction manual for exact details.

4.2.1.4 Using a PC and Communications Software

To access a TAC/Mini-TAC, you can use one of the popular communications software packages such as Procomm® or the Xmodem protocol. These programs often enable the PC to dial the TAC/Mini-TAC, open the host connection, and enter your Userid and Access Code automatically. If you use such a package, be sure you know how to dial the TAC/Mini-TAC by hand in case there are problems with the script or the equipment. It is also useful to know the address of the host you connect to and how to alter the script when changes are made to the network. Finally, for security reasons, you should enter your Userid and Access Code manually when logging in rather than including this information within the access script.

4.2.1.5 Hard-Wired TAC Connections

If you are to connect to a host via a hard-wired TAC connection, you will need to consult a local user representative or Node Site Coordinator to learn the procedure for getting to the TAC/Mini-TAC. The procedure will vary depending upon what equipment is used and how it is configured at your location.

4.2.2 TAC Login

After you have successfully connected to a TAC/Mini-TAC, you must supply a "wake-up" character to alert the TAC to your presence. Do this by holding down the <Control> key and typing the letter Q on your keyboard (^Q). The TAC/Mini-TAC should respond with a banner—often a message from the MILNET Monitoring Center. If you are dialing into a TAC modem capable of 9600 bps, enter a <Return> character instead of a ^Q. If you are unsure of the modem type at the TAC, try both characters.

Once the TAC banner is displayed on your screen, you can begin the process of logging into the TAC/Mini-TAC and connecting to a remote host.

Following is a sample scenario showing how to log in to a TAC/Mini-TAC.

```
CONNECT 1200                          After user dials or otherwise connects to the TAC/Mini-
                                      TAC, the modem may print a message similar to this.

^q                                    To alert the TAC/Mini-TAC, the user types a control-q.
                                      (It will not appear on the screen.)

FOR OFFICIAL USE ONLY                 The TAC responds; the user opens a host connection by
NIC 1-800-365-DNIC                    typing "@o" for open and entering the host address in
29 TAC 114 #:20                       dot notation format.
@o 192.112.37.10

TAC Userid:  NIC-GUEST                The TAC prompts for Userid and Access Code, and the
Access Code:                          user enters the data. The Access Code does not echo.

Login OK                              The connection is opened and NIC displays information.
TCP Trying...Open
* -- DDN Network Information Center --
*
* For TAC news, type:                        TACNEWS <return>
* For user and host information, type:       WHOIS <return>
* For NIC information, type:                 NIC <return>
*
* For user assistance, call (800) 365-3642 or (800) 365-DNIC or
                                                 (703) 802-4535
* Please report system problems to ACTION@NIC.DDN.MIL.

NIC, SunOS Release 4.1.1 (NIC) #1:
Cmdinter Ver 1.2 Wed Apr 8 11:18:20 1992 EST
@. . .
        User works on the host and logs off when finished.
        When disconnected from the host, user returns to the TAC command level.

@l                                    User types "@l" to log off the TAC/Mini-TAC and the
Logged out                            TAC confirms.
```

For more detailed instructions on using a TAC/Mini-TAC and setting terminal parameters, consult the *TAC Users' Guide* [1].

When you enter your TAC Userid and Access Code, remember the following:

- <Return> terminates each input line and causes the next prompt to appear.
- It doesn't matter whether you type your TAC Userid and Access Code in uppercase or lowercase letters.
- For security reasons, your Access Code input is not echoed or it is obscured from view with strikeover characters.
- If you make a mistake, try using the backspace key (^H) to delete a single character. Use ^U to delete an entire line. Although these commands do not work on every keyboard, they often do.
- If you make a mistake while entering either your TAC Userid or Access Code, type ^C to abort the login process and return to the TAC command mode. Then try again.
- Sometimes the TAC/Mini-TAC is unable to reach the requested host address. To tell the TAC/Mini-TAC to stop making connection attempts, issue a close command:

```
@c <Return>
Closed.
```

- As long as you have an open connection to a host, you remain logged in to the TAC/Mini-TAC. If you close the connection to the host or the connection is shut down for any reason, you are given ten minutes to open another connection with no further login to the TAC/Mini-TAC. If you do not open another connection within ten minutes, the TAC attempts to hang up your connection and automatically log you out. To open another connection, simply type the "open" command again and supply another host address, as in the example below:

```
@o 128.1.0.1 <Return>
```

4.2.3 Common TAC Login Problems

This section covers only TAC login problems. Problems specific to the Mini-TAC will be covered in a future revision of this document.

The TAC issues an error message when it does not receive the expected input. Some of the most common error messages are presented in this section, along with suggestions about what to do if you see one.

The TAC sends two kinds of messages. The first deals with errors in the TAC login process; the second deals with difficulties in opening a connection to the destination host.

4.2.3.1 TAC Login Error Messages

You may see one of the following error messages if you have problems logging in to a TAC Each message is accompanied by a brief explanation of its cause and suggestions for further action.

BAD LOGIN

This message means that the combination of Userid and Access Code you entered is invalid. Examine your TAC Access Card carefully to be sure you are typing the correct characters and that you are not using any of the characters that are invalid in an Access Code Note that Access Codes never contain a zero (0), a one (1), a Q (quebec), or a Z (zulu), since each of these characters may easily be mistaken for another. If your Access Code appears to contain one of these characters, it may be the letter O (oscar), the letter L (lima), the letter G (golf), or the number 2 (two).

This message is also displayed if you are using an expired or invalid TAC card. If you are sure you are typing correctly and suspect you are using a bad card, contact the NIC at 1-800-365-DNIC, and they can determine the validity of your card.

BAD

This message means you typed a string that is not a valid TAC command, and the TAC does not understand your input. Either you typed something incorrectly or there was some interference on your connection. Frequently, simply repeating the command corrects the problem. However, if repeating your input causes another error message, check to make sure that you understand the command you meant to type and that your input is in an acceptable format.

NUM

This message means that the TAC was expecting you to type a number, but you typed some other character. The message is displayed if you type the letter O (oscar) as part of the address of the host you are trying to connect to, or if you omit the numeric host address after typing @o (for open). Make sure that you are not typing letters in places you should be typing numbers; this will probably correct the problem.

WAIT

The TAC displays this message while it is attempting to validate your Userid and Access Code.

NO CARRIER

This message comes from your PC or modem. If this message is displayed on your initial attempt to dial the TAC/Mini-TAC, it means that the TAC/Mini-TAC did not answer the phone. This could be because of a power failure or other emergency at the site where the TAC/Mini-TAC is located, or it could be the result of a mis-dialed telephone number. Try calling the number with a telephone that is not connected to your terminal and see if your get a busy signal or other recording from the telephone company.

If this message appears after you have logged in and while you are working on the host, it means that something happened to disconnect your modem from the TAC/Mini-TAC. Try dialing the TAC/Mini-TAC again. If the problem persists, contact your site systems representative to check your modem, or call the Monitoring Center for your area to check the TAC/Mini-TAC.

4.2.3.2 Host Connection Errors

Host connection error messages are sent when you have successfully logged in to the TAC and while the TAC is trying to connect to the host you specified. You know that you have successfully logged in to the TAC when you see the "Login OK, TCP trying..." message.

DESTINATION HOST DEAD

This message means that the remote host is physically powered off or the cable to the network has been removed. The host is "down." Since host down-times are normally relatively short, wait a while and try to log in again. If the host remains unavailable, call the Host Administrator for the destination host and ask when the system will be available again. If you do not know the Host Administrator's phone number, the NIC can provide it or the name and number of the coordinator of the network to which the host is attached. This information can also be found by querying the NIC's WHOIS database.

DESTINATION HOST UNREACHABLE
DESTINATION NET UNREACHABLE
HOST NOT RESPONDING

Several network conditions can cause these messages. They may be displayed if the host or its PSN is down or if a gateway between the TAC and the host is down. Also, check to ensure that you specified the correct host address. Typing a nonexistent network address will cause such a message to be generated. If the condition persists, call the NIC for assistance.

4.2.4 Changing the TAC Intercept Character

The "@" sign is the default TAC intercept character. The intercept character is the character that signals the TAC to interpret any character(s) that follow immediately as TAC commands rather than passing them through to the network.

However, once you have connected to your host, you may want to send an @ directly through to the network—for example, when you type a DDN mail address. To make the TAC pass the @ on to the host rather than intercepting it, you must type @ twice—i.e., **@@**. When you do this, the TAC intercepts the first "@", transmits the second "@" to the host, and echoes that one back to you. You will see @@@ on your screen. Remember, when you want to type an "@" for anything other than a TAC command, you must type it twice. For example, to send a message to auser@milhost, you would have to type

```
auser@@milhost
```

and on your screen you would see

```
auser@@@milhost
```

To change the TAC intercept character, you must type **@i** (for intercept) followed by the decimal value of the ASCII code of the character you wish to use in place of the @. The *TAC Users' Guide* contains a list of ASCII codes. For purposes of text file transfers, we recommend that you change the intercept to a non-printing character, such as a control character. For example, to change the intercept character to control-y (^y), type the following:

```
@i 25 <Return>
```

(Be sure to insert a space between the @i and the ASCII code number.) After you change the intercept character, you must use the new character for all subsequent TAC commands. To return to the default TAC intercept character (the "@" sign) after changing it to ^y, type the following:

```
^yi e <Return>
```

where "i e" stands for *intercept escape.*

4.2.5 Using a TAC for File Transfer

This section presents several TAC command procedures that may facilitate file transfers through a TAC. The procedures covered here are

- Changing the TAC intercept character,
- Setting flow control on the TAC,
- Putting the TAC into binary mode.

4.2.5.1 Changing the Intercept Character

For executing file transfers, you may want to change the TAC intercept character to one that your file transfer program does not use. For example, the Kermit file transfer program uses the "@" (discussed in a subsequent section). To change the intercept character, follow the directions in Section 4.2.4 above.

4.2.5.2 Setting Flow Control on the TAC

Setting flow control on the TAC ensures that data will not be transferred at a rate that causes the TAC buffers to overflow. The example below assumes that you have changed the TAC intercept character to ^y. (The ^y characters are shown in the examples, but they will not display on your screen as you type them on your keyboard.)

```
^yd c a <Return>
^yf i s <Return>
^yf o s <Return>
```

where

^yd c a = device code ASCII, which clears any previously set flow control as well as any padding and parity. Flow control is incompatible with padding and parity.

^yf i s = flow control input start, which enables flow control so that the terminal sending data will not send it faster than the TAC can handle it.

`^yf o s` = flow control output start, which disables flow control from the TAC to the terminal.

4.2.5.3 Putting the TAC in Binary Mode

To transfer binary files over the network, you must first put the TAC into binary mode. Doing so disables the TAC intercept character. You must disable the intercept character because if the TAC receives what it considers to be an intercept character—even though the character is embedded in a file—it interrupts the transfer process and tries to interpret whatever follows the intercept as a command.

To put the TAC in binary mode, first open a connection to your host. After establishing the host connection, put the TAC in binary mode with the commands shown below. (Here again, the example assumes you have changed the intercept character to ^y.) The commands **must** be typed in the order shown, because if you start binary input before you initiate binary output, the TAC will ignore the "^yb o s command" and treat it simply as a character string to transmit over the network.

```
^yb o s <Return>
^yb i s <Return>
```

where

`^yb o s` = binary output start, which enables 8-bit binary output mode from the TAC.

`^yb i s` = binary input start, which enables 8-bit binary input mode to the TAC.

Logging out of your host returns the TAC to non-binary mode, re-enabling local control with @ commands. This is the only way to reset the TAC from binary to non-binary mode (short of hanging up or disconnecting from the TAC itself).

4.2.6 A Brief Word About Mini-TACs

Mini-TACS are new and improved DDN access controllers similar to the TACs currently in use. As with the original TACs, Mini-TACs provide DDN access to network users who are geographically distant from their host computers. When a user dials a local or toll-free phone number and types the required series of commands, it opens a long-distance connection to the user's host computer.

TACs support up to 63 asynchronous user ports. The smaller, more compact Mini-TAC can handle only 16 asynchronous terminal connections, but it has other capabilities (i.e., synchronous terminals, HFEP, etc.). Both TACs and Mini-TACs allow normally incompatible terminals and hosts to communicate with one another using the DDN as the go-between. While both types of access controllers serve similar roles, the Mini-TACs provide more advanced operational and security features.

Like a TAC, the Mini-TAC returns error messages to its users if it cannot understand a command. Currently, from a user standpoint, the Mini-TACs and the TACs are essentially the same. If you notice any difference in behavior between TACs and Mini-TACs and you need assistance, call the MILNET Monitoring Center or the NIC. At present, some TAC commands can be abbreviated to one character. However, in the future, Mini-TAC commands may need to be a least two characters long to ensure that they are differentiated from other commands starting with the same letters.

SECTION 5. NETWORK USE

A computer attached to the DDN can reach a large community of users and access a wide variety of software. Research tools, documents, files, and mailing lists are all readily accessible through the DDN. This section describes the procedures for using these network tools, three of which are major network services: electronic mail, file transfer (FTP), and remote login (TELNET). These services are integral to the DDN protocols and are offered by all hosts that have implemented the full set of network protocols.

Although the functionality of the services discussed here is the same on every host, what the user sees may differ from host to host because software is often customized to suit the host operating system. For this reason, it is important to read local online and hard-copy documentation and to consult online help files for specific details on using these services on your host. Check with your local Host Administrator or site systems representative if you need more information. The sections below provide generic instructions for using electronic mail, FTP, and TELNET.

5.1 Electronic Mail

The DDN capability that is used more often than any other is electronic mail. Electronic mail lets users send messages to one another over the network. System programs accept and store mail messages from users on other hosts that are directed to local users. These programs automatically recognize the incoming traffic as electronic mail, translate it to a format compatible with the receiving mail program, and direct the messages to the correct recipients. Most users have an online mail file where all messages addressed to them are stored.

You can print, read, or delete your mail using the local mail program. However, you should not edit or alter the structure of your mail file except through a mail program, as each message has unique characteristics that identify it as mail, such as a header, a character count, and a time stamp. Editing the mail file directly may alter these characteristics so that the mail program no longer recognizes the data as mail.

Host computers usually provide one or more programs for reading and sending mail. Most mail programs provide you with the following capabilities:

- Reading messages

  All mail programs have a command that allows you to read messages received over the network. Mail programs normally offer options for selecting and displaying specific messages from those received and stored in your mailbox.

- Printing, deleting, or moving messages

  With your local mail program, you can print your messages (if a printer is available), move them into other (editable) files, or delete them. It is important that you learn how to delete or move messages after reading them; otherwise, your mail file may overflow and prevent additional mail from being delivered.

- Sending messages

  You can send messages to other users on your own host or to anyone on the network that has a mail service. No passwords are required to send mail, but you must know the network mailbox, or address, of the person to whom you are sending mail. Network mailboxes usually take the form

  USERNAME@HOSTNAME.DOMAIN

  e.g., SMITH@NIC.DDN.MIL.

Mail that is transmitted over the DDN normally requires a network address made up of a username and a hostname. Occasionally, you can omit the hostname. For example, if you are sending a message to a user on the same host as the one you are using (your local host), you need not include the hostname. This is similar to sending an interoffice memo, which rarely needs a full name and address to reach its destination. On the other hand, a message sent to "John Smith, U.S.A" has little chance of being delivered without more information. The same is true of electronic messages without a valid address. Any message with an incomplete or incorrect address is returned to the sender with an error message. If a mail message is undeliverable due to network or machine problems, most mail programs try to resend it several times before returning it to the sender.

Many mail programs allow you to use a local text editor to revise or correct the text of the message you are preparing. The mail programs themselves usually have simple editing features that allow you to delete a character, word, or line, or to make simple corrections. An entire file may be sent as the text of a message, assuming the file is not too large. Many mailers outside the DDN truncate or discard messages that are longer than 50,000 characters in size, envelope and header data included. It is usually safer to limit the size of your messages to ensure reliable delivery.

Following are examples of some typical procedures for sending and reading mail and for getting help within a network mail program. These are general scenarios; your host may run a different program or implementation than the ones shown. Only the bare essentials for using these mail programs are included here. We urge you to read the manuals for your mail system and to explore the online help facilities to expand your knowledge of what your implementation has to offer.

In the examples that follow, note that the prompt character consistently indicates what operating system or program you are dealing with currently, and that the prompt character changes as you progress from one program to another.

[**NOTE**: Computer names, user names, electronic addresses, and other data used in examples throughout this manual are not intended to represent currently valid input/output—i.e., some of the data may be "ficticious" but the format is accurate.]

5.1.1 UNIX MAIL Examples

Sending Mail Via UNIX

[NOTE: UNIX is case-sensitive. Most UNIX systems require that commands be entered in lowercase.]

%mail nic@nic.ddn.mil <Return>	*User asks to send mail to a well-known mailbox. The percent sign (%) is a standard UNIX system prompt, while "mail" is the command that invokes the Mail program. User must insert a space before typing the message address on the same line.*
Subject: **How to get RFCs <Return>**	*The Mail program prompts for message subject, and the user supplies it.*
How do I retrieve RFCs using the electronic mail utility? Thanks for your help. <Return> ^d	*The user types the message text, ending with a control-d (^d) in the first character space of a line.*
%	*UNIX prompt returns.*

Reading UNIX MAIL

% mail <Return>	*User invokes the Mail program at the UNIX prompt.*
You have mail.	*The Mail program announces that there is mail waiting in the user's mailbox and prints the headers of messages received since user last checked his mail.*
New mail: 1) 16/Dec SMITH@ISI.EDU (292) Where is RFC 212? 2) 17/Dec JONES@NIC.DDN.MIL (115) Re: RFC 212 3) Etc...	
& **p 1 <Return>**	*Mail prompt (&) is presented, and user asks the Mail program to print message 1 (p 1). The full message text will be printed on the user's screen.*

Getting Help for UNIX MAIL

Typing

% **man mail**	connects you to the online Mail manual.
& **help**	displays help for Mail users.
& **?**	displays a list of Mail commands.

5.1.2 InfoMail Examples

Sending a Message Via InfoMail®

[NOTE: Since InfoMail runs under the UNIX operating system, and UNIX is case sensitive, InfoMail commands must normally be entered in lowercase.]

DDN1->**infomail <Return>**	*User invokes the InfoMail program at his local system prompt.*
InfoMail -- Version 0.3x Username: **code123 <Return>** Password: **<no echo> <Return>**	*The InfoMail banner is displayed, and user is asked to log in with his mail username and password.*
--> **compose <Return>**	*At the InfoMail prompt, the user asks to create a message ("compose").*
To: **command@ddn2.dca.mil <Return>** From: CODE123@DDN1.DCA.MIL	*InfoMail prompts for address of recipient and automatically supplies user's address on "From" line.*
Subject: **Dial-ups <Return>** Date: 12 July 1992	*InfoMail prompts for subject, and user enters the subject of the message. InfoMail automatically supplies the current date.*
Text: **Request dial-ups for our site. Usage demand is up.** .	*InfoMail prompts for text, and user enters, terminating the text with a carriage return, a period in the first space of the next line, and another carriage return.*
--> **quit <Return>** DDN1->	*User types "quit" to exit from InfoMail. The local system prompt returns.*

Reading Mail with InfoMail

```
DDN2->infomail <Return>                          User invokes the InfoMail program at his
                                                 local system prompt.

InfoMail -- Version 0.3x                         The InfoMail banner is displayed, and
Username: COMMAND <Return>                       user is asked to log in with his mail
Password: <no echo> <Return>                     username and password. These may be
                                                 entered in either upper or lowercase.
                                                 After a successful login, InfoMail notifies
                                                 user of mail in his "Inbox."

INBOX.
   1  FROM:  CODEB999 / SUBJECT: DIAL-UPS / 13 Jul
   2  FROM:  AF@DDN.A / SUBJECT: SCHEDULE / 14 Jul

--> next <Return>                                At the InfoMail prompt, user issues a
                                                 command to display the next message,
                                                 and InfoMail does so.

To: COMMAND@DDN2.DCA.MIL
From: CODE123@DDN1.DCA.MIL
Subject:  Dial-ups
Date: 13 July 1992
Text:
Request dial-ups for our site.  Usage demand is up.

--------------------END OF DOCUMENT----------------------

--> next <Return>                                User types "next" to ask for the next
                                                 message.

To: COMMAND@DDN2.DCA.MIL
From: AF@DDN1.DCA.MIL
Subject:  SCHEDULE
Date: 14 July 1992
Text:
What is the schedule for the next InfoMail demo?

--------------------END OF DOCUMENT----------------------

--> quit <Return>                                User types "quit"to exit from the
                                                 InfoMail program.
```

Getting Help for InfoMail

Typing

`-->?`	Prints a list of all the commands that can be issued at this stage of the Mail procedure.
`--><commandname> ?`	Lists possible input for completing the specified command.
`-->describe <commandname>`	Tells what the specified command does and how to use it.
`-->example <commandname>`	Prints an example of the specified command.

InfoMail manuals are available from

BBN Communications Division
10 Moulton Street
Cambridge, MA 02238

5.2 File Transfer Protocol (FTP)

FTP is a protocol that enables you to move a file from one computer to another—even if the computers have different operating systems and file storage formats. You can move data files, programs, text files, and/or anything that can be stored online.

To use FTP, you must know the hostname or the network address of the remote host. You must also have an authorized username and password on the remote host system, and you must know the name of the file you want to retrieve from or send to that system. You can then copy files either to or from the remote system. Not every file, however, can be FTP'd. Only those files that have public "read access" (i.e., a file protection designation that permits transfers) can be transferred from one system to another.

Some hosts provide the username "anonymous" for FTP file retrieval from their systems; this is called the "anonymous login convention." Any character string is accepted as a password for an anonymous login. An anonymous login account works *only* with FTP. It is not an account that can be accessed for general use. Normally, you cannot use the anonymous convention to *send* files to a remote host, as this requires a specific login account on that host; you may only use it to transfer files to your local workspace from a host on which you do not have a login account. However, some hosts now provide public directories where you can send files as well as retrieve them.

These are the general steps used for a file transfer procedure:

1. Log in to your local host and invoke the FTP program.
2. Provide the hostname or network address for the remote system.
3. When you have successfully established a connection to the remote host, log in with your authorized username and password on that system.
4. Issue commands to send or retrieve files.
5. When you are finished, log off the remote host and exit from the FTP program.

Depending on the FTP implementations on your host and on the remote host, it may be possible to display a directory listing of the public files on the remote host and to request remote system status information.

As you will see from the examples, when you transfer a file with FTP, messages regarding the status of the action you have requested are displayed throughout the process. The FTP server on the remote host sends the File Transfer messages. These messages generally have the following characteristics:

- Every FTP command generates at least one reply.
- A reply consists of a three-digit return code, followed by a line of text describing the response.

- If a single line of text accompanies the return code, a single space separates the code from the text.

- If more than one line accompanies the return code, a hyphen (-) separates the code from the text.

During a File Transfer session, you enter a command and then wait for a message indicating whether the command was accepted. Further system messages describe the outcome of any transfer you may request. The text that accompanies the FTP return codes may differ slightly from server to server, but the general meaning of the numeric codes remains constant.

Programs based on the FTP protocol vary a great deal in implementation details. The examples provided here should be taken only as guidelines. Consult your local system representatives for assistance with the FTP implementation on your host.

Before you begin a File Transfer session, it is best to become familiar with the general command sequence.

An example of an FTP session conducted between two UNIX systems appears on the next page. In the example, a user carries out several standard FTP procedures, such as asking for a directory listing of the public files on the remote system and then changing to another directory. Remember that the commands to accomplish these tasks may vary from host to host, and not all host FTP servers implement all commands.

5.2.1 Transferring a File on a UNIX System

In the following example, both hosts are running UNIX.

```
abacus-1>ftp fs3.nisc.nic.com <Return>
Connected to FS3.NISC.NIC.COM
```

User invokes the FTP program at his local system prompt, and the remote FTP server responds by displaying its banner and requesting a login, as shown below.

```
220 fs3 FTP server (NIC Version x.xx ... Wed July 17 16:20:33 EDT) ready.
Name (fs3.nisc.nic.com:barbv): anonymous <Return>
331 Guest login ok, send ident as password.
Password: guest <Return> (no echo)
230 Guest login ok, access restrictions apply.
ftp>ls <Return>
200 PORT command successful.
150 Opening ASCII mode data connection for
    file list.
etc
pub
netinfo
INDEX
ls-lR
226 Transfer complete.
47 bytes received in 0.02secs (2.3 Kbytes/sec)
```

After successfully logging in as "anonymous guest," the user asks for a directory listing of public files at the FTP prompt. FTP responds, printing messages regarding the transfer.

```
ftp>cd netinfo <Return>
250 CWD command successful.
ftp>ls <Return>
200 PORT command successful.
```

At the FTP prompt, user issues a command to change to the netinfo directory, then asks for a listing of files in the new working directory (netinfo).

```
150 Opening ASCII mode data connection for file list.
interest-groups
domains
nsfnet.policy
226 Transfer complete.
125 bytes received in 0.04. seconds (3.1 Kbytes/s)
ftp> get nsfnet.policy <Return>
```

User asks for a transfer of the specified file to his own file system. Since he does not specify a new filename, the file retains the same name on the local system.

```
200 PORT command successful.
150 Opening ASCII mode data connection for nsfnet.policy (2790 bytes).
226 Transfer complete.
local: nsfnet.policy   remote: nsfnet.policy
2847 bytes received in 0.12 seconds (23 Kbytes/s)
ftp> quit <Return>
abacus-2>
```

User types "quit"to exit from the FTP program. The local system prompt is displayed again.

5.2.2 How to FTP a Directory Listing

The example that follows demonstrates how to retrieve a list of file names from a public directory. (Not all hosts provide this feature; check with the online help system or your local user support representative.) In the example, the user is logged on to a host running the UNIX operating system. He uses FTP to connect to the host NIC.DDN.MIL, then logs in under username "anonymous" and password "guest." He enters the "**dir**" (directory) command for the directory "**RFC**" to see the names of accessible files. (Because the actual directory list is long, only the first few files and the last file are shown in the example.)

After the directory listing is displayed, the user can copy a file or files from the remote host directory, but this procedure is not included in the example. He issues the FTP command "**bye**" to exit from the program and close the connection to the remote host, which returns him to the local host operating system.

```
% ftp <Return>

FTP> nic.ddn.mil <Return>

(Assuming 36-bit connections, paged transfers)
                                <NIC.DDN.MIL FTP Server Process...

FTP> login anonymous <Return>

Password: guest <Return>

<User ANONYMOUS logged in at Thurs 7-Aug-92  14:14 EDT, job 31.
FTP> dir rfc <Return>


<List started.
PS:<RFC>
rfc-index.TXT.114
rfc189.TXT.1
rfc407.TXT.1
.
.
.
rfc931.TXT.1
226 Transfer complete.
47 bytes received in 0.02secs (2.3 Kbytes/sec)
FTP> bye <Return>
> BYE command received. Goodbye.

%
```

5.3 Using TELNET

Another valuable way to use the network is offered by the TELNET utility, which allows you to log in to a remote host from a local host (assuming that you have an authorized account on the remote host). Once you have established a TELNET connection and logged into the remote host, you can enter data, run programs, and otherwise operate just as though you were logged in directly. During a TELNET session, each transition to a different interactive program causes a shift to a different command level. With each level, the form of the prompt varies. Command formats also vary with each level. You can often tell which system/program you are using by the prompt symbol. The steps for running TELNET, very briefly summarized, are as follows.

- Log in to your local host.
- Invoke the TELNET program from that host.
- Identify by hostname or network address the remote host that you want access to.
- When the TELNET connection is established, log in to the remote host with the username and password that have been assigned to you on that host.
- Perform whatever tasks you like on the remote machine, being careful not to violate any remote operating system rules.
- When finished working on the remote host, type the remote logout command. Then close the TELNET connection—if it is not automatically closed on logout.
- You are once again operating in your local host system environment.

TELNET has other advanced features too numerous to discuss here. Check you local TELNET user program for online documentation, or talk to your local Host Administrator or user support representative for more information.

5.3.1 Invoking TELNET with the Hostname on the Command Line

In the following example, a user TELNETs from a local UNIX host to a remote SunOS host. Once the connection has been established, the prompts, commands, and responses are those of the Sun Operating System environment. To the user, it appears as though he/she were directly logged in to the remote computer.

After the user is done working on the remote host, he issues the remote system's logout command. This logout automatically returns him to the TELNET program on the local host, closes the TELNET session, and returns the local operating system prompt (%).

Note that instead of invoking the TELNET program and then issuing an "open" command to the remote host at a TELNET prompt, the user supplies the remote hostname directly on the program invocation line. (Not all implementations recognize this form of connection.) In addition, note that the user would need an authorized account on the NIC host to log in with username and password as shown in the example.

% telnet gsimail.ddn.mil <Return>	*User issues the telnet command, giving the remote hostname as an argument on the command line.*
Trying 192.112.37.10 Connected to gsimail.ddn.mil Escape character is '^]'	*TELNET prints messages during connection establishment, affirms the connection, and notifies the user of the escape character (see discussion of escape charaters in Chapter 4). The NIC host prints its banner and prompt (@).*
System 5 UNIX (gsimail) login: **<userid> <Return>** Password: **<Return>**	*User enters his remote system userid and password. The password does not echo on screen.*
...USER SESSION...	
@logout <Return>	*After completing his work, user issues a logout command to exit from the remote system. The connection is closed automatically and the local prompt reappears.*
Connection closed by remote host. %	

5.3.2 TELNET Using Host Address

Instead of invoking TELNET and specifying a hostname for the remote host, you may specify the remote address in dot notation format. Some hosts require the network address to be enclosed in brackets if it is supplied on the command line. (Many TELNET implementation prompt for a network hostname or address if you do not specify one, and they may allow you to open the connection after asking for help or issuing other TELNET commands.) To establish a TELNET connection using a host address, proceed as shown in the example below. The example presumes a user on a UNIX host connecting to the NIC's SunOS system via TELNET. After reaching the NIC host, the user looks up a name with the WHOIS program, exits from WHOIS, and then closes the connection. (Note the change from UNIX prompt symbol to the NIC prompt and back again.)

```
% telnet 192.112.36.5 <Return>
Trying 192.112.36.5 ...
Connected to nic.ddn.mil.
Escape character is '^]'.

SunOS UNIX (nic)

     -- DDN Network Information Center  --
*
* For TAC news, type:                    TACNEWS <return>
* For user and host information, type: WHOIS <return>
* For NIC information, type:            NIC <return>
*
* For user assistance call (800) 365-3642 or (800) 365-DNIC or
                                                  (703) 802-4535
* Report system problems to ACTION@NIC.DDN.MIL

NIC, SunOS Release 4.1.1 (NIC) #1:
Thu Sep 26 11:18:20 1991 EST
@ whois varallob <Return>
Connecting to id Database . . . . . .
Connected to id Database
Varallo, Barbara (BV36)          varallob@NIC.DDN.MIL
    Network Solutions, Inc.
    505 Huntmar Park Drive
    Herndon, VA 22070
    (703) 802-8461
    Record last updated on 08-Aug-91.

Enter a handle, name, mailbox, or other field, optionally preceded
by a keyword, like "host nic".  Type "?" for short, 2-page
details, "HELP" for full documentation, or hit RETURN to exit.
---> Do ^E to show search progress, ^G to abort a search or output <---
Whois: <Return>
@ logout <Return>

Thu Sep 26 11:19:28 1991 EST
Connection closed by foreign host.
%
```

SECTION 6. DDN NETWORK INFORMATION CENTER (NIC)

The DDN Network Information Center (NIC) is located at the DDN Installation and Information Services (DIIS) program office in Chantilly, Virginia. The NIC is funded by the Defense Information Systems Agency (DISA), Defense Network Systems Organization (DNSO). The NIC is responsible for providing general reference services to DDN users via telephone, electronic mail, and U.S. mail. The NIC also provides databases and information services of interest to network users, including the WHOIS registry of network users and other network entities, the NIC/Query browsing system, TACNEWS, and the official DoD Host Name Service. The NIC maintains the RFC (Request for Comments) collection on-line. Many other online informational files are also available through the NIC's automatic mail service, SERVICE@NIC.DDN.MIL.

Among its other duties, the NIC

- registers hosts and domains,
- assigns IP network numbers and Autonomous System Numbers (ASNs),
- provides hostname translation tables and domain name system server files to the DDN and the Internet,
- registers network users,
- issues MILNET TAC Access Cards.

6.1 Contacting the NIC

6.1.1 NIC User Assistance Help Desk

The NIC provides user assistance in a number of ways. Our main Help Desk phone numbers are

1-800-365-DNIC	(within the continental United States)
1-703-802-4535	(outside the continental United States and in the Washington, D.C. metropolitan area)
1-703-802-8376	FAX Number

The first number is toll free, while the area code 703 numbers are toll free in the Washington area only.

The NIC provides Help Desk assistance to those who experience problems with using the network in general and with terminal-to-TAC use in particular. Should you have a security problem or concern, the NIC can connect you with the Security Coordination Center. In addition, the NIC is happy to answer questions about any other service outlined in this section. The NIC Help Desk services are available from 7 a.m. to 7 p.m. (EST/EDT), Monday through Friday.

6.1.2 NIC Host

The NIC computer's hostname and network address are:

NIC.DDN.MIL
192.112.36.5

NIC online services are available 24 hours a day, 7 days a week.

6.1.3 NIC Online Contacts

The NIC supports several online mailboxes to provide assistance in specific areas. This list is provided here for easy reference. The following sections provide more detailed information regarding the type of inquiries each mailbox handles.

Type of Inquiry	Network Mailbox
General User Assistance	NIC@NIC.DDN.MIL
TAC and Non-TAC User Registration	REGISTRAR@NIC.DDN.MIL
Urgent Security Matters	NIC-ALERT@NIC.DDN.MIL
Host, Domain, and Net Registration	HOSTMASTER@NIC.DDN.MIL
NIC.DDN.MIL Computer Operations	ACTION@NIC.DDN.MIL
Comments on NIC Publications, Services	SUGGESTIONS@NIC.DDN.MIL
Security Concerns and Questions	SCC@NIC.DDN.MIL
Usage-Sensitive Billing Questions	BILLING@NIC.DDN.MIL
Automatic Mail Service	SERVICE@NIC.DDN.MIL
Reporting NIC Software Bugs	BUG-SERVICE@NIC.DDN.MIL

6.1.4 NIC U.S. Mail Address

The NIC's current mailing address is

Network Information Center
14200 Park Meadow Drive, Suite 200
Chantilly, VA 22021-2219

6.2 NIC Services

In addition to the user assistance Help Desk described in Section 6.1.1, the NIC provides registration, billing, and security support services.

6.2.1 Network and User Registration Services

The NIC registers the following network entities:

- domains
- IP network numbers
- inverse addressing data
- Autonomous System Numbers (ASNs)
- hosts
- TACs/Mini-TACs
- gateways and PSNs
- some network-related organizations.

Registration of MILNET hosts, TACs, gateways, and PSNs is coordinated with the MILNET Manager. If you wish to register an IP network, domain, or ASN, contact the NIC Help Desk for information regarding procedures. New users seldom need to register these entities.

Each individual who has TAC access to the DDN must be registered in the NIC WHOIS database. Host Administrators register individuals in the database as part of the process of authorizing TAC cards for them. You will find it useful to be registered in this database because it serves as an electronic white pages for DDN users. Non-military Internet Points of Contact are often listed there as well.

To be registered in the NIC WHOIS database, you will need to fill out a copy of the NIC registration template (Figure 6-1 on the following page) and send it to the network mailbox REGISTRAR@NIC.DDN.MIL. You may obtain this template via file transfer (FTP) from the NIC.DDN.MIL machine (192.112.36.5 is the numeric host address) using the pathname `netinfo/user-template.txt` or `templates/user-template.txt` — or you may reproduce the template yourself if you adhere strictly to the format of the online file. Detailed instructions for filling out the template are included in the file. The format of the template may change as DISA dictates, but the latest approved version will be maintained online at the NIC.

(Instructions for using FTP to copy/retrieve a file are presented in Section 5.1.2, or you may consult your local FTP documentation.)

6.2.2 Usage-Sensitive Billing Service Desk

Since the advent of usage-sensitive billing on the DDN, the NIC has provided a service to answer queries regarding DDN billing. This support is provided primarily for POCs who receive the bills and have questions about them. If you have received a bill for DDN usage and have any questions about it, you can contact the NIC Help Desk as described in Section 6.1.1 or send a message to BILLING@NIC.DDN.MIL.

```
D.  Sample Template

-------------------------------------------------------------------------
Sample User Registration Template Version U1.2 - 9/92
-------------------------------------------------------------------------
Do Not Change Format!                 |        Enter Data Here
-------------------------------------------------------------------------
+  U1. NIC Handle (See A.2,3).....: XYZ23
NAME INFORMATION
+  U2A. Last Name.................: Zosters
+  U2B. First Name................: Xary
   U2C. Middle Name or Initial....: Y.
   U2D. Name Suffix...............:
   U2E. Title/Rank................:
ADDRESS INFORMATION
+  U3A. Address Line 1............: Fictitious Solutions, Inc.
   U3B. Address Line 2............: 505 Huntmar Dr.
   U3C. Address Line 3............:
   U3D. Address Line 4............:
+  U3E. City or FPO/APO (See A.4)..: Imaginary
+  U3F. State or FPO/APO Code (A.4): VA
+  U3G. Zip Code (See A.4).......: 22079
   U3H. Country...................: USA
   U3I. Network Mailbox...........: xyz@nic.ddn.mil
+  U3J. Hostname..................: NIC.DDN.MIL
PHONE INFORMATION
+  U4A. Commercial Phone..........: (703) 999-8484
   U4B. Commercial Phone Extension.: 1134
   U4C. Alternate Phone...........:
   U4D. Alternate Phone Extension..:
   U4E. DSN Phone.................:
   U4F. DSN Phone Extension.......:
   U4G. Fax Phone.................:
USER STATUS
   U5A. Delete User? (See A.3)[Y/N]:
+  U5B. TAC Card Required? [Y/N]...: Y
-------------------------------------------------------------------------
```

Figure 6.1. User Registration Template

6.2.3 Security Coordination Center (SCC)

The NIC is the site of the DDN Security Coordination Center (SCC). The SCC acts in conjunction with the DDN Network Security Officer (NSO) to coordinate actions related to security incidents and network vulnerabilities. The SCC relays security-related information to the Network Security Officer (NSO) and works with him/her in handling network security problems. In addition, the SCC issues DDN Security Bulletins to network users. You can contact the SCC in the following ways:

By Electronic Mail:	SCC@NIC.DDN.MIL
By Phone:	1-800-365-DNIC (continental U.S.) 1-703-802-4535 (outside U.S. and in the D.C. metro area)
By FAX:	1-703-802-8376
By U.S. Mail:	Network Information Center ATTN: Security Coordination Center 14200 Park Meadow Drive, Suite 200 Chantilly, VA 22021-2219

Phone hours are from 7 a.m. to 7 p.m., Eastern Standard or Eastern Daylight Time.

6.3 NIC User Programs

The NIC offers several online programs that DDN users may access to retrieve various kinds of information. The WHOIS, TACNEWS, NIC/Query, and SERVICE programs and procedures for using them are described in this section. The NIC's Kermit server is also described.

6.3.1 WHOIS

WHOIS is the NIC program that looks up information in an electronic "white pages" directory of network users. You can also obtain information on hosts, gateways, TACs, domains, and other network entities from WHOIS. WHOIS lists the name, network mailbox, U.S. mail address, telephone number, host, and TAC user status, where applicable, for each user registered in its database. For other entities, it provides such information as domain names, a list of domain servers, domain contacts, network numbers, network contacts, known hosts on a given network or gateway, Host Administrators, and Node Site Coordinators. Phone numbers and network mailbox addresses are provided for all those who serve as Points of Contact (POCs).

6.3.1.1 Accessing WHOIS

Here are some instructions for accessing the WHOIS program from different points of origin:

From a TAC

- Type `@n`.
- After being greeted by the TAC banner, press <Return> and enter your TAC userid and TAC Access Code when prompted.
- After the NIC host banner and greeting are displayed, type **`whois <Return>`**.

From a DDN Host

- Log onto your local host and TELNET to the NIC, e.g.,

```
telnet nic.ddn.mil <Return>
```

or

```
telnet 192.112.36.5 <Return>
```

- After the NIC host banner and greeting is displayed, type **whois <Return>**.

Via Electronic Mail

- From your login host, invoke the mail program and send a message to

  SERVICE@NIC.DDN.MIL

- As the subject of the message (i.e., on the "Subject:" line), enter WHOIS and the string you want the program to search on—e.g.,

  Subject: **whois nic.ddn.mil**

  Any valid WHOIS search input string can be sent to the SERVICE program. However, if the response is large, it will be split into several return messages. If it is very, very large, it may exceed the capacity of the Mail server, but most search outputs are well within its limits.

You may also run the WHOIS program from a local host if you have one of the several WHOIS user programs that are available for various operating systems. Contact the NIC if you are interested in obtaining such a program.

6.3.1.2 Using WHOIS

To use WHOIS, you can supply either the name or the NIC "handle" of the person or entity you are trying to identify. The handle is a unique identifier that the NIC assigns to each entity registered in its database. Partial searches on the first part of a name are also possible.

The WHOIS program accessible on the NIC host also recognizes certain keywords. They tell WHOIS to limit its search to certain kinds of records—such as host records only, or domain records only. If you search with a keyword, you must insert the keyword in the search string before the entity for which you want information. Such keywords can increase the speed of a search. Some of the keywords that the NIC host's WHOIS program recognizes are as follows:

DOM	for domain records
GA	for gateway records
HO	for host records
NET	for network records
PSN	for PSN records
TAC	for TAC records.

WHOIS is not case sensitive. Some of the examples that follow use keywords and some do not. Those that do use keywords assume that you have used TELNET to connect to the NIC.DDN.MIL for access to their WHOIS program. For a complete list of keywords and examples of how to use them, simply type **help** or a question mark (?) at the WHOIS prompt, e.g.,

```
Whois: help <Return>
```

WHOIS responds to your query in one of three ways:

1. If WHOIS finds a unique record for the individual/entity you have identified as the subject of the search, it immediately displays the following information:

   - the name
   - the NIC handle
   - the organization (if applicable)
   - the mailing address
   - the phone number
   - the network mailbox.

2. If WHOIS finds several records that match the search input, it displays a brief list of the matching entries and asks you to choose the correct match by using the handle (a unique character string in parentheses following the name). A search by handle produces the expanded output for the matching entity.

3. If no record matches the search input, WHOIS displays the message "No match for <search-string>," where <search-string> is the character sequence you entered.

The following examples illustrate some of the WHOIS capabilities. For more information on using WHOIS, connect to the NIC host and type **whois help**.

6.3.1.3 WHOIS Search Examples

[NOTE: The names, addresses, phone numbers, and other information shown in the following examples are meant to be representative only; they are not necessarily actual or accurate data and should not be used for contacting any of the entities/persons identified!]

WHOIS Search by Name

```
SunOS UNIX (nic)

-- DDN Network Information Center  --
*
* For TAC news, type:                    TACNEWS <return>
* For user and host information, type: WHOIS <return>
* For NIC information, type:             NIC <return>
*
* For user assistance call (800) 365-3642 or (703) 802-4535
* Report system problems to ACTION@NIC.DDN.MIL

NIC, SunOS Release 4.1.1 (NIC) #1:
Thu Sep 26 14:11:08 1991 EST
@ whois roscoe <Return>          (There is only one "Roscoe," so a complete entry
                                 is displayed for him.)
Connecting to id Database . . . . . .
Connected to id Database

   ROSCOE, Joe A. (JAR1)              JROSCOE@HOST-1.DOMAIN.MIL
   Air Force Data Systems
   Design Center/SDTS
   Willits Air Force Base, WV  12345
   Phone:  (123) 456-7890
   MILNET TAC User

   Record last updated on 31-Jul-91
```

WHOIS Search by Partial Name

You may search using only a partial name as the search string by entering the partial name followed by one to three dots (...). This search feature will work only if the dots follow the partial name without any intervening spaces. This kind of search is apt to produce multiple "hits" (hits are entries that match a given search string).

Note that the partial name search also finds any NIC handles that begin with the partial name input ("ros" in the example that follows).

```
@whois ros... <Return>

Rosati, David (DR16)          Rosati@BAR.FOO                (234) 567-8901
Rosales, Alphonso L. (ALR)    Rosales@NIC.DDN.MIL           (345) 678-9012
Roscoe, Joe A. (JAR1)         Roscoe@HOST-1.DOMAIN.MIL      (123) 456-7890
.
.
.
Schuman, Richard O. (ROS)     Schuman@FOO.BOO.Com           (456) 789-0123

There are 25 more entries.  Show them?
```

To obtain all the information pertaining to any of these names, do a WHOIS search on the handle (the text in parentheses immediately following the name); this will produce a full entry.

WHOIS Search by Handle

If a WHOIS search produces multiple hits on your query, search by the unique handle to get the full entry of the hit you want to display. Precede the handle with an exclamation point. Users on hosts running a UNIX operating system may need to precede the exclamation point with a backslash (\).

```
@whois !jar1                    Jar1 is the handle for ROSCOE.

ROSCOE, Joe A. (JAR1)             JROSCOE@HOST-1.DOMAIN.MIL
Air Force Data Systems
Design Center/SDTS
Willits Air Force Base, WV  12345
Phone:  (123) 456-7890
MILNET TAC User

Record last updated on 31-Jul-91
```

WHOIS Search by Hostname

If you know a hostname and need to obtain the host address, you may use WHOIS to look it up by typing your input as shown in the following example:

```
NIC, SunOS Release 4.1.1 (NIC) #1:
Thu Sep 26 14:11:08 1991 EST
@whois ddn-conus.ddn.mil <Return>    (User enters known hostname after connecting
                                      to the NIC host and types a "^E" to see how
                                      the search is progressing.)
Connecting to id Database . . . . . .
Connected to id Database
^E 14:13:03 -- No matches yet.

BBN INC. (DDN1)
   1300 North 17th Street
   Arlington, VA 22209

   Hostname: DDN-CONUS.DDN.MIL
   Nicknames: DDN1.DCA.MIL,DDN.DCA.MIL
   Address: 26.21.0.17
   System: BBN-C/70 running UNIX
   Host Administrator:
      Bolden, Michelle L. (Shelly)   (MLS6)  Bolden@BBN.COM
      (703) 284-4600

   Record last updated on 05-Sep-91.

Would you like to see the registered users of this host? y <Return>

      There are 202 registered users:

   Adams, Quentin (QAA1)              nsc-robins@DDN-CONUS.DDN.MIL
                                      (912) 926-6912 (DSN) 468-6912
   Agney, Violet (VA24)               NSCElmen@DDN-CONUS.DDN.MIL
                                      (907) 552-4919 (DSN) 317-552-4919
   Agnor, Robert J. (RJA25)           NAVTELCOM@DDN-CONUS.DDN.MIL
                                      (202) 282-0824 (DSN) 292-0824
   Atkinson, Barry K. (BKA)           DIA-RSE@DDN-CONUS.DDN.MIL
                                      (703) 284-0801 (DSN) 251-0801
   Bailey, Erich (EB68)               NSC-Presidio@DDN-CONUS.DDN.MIL
                                      (415) 561-2241 (DSN) 586-2241
   There are 197 more matches.  Show them? n <Return>
   Enter a handle, name, mailbox, or other field, optionally preceded
   by a keyword, like "host sri-nic".  Type "?" for short, 2-page
   details, "HELP" for full documentation, or hit RETURN to exit.
---> Do ^E to show search progress, ^G to abort a search or output <---
```

Note that this search produces the hostname, the host address, and the name and phone number of the Host Administrator. Pressing <Return> will produce a list of the people registered with the NIC as users of that host. You will find the same information if you know the host address or nickname and search on one of those instead of the official hostname.

WHOIS Search by TAC Name

You may use WHOIS to obtain a TAC telephone number if you know the name of the TAC. A search by TAC name will also show contact information on the Node Site Coordinator for the TAC. Follow the example below to do this type of search.

```
   Enter a handle, name, mailbox, or other field, optionally preceded
   by a keyword, like "host sri-nic".  Type "?" for short, 2-page
   details, "HELP" for full documentation, or hit RETURN to exit.
---> Do ^E to show search progress, ^G to abort a search or output <---

   Whois: tac belvoir.mt.ddn.mil <Return>
   Fort Belvoir (BELVOIR-MIL-TAC)
      Army Information Systems Command (USAISC)
      Building 246, Room 202, 2nd Floor
      Fairfax, VA 22060

      (703) 781-0050 (R8) [300/1200 bps] (B)
      (703) 781-0100 (R8) [300/1200 bps] (B)

      Hostname: BELVOIR.MT.DDN.MIL
      Address: 26.0.0.142
      TAC number: 162
      Hardware: C/30

      Coordinator:
         Jewell, Brenda K.  (BJ53)  NSCBelvoir@DDN-CONUS.DDN.MIL
         (703) 664-3458 (DSN) 354-3458

      Record last updated on 22-Jun-90.
```

WHOIS Search by PSN Number

You may use WHOIS to search by node (PSN) number. The output from this search will show the usual POC information as well as a list of the hosts connected to that node that are registered with the NIC.

```
Whois: psn 202 <Return>
GSI (CHANTILLY2-IMP)
   14200 Park Meadow Drive
   Chantilly, VA 22021

   CHANTILLY2 is PSN/IMP 202 on network 26

   Coordinator:
      Zalubski, John  (JZ7)  zalubskij@NIC.DDN.MIL
      (703) 802-8462

   Record last updated on 04-Sep-91.

   No hosts found on this PSN.

Whois: psn 201 <Return>
GSI (CHANTILLY-IMP)
   14200 Park Meadow Drive
   Chantilly, VA 22021

   CHANTILLY is PSN/IMP 201 on network 26

   Coordinator:
      Zalubski, John  (JZ7)  zalubskij@NIC.DDN.MIL
      (703) 802-8462

   Record last updated on 04-Sep-91.

   Hosts on this PSN:

   CHANTILLY1.MT.DDN.MIL          26.0.0.201
   NIC1.DDN.MIL                   26.1.0.201
   SUN1.DDN.MIL                   26.24.0.201
   GSI-GW1.DDN.MIL                26.25.0.201, 192.112.36.1,
                                  192.112.37.1, 192.112.38.1
```

WHOIS Search by Network Number

You may use WHOIS to search by network number. To search for information about a Class C network, make sure the last octet in the network number is zero. To search for a Class B network, make sure that the last two octets are zero. See section 8.4 for a discussion of network addresses and classes.

```
@ whois 192.112.36.0 <Return>
Government Systems, Inc. (NET-LOCALNET)
   14200 Park Meadow Drive, Suite 200
   Chantilly, VA  22020

   Netname: LOCALNET
   Netnumber: 192.112.36.0

   Coordinator:
      McCollum, Robert   (RM584)   bobm@NIC.DDN.MIL
      (703) 802-8476

   Domain System inverse mapping provided by:

   NIC.DDN.MIL                    192.112.36.5
   NIC-DEV.DDN.MIL                192.112.38.89

   Record last updated on 14-Aug-91.

Would you like to see the known hosts on this network? y <Return>

   There are 2 known hosts:

   NIC.DDN.MIL                    192.112.36.5
   GSI-GW1.DDN.MIL                26.25.0.201, 192.112.36.1,
                                  192.112.37.1, 192.112.38.1
```

The user can enter "y" or simply press <Return> to see a list of hosts registered with the NIC as part of this network.

WHOIS Search by Domain Name

```
Whois: dom dca.mil <Return>
Defense Information Systems Agency (DCA-DOM)

   Domain Name: DCA.MIL

   Administrative Contact, Technical Contact, Zone Contact:
      Hostmaster  (HOSTMASTER)  HOSTMASTER@NIC.DDN.MIL
      (800) 365-DNIC (703) 802-4535

   Record last updated on 18-Sep-91.

   Domain servers in listed order:

   NS.NIC.DDN.MIL                192.67.67.53
   A.ISI.EDU                     26.3.0.103, 128.9.0.107
   C.NYSER.NET                   192.33.4.12
   TERP.UMD.EDU                  128.8.10.90
   NS.NASA.GOV                   128.102.16.10, 192.52.195.10
   AOS.BRL.MIL                   192.5.25.82

Would you like to see the known hosts under this secondary domain? y

   There are 60 known hosts:

   ANTARES.DCA.MIL               128.19.0.14
   BELLATRIX.DCA.MIL             128.19.0.5
   C4SD.DCA.MIL                  26.8.0.76
   CMMC-BBN.DCA.MIL              26.18.0.70
   CMMC-IMW.DCA.MIL              26.29.0.76
There are 55 more matches.  Show them? n <Return>
Whois:
```

As you can see, domain searches allow you to identify the hosts providing name service for the domain, as well as the names and phone numbers of the administrative and technical contacts for the domain (in this case, the NIC Hostmaster group).

6.3.2 NIC/QUERY

NIC/Query is a browsing service that allows you to page through general information about the Defense Data Network (DDN). Topics included under NIC/Query are presented in a numbered menu. All the services of the TACNEWS program are also available via NIC/Query for the sake of simpler user accessibility.

The program is largely self-explanatory, and online help is available if you need it. You do not need a login account on the NIC machine for access. To access NIC/Query, simply open a TELNET connection to NIC.DDN.MIL, and then type **nic** or **query**, as shown below.

```
%telnet nic.ddn.mil <Return>

 Trying... Open

 NIC.DDN.MIL  SunOS ...
 @nic <Return>
 NIC/Query Version: 1.4 Thu, 26 Sep 91 14:27:13


 Stop output every 24 lines? ([Y]/N/# of lines) y <Return>
 ROOT

 Use NIC/Query to access a hierarchy of information about the Defense
 Data Network (DDN) and the Network Information Center (NIC) using
 simple menus.  Bugs to BUG-QUERY@NIC.DDN.MIL.

 **
 ** Note that a carriage return is required after every command.
 ** Select menu item 1 for help using this program.
 **

    1) HELP -- Introduction, changes, detailed help, help summary.
    2) WHOIS -- Directory of DDN users.
    3) HOSTS -- Describes DDN hosts.
    4) PROTOCOLS -- Describes DDN protocols.
    5) RFCS -- Requests For Comments technical notes.
    6) NIC DOCUMENTS -- Documents available from the NIC.
    7. TACNEWS -- TACnews program.

 ROOT: Enter a menu# (1 - 7), or a command ('?' to list).
 NIC/Query: 1 <Return>
    HELP -- Introduction, changes, detailed help, help summary.
    1. INTRODUCTION -- An introduction to the NIC/Query system.
    2. CHANGES -- Differences from the old version of NIC/Query.
    3) NOVICES -- Detailed help for new users.
    4. HELP SUMMARY -- Brief description of NIC/Query concepts and
       commands.

    HELP: Enter a menu# (1 - 4), or a command ('?' to list).
    NIC/Query: 1 <Return>
```

In the example above, the user asks for help at the "NIC/Query:" prompt. A submenu is presented so he can select the level or type of information he wishes to have displayed.

6.3.2.1 TACNEWS

TACNEWS is a NIC online service that offers login help to TAC users. It also offers access to the interactive TAC locator program that allows you to find the three TAC phone numbers closest to a phone number you enter. TACNEWS provides a mechanism for reading the DDN Newsletters, DDN Management Bulletins, and DDN Security Bulletins. Users should read these publications regularly to stay current on DDN policies, announcements, and network news items.

If you wish to have newsletters and bulletins delivered online to your network mailbox, send a message to REGISTRAR@NIC.DDN.MIL including your name and address and indicating that you wish to be on the online distribution for the newsletters and bulletins.

You may access TACNEWS by logging into a TAC and typing **tacnews**. Alternatively, you may open a TELNET connection to NIC.DDN.MIL from a local host to read TACNEWS, as shown in the examples on the following pages.

TACNEWS services are also available via the NIC/Query program; this redundancy allows users connecting to the NIC via TELNET to take advantage of all services in a single connection session.

```
@n <Return>
TAC Userid: <Username> <Return>          Enter your TAC Username here.
Access Code: <Access Code>               Enter your TAC Access Code. It will not
                                         echo on screen.
Login OK
TCP Trying...Open

Trying 192.112.36.5 ...
Connected to NIC.DDN.MIL.
Escape character is '^]'.
*  -- DDN Network Information Center --
*
*  For TAC news, type:                      TACNEWS <Return>
*  For user and host information, type:     WHOIS <Return>
*  For NIC information, type:               NIC <Return>
*
*  For user assistance call (800) 365-DNIC or (703) 802-4535
*  Report system problems to ACTION@NIC.DDN.MIL or call
                                                  (703) 802-4535
@ tacnews <Return>
TACnews Version: (xxxx.xxx) Thu, 26 Sep 91 14:30:14

Stop output every 24 lines? ([Y]/N/# of lines) y <Return>

  1. Announcements -- Updated 11-Jul-91
  2. TACs, List of U.S. TAC Dial-Ins, 23K
  3. Locator, Finds U.S. TAC Dial-Ins
  4. Eur/Pac, List of European/Pacific TAC Dial-Ins, 15K
  5. Login, Help with TAC login, 6K
  6. Newsletters, DDN -- Updated 16-Sep-91
  7. Bulletins, DDN Management -- Updated 16-Sep-91
  8. Bulletins, DDN Security -- Updated 16-Sep-91

Type a menu number (1 - 8), ? for options, "HELP" for instructions.
TACnews: 7 <Return>   (After telling the TACNEWS program to limit each display page to
                       24 lines and seeing the menu display, user elects to read the DDN
                       Management Bulletins.)
There are 30 Bulletins online.  The latest:
    .
    .
    80  21-Dec-90   REGISTRATION OF IP NETWORK NUMBERS
    81   9-Apr-91   MTACs Operational with Limited Monitoring and
                    Control Capability
--> 82  23-Apr-91   Corrected  MTACs Operational with Limited
                    Monitoring and Control Capability

Type an issue number (22-82), ? for options, or HELP for full help.
TACnews: 82 <Return>
```

```
% telnet nic.ddn.mil <Return>
Trying 192.112.36.5 ...
Connected to nic.ddn.mil.
Escape character is '^]'.

SunOS UNIX (nic)

 -- DDN Network Information Center  --
*
* For TAC news, type:                    TACNEWS <return>
* For user and host information, type: WHOIS <return>
* For NIC information, type:             NIC <return>
*
* For user assistance call (800) 365-3642 or (800) 365-DNIC or
                                                (703) 802-4535
* Report system problems to ACTION@NIC.DDN.MIL

NIC, SunOS Release 4.1.1 (NIC) #1:
Thu Sep 26 14:11:08 1991 EST
@ tacnews <Return>
TACnews Version: (xxxx.xxx) Thu, 26 Sep 91 14:30:14

Stop output every 24 lines? ([Y]/N/# of lines) y <Return>

  1. Announcements -- Updated 11-Jul-91
  2. TACs, List of U.S. TAC Dial-Ins, 23K
  3. Locator, Finds U.S. TAC Dial-Ins
  4. Eur/Pac, List of European/Pacific TAC Dial-Ins, 15K
  5. Login, Help with TAC login, 6K
  6. Newsletters, DDN -- Updated 16-Sep-91
  7. Bulletins, DDN Management -- Updated 16-Sep-91
  8. Bulletins, DDN Security -- Updated 16-Sep-91

Type a menu number (1 - 8), ? for options, "HELP" for instructions.
TACnews:
```

6.3.3 NIC Kermit Server

For PC users who cannot access FTP from their hosts, the NIC has an anonymous Kermit server available. (A server is a software module that provides a service to users or user programs that request it.) You should be familiar with the Kermit file transfer protocol and have a PC communications program that supports that protocol Before you attempt to transfer documents with it.

To download a file from the NIC using the Kermit server, proceed as follows:

1. Set the receive packet size on your PC Kermit to 60.

2. Connect to NIC.DDN.MIL (192.112.36.5) through a TAC or Mini-TAC.

3. Once you get the NIC login prompt (@), change the TAC intercept character to a control-y (^y) by issuing the following TAC command: **`@i 25 <Return>`**. Notice that you must type the "@" symbol because it signals the TAC that you are issuing a command.

4. Press <Return> to get the NIC prompt (@ is now the NIC prompt symbol), then type **`Kermit<Return>`**. This command activates the Kermit server on the NIC.

5. Drop back to your PC Kermit and get the file that you want from the NIC.

6. When you are finished, type "**`bye`**" to end the Kermit session on your PC.

For more information on using Kermit through a TAC, see the files `KERMIT-TAC-INFO.TXT` and `KERMIT-NICSERVER.TXT` in the NETINFO/ directory on the NIC.DDN.MIL host. These files are available via the SERVICE mail server (see Section 6.3.5).

6.3.4 NIC Automated Mail Service

SERVICE is an automated electronic mail system provided by the DDN Network Information Center. It allows access to most online NIC documents and information via electronic mail.

To use the mail service, send a message to `SERVICE@NIC.DDN.MIL`. In the SUBJECT field, enter the type of service you are requesting, followed by any arguments needed to further define your request. The message body is normally ignored; however, if you leave the SUBJECT field empty, the first line of the message body is used as the request. If your request involves the transmission of large files, they are broken into smaller, separate messages; however, a few files are too large to be sent through the mail system. SERVICE requests are processed automatically once a day.

The following services are currently available. Each item on the list is followed by an example of a subject line for requesting that service:

HELP	This message; a list of current services. Subj: HELP
RFC nnnn	nnnn is the RFC number. Subj: RFC 822
RFC Index	Retrieves the index of RFCs. Subj: RFC INDEX
IEN nnn	nnn is the IEN number or the word INDEX. Subj: IEN 828
NETINFO xxx	xxx is a file name or the word INDEX. Subj: NETINFO DOMAIN-TEMPLATE.TXT
SEND xxx	xxx is a fully specified file name. Subj: SEND IETF/1WG-SUMMARY Subj: SEND INTERNET-DRAFTS/DRAFT-IETF-IWG-BGP-OO.TXT
HOST xxx	Returns information about host xxx. Subj: HOST NIC.DDN.MIL

INDEX	Returns the master list of available index files.
FYI nnn	Returns the specified FYI document, where nnn is the FYI number or the word INDEX. Subj: FYI 1
WHOIS xxx	Returns information about xxx from the WHOIS service. Use "WHOIS HELP" for information on using WHOIS. Subj: WHOIS MCCOLLUMB

6.4 Documents Published by the NIC

The NIC compiles and publishes online versions of the documents listed below. The file nic-pubs.txt in the netinfo directory on NIC.DDN.MIL contains an expanded, annotated list of publications that are currently available online. Many of these documents are deposited at the Defense Technical Information Center (DTIC), where they are available to military network users. Hardcopies of some documents and RFCs are available from the former NIC, SRI International in Menlo Park, CA. Contact SRI for prices and ordering information. Ordering instructions are also provided in the online file nic-pubs.txt. You may contact the NIC to confirm document availability or to learn about newly available documents.

THE DDN NEW USER GUIDE

The document you are reading. A brief guide to DDN network tools and services designed to introduce users to the network. The Guide is available online as `netinfo/nug.doc`.

THE NETWORK PROTOCOL IMPLEMENTATIONS AND VENDORS GUIDE

The Vendors Guide lists software and hardware implementations of the DDN protocols, based upon information supplied by vendors. This document is for informational purposes only. Entry on this list does not imply endorsement. Available online as `netinfo/vendors-guide.doc`.

RFCs

Requests for Comments, or RFCs, are network technical notes, each of which is identified by a unique number. The RFCs are available online as `rfc/rfcnnnn.txt` (where nnnn is the RFC number). Hardcopies are available by subscription from SRI International, Menlo Park, CA.

6.5 Online Reference Files at the NIC

Several other public files on the NIC.DDN.MIL host are of special interest to network users. The pathnames and brief descriptions of some of these files are listed below. You may retrieve these files via FTP (using USERNAME *anonymous*, PASSWORD *guest*). See Section 5.1.2 for FTP instructions. You may also obtain the files by electronic mail using the NIC Mail SERVICE program (see Section 6.3.5) or via the NIC Kermit Server (see Section 6.3.4).

`netinfo/mil-nsc.txt`

Node Site Coordinators for each node or PSN on the MILNET.

`netinfo/hosts.txt`
Official Internet DoD Hostname Table, which lists the names and numbers of domains, networks, gateways, and hosts on the DoD Internet. It is designed to be machine readable. From this file, two additional files are generated:

`hosts.txt.z`, a UNIX compressed version of the hosts.txt file, and `mil-hosts.txt`, a complete listing of the MILNET hosts in hosts.txt.

`netinfo/host-location.txt`
Addresses of MILNET hosts locations, sorted geographically.

`netinfo/hostserver-instructions.txt`
Instructions for using the NIC's hostname server to transfer the host table.

`netinfo/mil-host-administrators-a-l.txt`
Military Host Administrators "A" through "L," sorted by hostname.

`netinfo/mil-host-administrators-m-z.txt`
Military Host Administrators "M" through "Z," sorted by hostname.

`netinfo/nic-pubs.txt`
Information about publications available from the NIC.

`netinfo/nug.doc`
Online version of this document.

`netinfo/what-the-nic-does.txt`
General information regarding NIC services.

`netinfo/user-template.txt`
Template for users who want to be registered in the WHOIS database.

`netinfo/tac-location.txt`
Geographic location of each TAC. This file is useful for locating the TAC closest to you.

`netinfo/usa-tac-phones.txt`
Phone numbers for TACS within the fifty states.

`netinfo/foreign-tac-phones.txt`
Phone numbers for TACs outside the U.S.

`netinfo/domain-contacts.txt`
Name, mailbox, and phone number for each domain contact registered with the NIC.

`netinfo/network-contacts.txt`
Name, mailbox, and phone number for each network contact registered with the NIC. The NIC registers all IP networks and designates a contact for each one.

`netinfo/00netinfo-index.txt`
Name and a brief description of each file available in the publicly accessible NETINFO directory on the NIC host.

`netinfo/kermit-info.txt`
General information on the Kermit program.

`netinfo/kermit-nicserver.txt`
Specific information on the NIC Kermit server.

`netinfo/kermit-tac-info.txt`
Specific information on TAC usage with Kermit.

`protocols/gosip-v1.doc`
Version 1 of the GOSIP document.

`protocols/gosip-order-info.txt`
Descriptions of GOSIP-related documents and information on how to obtain them.

`rfc/rfcnnnn.txt`, where nnnn is the RFC number
Network technical notes, known as Requests for Comments, or RFCs, are online in the directory RFC: on the NIC.DDN.MIL host. New RFCs are announced to network users via an online distribution list maintained by the NIC. Individuals who want to be added to the RFC notification list should send a message to `RFC-REQUEST@NIC.DDN.MIL`.

`rfc/rfc-index.txt`
Lists all RFCs in reverse numerical order, with the most recent RFC at the top. Includes author, title, date of issue, RFC number, number of hardcopy pages, number of online bytes, format (ASCII text or PostScript), and information regarding other RFCs that make a given RFC obsolete or update it. Notes whether an RFC is also an FYI.

`fyi/fyinn.txt`, where nn is the FYI number
(FYI = For Your Information) General information technical notes issued as special RFCs.

`fyi/fyi-index.txt`
Mirror of the RFC Index, but listing only FYIs. Notes the corresponding RFC number for each FYI.

SECTION 7. SECURITY CONSIDERATIONS AND NETWORK CONDUCT

7.1 Requirements for Legitimate DDN Access

Only authorized users engaged in U.S. Government business or applicable research or those who are directly involved in providing operations or system support for Government-owned or Government-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. Users of the DDN must not violate privacy or other applicable laws and should not use the networks for advertising or recruiting purposes without the express permission of the Defense Information Systems Agency.

Unauthorized use of the DDN is illegal. Persons who break into Government networks or use Government computer resources without authorization will be prosecuted. Hosts that permit this type of access will be disconnected from the network.

> [NOTE: DISA reserves the right to discontinue DDN access to any user(s) who are, in DISA's opinion, not conducting legitimate Government business/activity. DISA will send one letter of warning through command channels (via registered mail) to any user found to be conducting illegitimate business. Should the illegitimate activity continue, DISA will terminate the user's access without additional notice.]

7.2 Security Considerations and Guidelines for Network Conduct

Several levels of responsibility provide security for the DDN. At the most basic level, individual users should take precautions to minimize the chances that their accounts could be compromised. They bear the primary responsibility for the protection of their information. If more users were to take this responsibility seriously and act accordingly, the majority of computer security breaches would not occur.

You can best protect your own files via careful password management. Do not use an unmodified word from any language; this includes words spelled backward. Your Host Administrator should have suggestions as to proper password choices.

Follow these recommendations to reduce the possibility of compromise of your computer system or files:

- Do not leave your terminal logged in and unattended.
- Know your operating system's protection mechanisms and make sure that all your files are set up with appropriate protection modes.
- Choose a password that meets the guidelines of your site or, at minimum, one that is not an unmodified word from any language. A simple modification involves prefixing a word with a numeral (or several numerals).
- Change your password as required by your site or, at minimum, every six months.

- Do not write your password down on paper or record it in a file stored on any computer disk, floppy disk, PC, or magnetic tape.

Users have the primary responsibility for protecting their own accounts, but several other people have roles in providing system and network security.

Host Administrators are generally responsible for ensuring that their host sites maintain a reasonable level of protection from the possibility of network compromise. They must act as liaisons with the DDN Network Security Officer (DDN NSO), the Security Coordination Center (SCC), vendors, law enforcement bodies, and other appropriate agencies to resolve any outstanding security problems and prevent their recurrence. They are responsible for the enforcement of all DDN policies at their site.

The NSO recommends security policy affecting the DDN and is responsible for its general enforcement. The NSO also works closely with Host Administrators to resolve network and related computer security problems or incidents affecting their sites.

The DDN Security Coordination Center is located at the NIC. The SCC acts as a liaison between Host Administrators and the NSO and between MILNET sites and Internet security response centers such as the Computer Emergency Response Team (CERT).

If you suspect that a computer break-in has occurred, you should contact your Host Administrator. The flow of security incident reporting should be from the end user to the Host Administrator or other appropriate individual, who then determines if the problem is local or network related. If the problem is network related, the Host Administrator should refer the problem to the appropriate site as noted in DDN Security Bulletin 9003 [7]. In such cases, the Host Administrator's first step is to call the MILNET Monitoring Center for your area. Phone numbers for the Monitoring Centers are found in Section 9.2.

7.3 Network Conduct

The network environment is somewhat different from the traditional workplace. Rules for proper conduct are gradually emerging to fit this new environment. The rules and guidelines presented here relate to four areas:

- passwords
- file protection
- plagiarism
- network mail

7.3.1 Passwords

Since use of the network is restricted, passwords, access codes, and TAC cards should never be shared. Change your host login password regularly and report any unauthorized use of passwords to your Host Administrator. MILNET TAC cards and records of host Userids and Access Codes should be kept in a safe place. Users should be familiar with and follow local security guidelines.

7.3.2 File Protection

Most operating systems have a method of protecting files from network read and write access. The recommended file protection default for directories is "no read and no write to outside users." If your files are protected in this way, you can still make them accessible to outside users over the network, but you must take action to reset file and directory protections to make this happen.

As a new user, you should find out what the protection default is on your host and ensure that files you don't want accessible to other users are protected. Ask you Host Administrator about default file and directory protection settings and for instructions on protecting/unprotecting files.

7.3.3 Plagiarism

Even if a file is unprotected, you are not free to copy or read it without first asking permission. It is as inappropriate to read online mail or browse through online files without permission as it would be to read a colleague's hardcopy mail or rummage around in his desk.

Electronic plagiarism of another's work is just as unethical as plagiarism by any other means. Be sure to credit users whose work you cite or whose ideas you express. Copyright laws must also be carefully observed and obeyed.

It is easy and convenient to exchange code and programming across the network. Many code developers are extremely generous in sharing their work. Even so, before copying or using someone else's code, be sure to get permission from the developer or maintainer and credit the source in your documentation. Under no circumstances should programming or code from anywhere on the network be used (verbatim or edited) commercially without the owner's explicit permission.

7.3.4 Mail

Electronic mail is a powerful communication tool that must be used with care. The following guidelines will help you avoid offending other users and overloading the network.

It is easy to forward mail you receive; but the writer may never have intended that anyone else read the message. For this reason, it is wise to check with the sender before forwarding a private message of any significance.

The DDN is a business environment, so try to keep your messages short and to the point. It is easy to send off a quick message, only to realize a moment later that you needed to say more. To avoid this, organize your thoughts and send a single message rather than several incomplete ones. This will make your mail far more useful to the recipients, and minimize the load on the network.

Online mail tends to change a person's style of communication. Sending mail is so quick that it is tempting to send your immediate reaction to a message rather than a more considered, appropriate response. Do not use derogatory or inappropriate language in messages, especially those sent to discussion groups. Keep in mind that no one likes to be offended or embarrassed by careless comments.

Finally, if you regularly send mail to a large group, learn how to create a mailing list. Otherwise, each recipient must scroll through a list of the mailboxes of all other recipients as a part of the message header.

Remember, use of the network is a privilege. It is your duty to use the network responsibly as it was intended to be used and to obey general network policies. In return, the network gives you access to many tools and to an online community of other network users.

7.4 Additional Security Information

Host and system administrators are encouraged to order "DCAC 310-P115-1, DDN Security Management procedures for Host Administrators," May 1991. Copies may be obtained in the following manner:

1. Government agencies may request a publication by submitting a DCA Form 117, Publication of Blank Form Request, to the Director, DISA, ATTN: BIAR, Arlington, VA 22204-2199.

2. Other organizations may request a publication by submitting a letter with appropriate justification to the address given above. **The DCA Form 117 is used by Government agencies only.**

SECTION 8. NETWORK CONCEPTS OVERVIEW

8.1 Introduction

In the following paragraphs, we provide some general information about topics such as usage-sensitive billing, network gateways/concentrators, network addresses, the Domain Name System, and GOSIP. Although most new DDN users will not be actively involved in any of the areas covered in this section, they do involve concepts you should become familiar with, since they are important to all DDN users.

8.2 Usage-Sensitive Billing

The usage-sensitive billing system was implemented on the DDN to distribute costs more equitably, based on actual use of network resources. The tariff structure is designed to support cost recovery so that the amount recovered from each subscriber is proportional to that subscriber's use of network resources.

Generally speaking, all hosts and dedicated terminals are charged a basic monthly rate. Users' network connections are charged on a per-minute basis. A charge is also levied for each kilopacket of traffic sent by each host or terminal user. Charges reflect peak-versus-nonpeak usage and precedence level.

Monthly bills are sent to designated representatives of the military branches as well as to other Government agencies. The bills are then distributed according to locally established policies. That is, a packet of several bills might be sent to a site and then distributed to other individuals by the billing Point of Contact (POC) at that site.

It is rare for an individual user to see a bill. However, you should be aware that your use of the DDN does affect costs charged back to your service and, perhaps, to your host site. Therefore, all users should be conscientious in conforming to host-site usage policies.

The NIC provides a Usage Sensitive Billing (USB) Service Desk to help answer inquiries from DDN users or user organizations regarding the traffic and/or connection charges shown on their billing reports. USB Service Desk personnel are available by phone Monday through Friday from 9:00 a.m. to 5:00 p.m., Eastern time. Electronic mail is accepted 24 hours per day.

Service Desk personnel have access to many sources of DDN usage information. They are available to answer general questions as well as site- or user-specific questions. In the event a question or inquiry goes beyond the scope of the Service Desk, the caller can be referred to a more appropriate contact or agency.

Use the following information to contact the USB Service Desk:

By Electronic Mail:	BILLING@NIC.DDN.MIL
By Phone:	1 (800) 365-DNIC (inside the U.S.) 1 (703) 802-4535 (outside the U.S. or in the Washington D.C. area)
By U.S. Mail:	DDN Network Information Center ATTN: Usage-Sensitive Billing Desk 14200 Park Meadow Drive, Suite 200 Chantilly, VA 22021

8.3 Network Concentrators

Networks can be categorized according to size or geographic distribution, and they can be referred to as local area networks (LANs) or wide area networks (WANs). A LAN might serve a single office, a building, or an entire military site. WANs are typically cross-country networks employing technologies such as satellites or long distance land lines; they can serve large geographic areas such as military installations located throughout the world. The DDN is a WAN that reaches all major DoD installations worldwide.

To expand computer communications not only across geographic distances, but also across different networking technologies, gateways are used to connect networks together into internetworks or "internets." The DDN is part of an IP-based internetwork, known to DDN users as "the Internet."

The use of gateway concentrators as a method of connecting to the DDN is a relatively new trend. Gateway concentrators enable LANs and hosts at military installations to connect to the DDN. Concentrators lessen the need for individual host connections without limiting local users' access to full DDN service.

Gateway concentrator use increased when DISA limited the number of PSN ports that would be available to connect hosts directly to the DDN. This limitation, coupled with the long lead time required for direct host connections, lent impetus to the establishment of gateway concentrator programs for the military. Currently, the Air Force and the Army have concentrator programs to fulfill their long-haul data communication requirements. These programs have become their primary method of connecting unclassified computer systems to the DDN.

Gateway concentrators provide a number of advantages for connecting installations to the DDN:

- **Greater Connection Capacity**
  With the installation of a gateway concentrator at a local site, the number of hosts that can be connected to the DDN is no longer limited by the number of ports available on a PSN. Instead, many hosts can be connected to a concentrator, and the total amount of traffic they pass to the DDN is accommodated by the connection between the gateway concentrator and the MILNET PSN to which it is attached.

- **Quick Connection**
  The gateway concentrator program was designed to allow multiple hosts to access a single DDN port simultaneously. Computers at an installation that requires unclassified worldwide communication will be connected to the Internet automatically because their local networks are attached to the Internet via the concentrator. Thus, these hosts will not require direct connections to DDN ports. This configuration enables the various military services (e.g., Air Force, Army) to manage their host connections directly and to avoid the long wait for individual host connections to DDN ports.

- **Lower Cost Per Host**
  Because of the DDN usage-sensitive billing system structure, the gateway concentrator programs reduce costs for DDN connection. With the installation of a gateway concentrator, the charges for initial host connections are reduced, as the service is charged only once for the initial connection of the concentrator itself rather than for each individual host connection. In addition, traffic between local hosts on the network behind a gateway concentrator will not be billed because such traffic will not travel across DDN facilities.

The Air Force has a help desk at the Internet Control Center (INCC) to aid concentrator users in accessing the DDN:

AFINCC@SERVER.AF.MIL
Headquarters Standard Systems Center/AQFC
Building 857, Room 200A
Gunter Air Force Base, AL 36114-6343
(205) 416-5771, (205) 416-5861; (DSN) 596-5771, 596-5861

8.4 Network Addressing

The network address is the official numeric address of a host, TAC, or gateway (as opposed to the official name by which these entities are addressed). Network addresses take the format "nnn.nnn.nnn.nnn" (dotted decimal format), where nnn represents an up to 3-digit decimal identifier from 0 through 255, and each numeric component is separated from the next with a period. Each decimal part represents one octet of a 32-bit network address. The standard Internet address is divided into two parts: a network part and a local host part. Based on this two-part division, three classes of Internet addresses have been defined: Class A, Class B, and Class C.

CLASS A Network Addresses

Class A network addresses have the following characteristics:

- Composed of a 1-byte network address and a 3-byte local address.
- The highest-order bit of the (1-byte) network address is set to 0.
- Therefore, **the first (or network address) byte of a CLASS A address must be in the range from 0 to 127.**
- Consequently, CLASS A could have as many as 128 networks with 2^{24} (16,7[illegible],216) hosts on each of these networks.

All directly connected MILNET hosts are on network 26, which is a Class A network.

For MILNET hosts,

- the first part of the address is the network number (26);
- the second part is the physical port number on the host's PSN;
- the third part is the logical port number (normally zero for MILNET hosts);
- the fourth part is the number of the PSN to which the host is connected.

Therefore, a host with the address 26.31.0.73 is on network 26 (the number assigned to the MILNET) and is attached to port 31 on PSN 73.

CLASS B Network Addresses

Class B network addresses have the following characteristics:

- The two high-order bytes of the Internet address contain the network number, while the two low-order bytes contain the local host number.

- The highest order bits are set to 10, which means that **the first byte must be a number in the range 128 to 191.**

- Consequently, CLASS B could have as many as 16,384 networks with 2^{16} (65,536) hosts on each of these networks.

CLASS C Network Addresses

Class C network addresses have the following characteristics:

- The network number is contained in the three high-order bytes of the Internet address, while the local host address is represented in the single low-order byte.
- The three highest-order bits of the network address are set to 110.
- Therefore, **the first byte must be in the range 192 to 233.**
- Consequently, CLASS C could have as 2,097,152 networks with 2^8 (256) hosts on each of these networks.

The Internet Registry (IR) at the DDN NIC assigns the network portion of an address to a network. The local network coordinator for a specific host assigns the local portion of that host's network address.

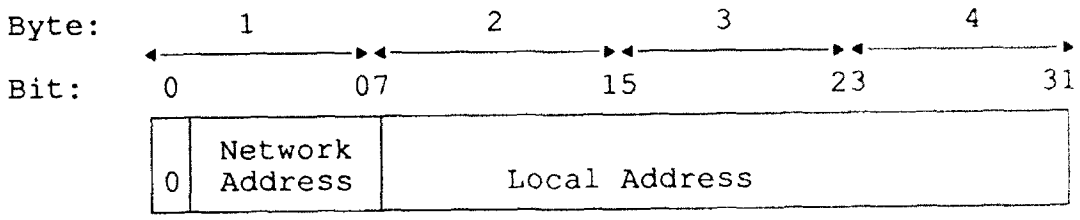
Here are some examples of how each type of network number looks:

Class A:	26.31.0.73	26.0.0.0
Class B:	128.18.1.1	128.18.0.0
Class C:	192.67.67.20	192.67.67.0

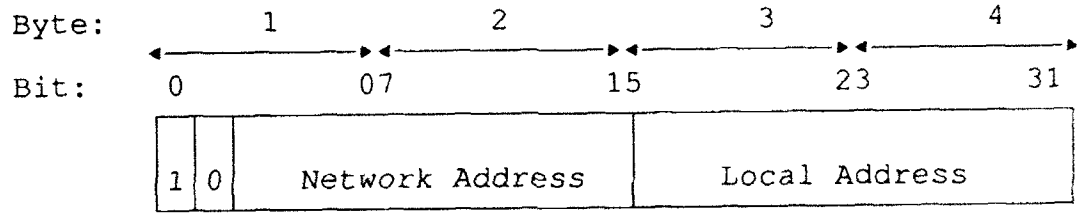
[NOTE: A network address is different from a user's address. The term "user address" refers to a person's electronic mailbox, such as `henry@nic.ddn.mil`.]

In addition to the three classes defined above, a class of addresses whose three highest order bits are 111 has been defined. It is currently in limited use. This class is sometimes referred to as "CLASS D." Figure 8-1 on the next page graphically represents the three major Internet address classes.

CLASS A Internet Address:



CLASS B Internet Address:



CLASS C Internet Address:

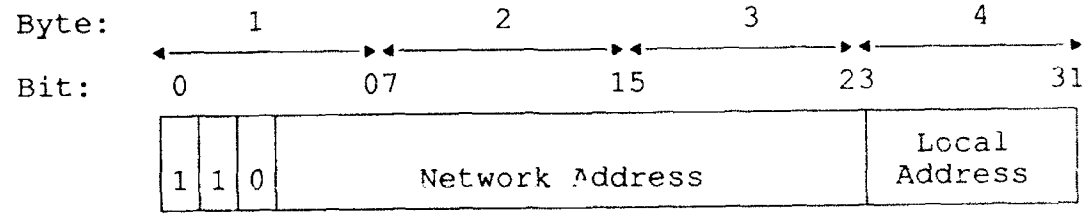


Figure 8-1. Internet Address Classes

8.4.1 Finding Network Address Information

The WHOIS database at the NIC contains POC information for every network the IR (Internet Registry) assigns; however, it may not contain information for every host on a network. Therefore, remember to search on the network portion of the address rather than the complete address when you are using the WHOIS program to obtain information on a host.

For example, the Class C address

```
192.112.36.70
```

is not in the database, but searching on

```
192.112.36.0
```

shows you information for LOCALNET. When using WHOIS to find the POC information for a network, set the local portion(s) of the address to zero. (See Section 6.3.1.3 for an example of using WHOIS to search for a network address.)

8.4.2 Obtaining Network Addresses

DISA assigns all MILNET network addresses (Class A, network 26), and the MILNET Manager must approve any changes to or deletions of MILNET network addresses.

The NIC assigns all other Class B and C network addresses. Requests to obtain an official Class B or C number or to make changes to hosts registered with these addresses should be directed online to HOSTMASTER@NIC.DDN.MIL. To arrange for a hardcopy application, call the NIC at 1 (800) 365-DNIC. Applications can also be requested through the SERVICE mail server (see Section 6.3.5).

8.4.3 Knowing Your Network Address

Each user should know the network address of his/her host. It is especially important to know your host's address if you use a TAC or Mini-TAC because you will have to enter the address as part of the TAC login sequence. Your host address is often—but not always—the address printed on your TAC card by the label AUTHORIZING HOST. Even if you have a script file or program that enters this information for you as you log in, learn your address so you can tell it to the NIC or the MILNET Monitoring Center if you call them about a login problem.

8.5 The Domain Name System

Until the mid-1980s, a DDN host could find data on hostname-to-network-address translation solely through the use of a file called the host table, which was generated at the NIC.

The host table contained the name and network address of every host that was registered with the NIC. Individual host sites had to transfer and install new copies of the host table regularly in order to have correct host addressing information. The host table had to be updated frequently to enable mail and other data to be sent back and forth across the Internet.

As time went on, however, the number of hosts listed in the host table became so large that the file was difficult to maintain efficiently, as well as difficult and time-consuming for sites to transfer. As an alternative to the host table file, the Domain Name System (DNS) was developed. Currently, the NIC maintains data for both the host table and the DNS. The host table listing is an extremely restricted subset of the hosts registered in the Domain Name System.

In a nutshell, the DNS is a way of administratively grouping hosts into a hierarchy of authority. The DNS allows addressing information to be widely distributed and updated locally, which results in more efficient data retrieval and maintenance. Complete conversion to the DNS will eliminate the need for one site to maintain a centralized table of names and addresses.

Under the DNS, host name and address information, along with other data, is distributed throughout the network in a hierarchical scheme. At the top of the hierarchy are the root servers that contain information about the top-level and second-level domains. At the bottom of the hierarchy are the individual hosts.

Each domain within the DNS must have two hosts that provide name service for it, which means that these hosts must run programs called name servers. When queried by programs known as resolvers (located on individual hosts), these name servers provide name and address information to/for the particular hosts within their domain. (The hosts themselves are called servers, even though, technically, a server is a program.) Each server contains a subset of Internet domain information. If a query arrives at a server that does not have address information for a particular host, it will be able to direct the query to the server where the information resides.

Queries regarding specific hostnames usually begin by asking a server that knows about the top-level domain under which that host falls. Currently, most domains on the Internet are registered within one of the following top-level domains:

- COM for commercial institutions
- EDU for educational institutions
- GOV for non-military government agencies and organizations
- MIL for military agencies and organizations
- NET for backbone networking entities
- ORG for non-profit institutions.

Top-level domains are also registered for countries—e.g., BE for Belgium and FI for Finland. The NIC registers information for only the top level of these country domains. Lower-level domains are registered within the country.

Hosts registered on the Internet must have names that reflect the domains under which they are registered. Such names are called Fully Qualified Domain Names (FQDNs) and include all domains of which the host is a part. For example, NIC.DDN.MIL is the name of the NIC's main host. The hostname NIC.DDN.MIL, when taken piece by piece, gives information about the host itself. A hostname ending in MIL signifies sponsorship from a military-related organization. The second-level domain, DDN, indicates that the host is used by an organization within the DDN. The third-level domain, NIC, indicates the host is used by the NIC.

Between the root servers and the individual hosts are other hosts that act as servers and contain part of the information within the DNS hierarchy. For example, a program looking for the address of NIC.DDN.MIL might first send a query to a root server. The root server would not know the address of NIC.DDN.MIL in particular, but would direct the query to another server that had information about the DDN.MIL domain. The second server would know which hosts provide name service about NIC.DDN.MIL and direct the query to those hosts. Finally, the query would arrive at the specific host providing name service for NIC.DDN.MIL. That host would return the network address information via the DNS to the host that initiated the query. All of this happens very quickly—in less than a minute.

Mail programs must know the address of each host to which they send mail. Users normally include a hostname in the headers of their messages. The mail program queries either the DNS or a host table to translate that hostname to a network address. This enables the mail message to be delivered across the network.

For example, if a user named Sam wants to send mail to his friend Joe at the host EXAMPLE.SAMPLE.COM, he can do so in one of two ways.

1. Via the Host Table—

   - The host EXAMPLE.SAMPLE.COM is registered in the host table along with its netaddress.
   - The mail program finds the correct netaddress from the host table on the sender's local host and sends the mail to Joe.

   In this method of transmission, every host that Sam wants to communicate with must be listed in the host table file on his own host. Sam may not be able to reply to messages sent to him if his host does not recognize the hostname in the sender's return address.

2. Via the Domain Name System –

   - The mail program trying to deliver a message addressed to JOE@EXAMPLE.SAMPLE.COM sends a tracker called a query to one of seven root servers.
   - The root server has information on the COM top-level domain and knows which two domain servers hold further information on the SAMPLE.COM domain.
   - The root server points the query to those domain servers.
   - When the query arrives at the ultimate destination server, it learns the netaddress of the host EXAMPLE.SAMPLE.COM, and the mail program obtains the information necessary to establish a path from the sender's host to Joe's host.
   - The query directs the mail down that path to Joe's mail account on the EXAMPLE.SAMPLE.COM host.

8.6 Government Open Systems Interconnection Profile (GOSIP)

The Government Open Systems Interconnection Profile (GOSIP) is a document that describes the Government's plans to transition its networks from the TCP/IP-based protocols to international protocols based on the Open Systems Interconnection (OSI) Reference Model. The goal is to add OSI-based functions to the Internet without sacrificing services now available to Internet users.

Several documents pertain to GOSIP or its implementation; however, we will mention only one resource that will point you toward the most current information available.

RFC 1169, "Explaining the Role of GOSIP," [6] discusses how GOSIP should be applied to near-term network planning and explains the role and applicability of the GOSIP document. In addition, it has an appendix that describes other GOSIP documents and tells how to obtain them. The appendix also lists contacts for further information regarding the documents. This RFC will probably be updated as the status of GOSIP changes, so check the RFC Index, available at the NIC, to ensure that you have the most current information.

SECTION 9. NETWORK SERVICE CENTERS AND CONTACTS

The three main service centers on the DDN are:

- The DDN Network Information Center (NIC)
- The DDN Network Monitoring Centers (NMC) for the United States, Pacific, and European areas
- The Defense Information Systems Agency's Defense Network Systems Organization (DISA DNSO).

This section of the *Guide* describes the services provided by these organizations and gives a list of key contacts for each.

This section also tells you how to obtain the names of other key network contacts, including the following:

- Host Administrators
- Node Site Coordinators
- Military Communications and Operations Command Contacts.

These people and places are sources of network-related information and help, so it is important for you to familiarize yourself with them.

9.1 The DDN Network Information Center (NIC)

The DDN Network Information Center (NIC) is located at Government Systems, Inc. (GSI) headquarters in Chantilly, Virginia. The NIC is funded by the Defense Information Systems Agency's Defense Network Systems Organization (DISA DNSO). Its mission is to provide general reference services to DDN users via telephone, electronic mail, and U.S. mail. The NIC is the first place to turn to if you are not sure who provides the service you need or who is the right person to contact. Section 6 describes the NIC services in detail.

9.1.1 General Reference Service Provided by the NIC

The NIC provides several kinds of user assistance. Its main Help Desk phone numbers are

1 (800) 365-DNIC (inside the U.S.)
1 (703) 802-4535 (outside the U.S. and in the Washington, DC, metro area)

The first number is toll-free. Service is available Monday through Friday, from 7 a.m. to 7 p.m., Eastern time.

The NIC Help Desk assists those who experience problems with the network and with terminal-to-TAC use. In addition, the NIC is happy to answer questions about any other service outlined in this section.

The NIC host computer's hostname and its network address are:

NIC.DDN.MIL 192.112.36.5

NIC online services are available 24 hours a day, 7 days a week.

9.1.2 NIC Online Contacts

The NIC supports several online mailboxes to provide assistance in specific areas.

Type of Inquiry	Network Mailbox
General User Assistance	NIC@NIC.DDN.MIL
TAC and Non-TAC User Registration	REGISTRAR@NIC.DDN.MIL
Urgent Security Matters	NIC-ALERT@NIC.DDN.MIL
Host, Domain, and Net Registration	HOSTMASTER@NIC.DDN.MIL
NIC.DDN.MIL Computer Operations	ACTION@NIC.DDN.MIL
Comments on NIC Publications, Services	SUGGESTIONS@NIC.DDN.MIL
Security Concerns and Questions	SCC@NIC.DDN.MIL
Usage-Sensitive Billing Questions	BILLING@NIC.DDN.MIL
Automatic Mail Service	SERVICE@NIC.DDN.MIL
Reporting NIC Software Bugs	BUG-SERVICE@NIC.DDN.MIL

9.1.3 NIC U.S. Mail Address

Network Information Center
14200 Park Meadow Drive, Suite 200
Chantilly, VA 22021-2219

9.2 Network Monitoring Centers (NMCs)

The three Network Monitoring Centers are:

- The CONUS MILNET Monitoring Center (CMMC) located at DISA headquarters in Washington, DC. The CMMC provides a toll-free hotline Trouble Desk phone number for quick reporting of network problems.
- The Pacific MILNET Monitoring Center (PMMC) located at Wheeler AFB in Hawaii.
- The European MILNET Monitoring Center (EMMC) located in Patch Barracks, Vaihingen, Germany.

All NMCs provide operations support for several DoD packet-switching networks. The NMCs concentrate on real-time network management, with the primary objective of maximizing each network's operating efficiency. In addition, they receive the first DDN security incident reports.

Bolt Beranek and Newman, Inc., Communications Division (BBNCD) provides DDN with operations and technical support, configuration management, software maintenance and enhancement, hardware maintenance, and required hardware.

9.2.1 NMC Services

NMC services include remote status monitoring, coordination of network outage troubleshooting efforts, and 24-hours-per-day, 7-days-per-week technical assistance to users. The NMCs typically work on backbone-related outages consisting of node and circuit problems; they provide help in determining whether host connectivity problems are network related.

Your Host Administrator contacts the appropriate NMC for all network hardware problems, hardware field service, problems with host interfaces, suspected node software problems, or DDN security problems.

9.2.2 NMC Contacts

Title	Telephone	Network Mailbox
CONUS MMC	1 (800) 451-7413 1 (703) 692-2268 1 (703) 692-5726	DCA-MMC@DCA-EMS.DCA.MIL
European MMC	011 49 711 687 7766	STT-CONTROL@FRG.BBN.COM
Pacific MMC	1 (808) 656-1472	PMMC@PAC-MILNET-MC.DCA.MIL

9.2.3 NMC U.S. Mail Addresses

CONUS MILNET Monitoring Center
DISA Headquarters
701 South Courthouse Rd.
Arlington, VA 22204-2199
Attn: MILNET Manager

Pacific MILNET Monitoring Center
Defense Information Systems Agency, Pacific
Wheeler AFB, HI 96854-5000
Attn: P-600

European MILNET Monitoring Center
BBNCD
DISA-Europe
Box 1000, Att: DED
APO AE 09131-4103

9.3 Host Administrators and Node Site Coordinators

Each host has a representative who serves as its technical and administrative contact—the Host Administrator. The Host Administrator provides important host-related services such as the following:

- Collaborates with the DDN PMO on security matters involving hosts,
- Interprets network policies as they apply to his/her host,
- Decides which users may access the network (within the guidelines set by the DDN PMO),
- Authorizes user access to the MILNET Terminal Access Controllers (TACs) and Mini-TACs,
- Helps network users with technical problems involving hosts, and
- Works with the Network Information Center and the Network Monitoring Centers to provide information and technical assistance.

Each network node, or PSN, has a Node Site Coordinator (NSC). The Node Site Coordinator is the local site representative who has access control, accountability, and coordination responsibility for the DDN-owned network hardware, software, and circuits located at the node site.

Occasionally, one person serves both roles. A Host Administrator or Node Site Coordinator may also designate an alternate who can assist with the administrative or technical demands of the position.

To find the names, addresses, telephone numbers, and network mailboxes for these contacts, see Section 6.3.

9.4 Military Communications and Operations Command Contacts

Each military department has designated an organization to serve as the primary DDN Point of Contact. Requests for information or assistance should be directed to the following organizations:

Service	Address	Telephone	DSN
Air Force	AFDDN PMO Gunter AFS, AL 36224-6340	1 (205) 279-4075/3290	446-4075
Army	USAISC, AS-PLN-RF Fort Huachuca, AZ 85613-5000	1 (602) 538-6915	879-6915
Navy	COMNAVTELCOM, Code N521 Washington, DC 20390-5290	1 (202) 282-0381/2	292-0381

9.5 Defense Information Systems Agency, Defense Network Systems Organization (DISA DNSO)

[NOTE: The Defense Communications Agency, DCA, became the DISA in 1991; in the same year, the Defense Communications System Organization became the DNSO.]

The Defense Information Systems Agency, Defense Network Systems Organization (DISA DNSO) is responsible for overall management of the Defense Data Network (DDN). DDN Newsletter 58, available online as DDN-NEWS/DDN-NEWS-58.TXT from the NIC.DDN.MIL host, contains the most current listing of DISA DNSO personnel and their areas of responsibility. Contact the NIC to ensure that this newsletter still reflects the most current information on DNSO staff contacts.

9.6 If You Have a Network Use Problem

For Questions on:	Contact:
Terminal settings	Host Administrator or User Representative
Host login	Host Administrator or User Representative
MILNET TAC access	Host Administrator for your primary MILNET host
TAC login procedure	Network Information Center
TAC line problems	TAC Node Site Coordinator or the Monitoring Center
TAC phone numbers	NIC TACNEWS program
General DDN information	Network Information Center
Host line problems	Respective Network Monitoring Center

This page has been left blank intentionally.

SECTION 10. BIBLIOGRAPHY

Many of the manuals and documents listed below are cited in this *Guide*; others provide information that should be helpful to you as users of the DDN. When available, ordering numbers are given for items that can be ordered from the Defense Technical Information Center (DTIC)[1] or from DISA. Hardcopies of some of the documents are available from SRI International, Menlo Park, CA.

If the NIC offers online versions, the filenames are shown in brackets.

Cited References

1. *TAC Users' Guide*. DCAC 310-P70-74. June 1988.

2. *DDN Subscriber Interface Guide*. Defense Data Network, Program Management Office, Defense Information Systems Agency, 701 S. Courthouse Rd, Arlington, VA 22204-2199. 1983. (AD-A132 877/2).

3. DeLauer, R.D., *DoD Policy on Standardization of Host-to-Host Protocols for Data Communications Networks*. Office of the Secretary of Defense, Washington, D.C., March 1982. [ien/ien-207.txt]

4. Carlucci, F. C., "Autodin II Termination," Memorandum for Secretaries of the Military Departments, Deputy Secretary of Defense, Washington, D.C., April 1982.

5. Defense Information Systems Agency, DDN Network Systems Organization. Defense Data Network Management Bulletin 76, "TAC User Registration Clarification." Menlo Park, CA. SRI International, 24 August 1990. 1 p. [ddn-news/ddn-mgt-bulletin-76.txt]

6. RFC 1169, *Explaining the Role of GOSIP*. August 1990. 15 p. [rfc/rfc1169.txt.]

7. Defense Information Systems Agency, Defense Network Systems Organization. Defense Data Network Security Bulletin 9003, "Security Violation Reporting." Menlo Park, CA: SRI International, DDN Security Coordination Center; 15 February 1990; DDN Security Bul. 9003. 2 p. [scc/ddn-security-9003]

8. RFC 1177, FYI on Questions and Answers: Answers to commonly asked "new Internet user" questions. August 1990. 24 p. (Also FYI 4) [rfc/rfc1177.txt]

9. Defense Information Systems Agency, DDN Network Systems Organization. Defense Data Network Management Bulletin 101, "MILNET TAC User Validation and Registration." Chantilly, VA. GSI, Inc., 24 September 1992. 5 p. [ddn-news/ddn-mgt-bulletin-101.txt]

[1]Order from: DTIC, Cameron Station, Alexandria, VA 22314. Tel: (202) 274-7633.

General References

Bolt Beranek and Newman Inc. *A History of the ARPANET: the First Decade.* Report No. 4799, Defense Advanced Research Agency, Arlington, VA, 1981. [AD-A1115 440].

Cerf, V. and Lyons, R. "Military Requirements for Packet-Switched Networks and Their Implications for Protocol Standardization." *Computer Networks.* 7(5): 293-306; October 1983.

Chou, W. (Ed.). *Computer Communications: Principles.* Englewood Cliffs, NJ: Prentice-Hall, Inc.; 1983.

Comer, D.E. *Internetworking with TCP/IP: Principles, Protocols, and Architecture.* Englewood Cliffs, NJ: Prentice-Hall, Inc.; 1988. 382 p.

DDN Defense Data Network Brochure. Defense Information Systems Agency, Defense Network Systems Organization, Washington, DC, 1984.

DDN Protocol Handbook, 4 Volumes. SRI International (NIC), Menlo Park, CA. 1985.

DDN Subscriber Security Guide. Defense Data Network, Program Management Office, Defense Information Systems Agency, Washington, D.C. 1983. [AD-A152 524]

Frey, D.; Adams, R. *!%@:: A Directory of Electronic Mail Addressing and Networks.* Newton, MA: O'Reilly and Associates; August 1989. 284 p.

FYI 2; *FYI on a network management tool catalog: Tools for monitoring and debugging TCP/IP internets and interconnected devices.* April 1990. 126 p. (Also RFC 1147) [fyi/fyi2.txt]

FYI 3; *FYI on where to start: A bibliography of internetworking information.* August 1990. 42 p. (Also RFC 1175) [fyi/fyi3.txt]

Hinden, R., Haverty, J. and Sheltzer, A. "The DARPA Internet: Interconnecting Heterogenous Computer Networks with Gateways." *Computer.* 16(9): 38-48; September 1983

Jennings, D.M., et al "Computer Networking for Scientists." *Science.* Vol 231: 943-950; February 1986.

LaQuey, T.L. (Ed.) *Users' Directory of Computer Networks.* Bedford, MA: Digital Press; 1990. 630 p.

Network Protocol Implementations and Vendors Guide. SRI International (former DDN NIC), Menlo Park, CA. 1990. [netinfo/vendors-guide.doc]

Partridge, C. (Ed.) *Innovations in Internetworking.* Norwood, MA: Artech House; 1988.

Perry, D.G., et al — *The ARPANET and the DARPA Internet.* Library Hi Tech. 6(2): 51-62; April 1988.

Quarterman, J.S. — *Matrix: Computer Networks and Conferencing Systems Worldwide.* Bedford, MA: Digital Press; 1989. 719 p.

Ubois, J. — "Defense Data Network." *National Defense.* Vol.74: 33-35; February 1990.

This page has been left blank intentionally.

SECTION 11. GLOSSARY

acoustic coupler — A type of modem that converts digital signals into sound for transmission through telephone lines and performs the reverse operation when receiving such signals. Acoustic couplers generally have cups into which the telephone handset is placed to make the connection.

anonymous login convention — Standard username (anonymous) and password (guest) that allows a user to log in within FTP for the purpose of retrieving an unprotected public access file.

ARPANET — Packet-switched network developed by the Defense Advanced Research Projects Agency.

ASN — Autonomous System Number. A number assigned by the NIC to an autonomous network that request connection to the Internet.

backbone — The nodes (PSNs), the TACs, and the telephone lines connecting them that form the core of the DDN.

BBNCD — Bolt Beranek and Newman, Inc., Communications Division; a major hardware and software developer for the DDN.

bps — Bits per second. The unit used for measuring line speed, i.e., the number of information units transmitted per second.

case sensitive — Software differentiation between uppercase and lowercase characters.

CERT — Computer Emergency Response Team, the DARPA-sponsored group responsible for coordinating many security incident response efforts.

circuit-switched — A type of network connection. A circuit-switched connection is a continuous electrical connection established between sending and receiving users for their exclusive use. The connection remains active until it is closed by the using parties.

concentrator — A gateway; that is, a computer that interconnects networks.

connection — An access path between two ports on a network, established for data transmission between the ports.

CONUS — Military acronym for the Continental United States.

DARPA — Defense Advanced Research Project Agency. The agency that created and administered the ARPANET.

DCA DCSO — Defense Communications Agency, Defense Communications System Organization; the group responsible for administering the DDN. (Now known as the Defense Information Systems Agency, Defense Network Systems Organization—DISA DNSO.)

DDN	Defense Data Network. The DoD long-haul, packet-switched computer communications network that includes the MILNET as one of its subnetworks.
DIIS	The DDN Installation and Information Services contract, which encompasses the NIC and its services. Also the NIC handle of the DIIS.DDN.MIL host.
DISA DNSO	Defense Information Systems Agency, Defense Network Systems Organization. Formerly the DCA DCSO (see above).
DNS	Domain Name System. The hierarchical, distributed database used for host name and address resolution that has replaced the need for a centralized host table.
DoD	Department of Defense.
DRI	Defense Research Internet. A network that will provide state-of-the-art internetworking services for the DoD. It is still in the planning stages.
DSN	Defense Switched Network. A proprietary Government telephone network.
DTIC	Defense Technical Information Center, Cameron Station, Alexandria, VA 22314. A depository for many DoD technical reports.
FQDN	Fully Qualified Domain Name. The complete hostname that reflects the domains of which the host is a part.
FTP	File Transfer Protocol. A network utility for copying files across the network; defined in RFC 959.
FYI	A "For Your Information" document, issued also as an RFC, that contains information of general interest to the Internet community.
gateway	A computer that interconnects networks.
GOSIP	Government Open Systems Interconnection Profile. A document that addresses the DDN's planned transition from TCP/IP protocols to OSI protocols.
handle	Unique character string identifier assigned to each entry in the NIC WHOIS database.
host	A computer connected to a PSN on the DDN.
hostname	A name that officially identifies each computer attached to the DDN.
IMP	Interface Message Processor; see PSN.
INCC	The Internet Control Center. The service center that provides help to Air Force concentrator users.
Internet	The specific IP-based internetwork of which the DDN is a part.
internetwork	A network, such as the DDN, that consists of many interconnected networks.
IP	Internet Protocol. A DoD standard protocol that allows dissimilar hosts to connect to each other through the DDN, defined in RFC 791.

IR	Internet Registry. The function at the NIC that assigns official IP network numbers.
Kermit	An error-checking file-transfer protocol used to copy files from one computer to another. Also the name given to the public domain software, distributed by Columbia University, that supports this protocol.
LAN	Local Area Network. A network of directly connected machines usually located within 10 miles of one another.
long-haul net	A network spanning long geographic distances, usually connected by telephone lines or satellite radio links.
mailbridge	A gateway between the MILNET and the Internet, through which mail and other data passes.
MIL STD	Military Standard. The official military version of a specification.
MILNET	The DDN unclassified operational military network.
modem	A device that converts digital signals into analog signals (and back) for transmission over telephone lines (modulator/demodulator).
MTAC	Or Mini-TAC. A new, improved machine that allows remote network access in essentially the same manner as a TAC, but accommodates a wider variety of operating systems.
NETINFO	The name of the publicly accessible directory on the NIC.DDN.MIL host that stores many files of interest to users of the network.
network	The hardware, software, and connections needed to distribute the processing of data in a reliable and efficient manner and to enable users to exchange and share that data.
NIC	DDN Network Information Center, located at GSI headquarters in Chantilly, VA.
NIC.DDN.MIL	The hostname of the NIC host. Its network address is 192.112.36.5.
NICNAME	See WHOIS.
NIC/Query	A general information program on NIC.DDN.MIL.
NMC	Network Monitoring Center. The CONUS MILNET NMC is located at 701 S. Courthouse Rd., Arlington, VA 22204-2199. Others are located in Europe and Hawaii.
NNSC	The National Science Foundation's Network Service Center. The center that provides support for the NSFNet backbone. The NNSC also publishes the Internet Resource Guide.
node	On the DDN, a packet switch or PSN. A computer that handles network message traffic.
NREN	The National Research and Education Network, the planned high-speed national network that will provide a platform for research and educational networking efforts.
NSC	Node Site Coordinator. The local DDN contact responsible for node or TAC equipment.
NSFNet	The packet-switched network that is the backbone of much of the Internet.

NSO	Network Security Officer. The NSO is responsible for setting DDN security policy and overseeing its implementation.
NTIS	National Technical Information Service, U.S. Department of Commerce, Springfield, VA 22151, (703) 487-4650. A national depository for unclassified technical documents.
OCONUS	A military acronym for "Outside the Continental U.S."
operating system	Software that supervises and controls tasks on a computer.
OSD	Office of the Secretary of Defense.
packet switching	A data transmission system that uses addressed packets, and in which a communications channel is occupied only for the duration of the packet transmission.
pathname	A character string that fully identifies a file. Pathnames normally contain (or imply) device and/or directory names and a filename specification. FTP, TELNET, and electronic mail do not specify a standard pathname convention. Each user must follow the file naming conventions of the file systems he wishes to use.
packet	The basic unit of data transmitted over the DDN. Each packet contains a header, which consists of addressing and other control information and, optionally, any associated data destined for a network user process.
POC	Point of Contact.
protocol	Technical specifications governing the format and timing of information exchange between two communicating software processes.
PSN	Packet Switch Node. A store-and-forward packet switch (formerly called an IMP).
RFC	Request For Comment. A series of technical notes describing DARPA and DDN research and development, particularly in the areas of protocol design and internetworking. Available for anonymous FTP at NIC.DDN.MIL in the /rfc directory.
SCC	The Security Coordination Center, located at the NIC, that is responsible for collecting security-related information, cooperating with the NSO in security incident response, and issuing DDN Security Bulletins.
server	A process providing a generalized service to subscribing user processes. Server processes normally "listen" on a network address, ready to respond to an incoming service request. The FTP Server is such a process; it responds to file transfer requests from FTP users.
SERVICE	The name of the NIC's automatic mail server, SERVICE@NIC.DDN.MIL. Send a message to SERVICE@NIC.DDN.MIL with subject: HELP for more information.
session	The time during which a connection remains open between a user and server port on a network. For example, in an FTP session, the end-user invokes FTP, names the server host he wishes to connect with, issues FTP commands, and logs off.
SIG	Special Interest Group. An online mailing group whose members exchange information on a particular topic.

site	Organization or facility where a host is located.
SMTP	Simple Mail Transfer Protocol. Defined in RFC 821.
socket	Logical address of a communications access point to a specific device or program on a host.
SRI	SRI International, Menlo Park, CA, former location of the DDN Network Information Center and early contributor to the development of the DDN.
SunOS	Sun Microcomputer Systems' proprietary UNIX-based operating system. The operating system used by the NIC host.
TAC	Terminal Access Controller. A special type of computer attached to a PSN. It allows direct terminal access to the DDN backbone.
TAC Access Code	Password assigned to MILNET TAC users for TAC login.
TAC Userid	Alphanumeric character string that identifies a TAC user upon TAC login.
TACACS	TAC Access Control System. A password system that limits use of TACs to authorized users.
TACNEWS	NIC program for reading DDN Newsletters, Bulletins, and other items of interest to TAC users.
TCP/IP	Transmission Control Protocol/Internet Protocol. DoD standard network protocols defined in RFC 793 (TCP) and RFC 791 (IP).
TELNET	A protocol for opening a transparent connection to a distant host; defined in RFC 854.
terminal	A communication device that lets a user send information to a computer by typing on a keyboard. It prints responses from the computer on paper or a screen.
TIP	Terminal Interface Processor. A predecessor of the TAC, serving a similar function. See TAC.
UNIX	An AT & T Bell Laboratories proprietary operating system that runs on large and small computers. It has become widely used in the scientific research and development community.
user	A human end-user or an automated user process authorized to access network services.
WHOIS	NIC program used to access the NIC electronic white pages database.

This page has been left blank intentionally.

APPENDIX A. NETWORK RESOURCES

One of the questions new users frequently ask when they finally get access to the network is, "Now what? What's out there?" This section lists a few places you can look for more information about what is available to Internet users.

Special Interest Groups

An important part of the Internet are its many online Special Interest Groups (SIGs), which discuss topics ranging from artificial intelligence to Zenith PCs. A SIG is an electronic mailing list dedicated to the discussion of a particular topic. SIGs are a good way for a new user to learn more about the network. Anyone can contribute to a SIG by simply sending mail, and most SIGs are open for anyone to join. Information on network SIGs can be found in a file nicknamed the List-of-Lists, a master list of SIGs with a brief description of each group and how to join it.

For users who have never done a file transfer before, this is a perfect first opportunity. You can use FTP to copy the List-of-Lists from the FTP.NISC.SRI.COM host by logging in with "`USERID anonymous`" and "`PASSWORD guest`" and using the pathname NETINFO:INTEREST-GROUPS.

Note that many individual hosts redistribute mail for their users—that is, mailing list messages or digests are delivered once to a single local mailbox, and then they are announced or forwarded to a list of interested local users. Mail redistribution eliminates the need for the local mailer to process myriad copies of the same message directed to different users and so conserves local computer resources. Before adding your name to a SIG distribution list, ask your Host Administrator or User Representative if SIG or digest mail is redistributed on your host or posted in a centralized place to be read by all local users.

In addition, all traffic on the MILNET is subject to usage-sensitive billing, so before adding your name to a SIG, be sure that the mail traffic you would generate is consistent with the usage policies of your host.

NNSC Internet Resource Guide

The NSF Network Service Center (NNSC) compiles and makes available an *Internet Resource Guide*. The goal of the guide is to increase the visibility of various Internet resources that might help users do their work better. While not yet an exhaustive list, the guide is a useful compendium of many resources and can be very helpful to a new user.

In the NNSC guide, resources are grouped into sections by type. Current sections include descriptions of online library catalogs, data archives, online white pages directory services, networks, network information centers, and computational resources such as supercomputers. Each entry contains the following information:

- a description of the resource,
- an identification of who can use the resource,
- an explanation of how to reach the resource network via the Internet,
- a list of contacts for more information.

The NNSC distributes the list electronically. To receive a guide, or to get on a mailing list that alerts you when it is updated, send a message to RESOURCE-GUIDE-REQUEST@NNSC.NSF.NET.

FYI Documents

"FYIs" are a series of special RFCs. The FYI documents address information that is of general interest to the Internet user community. They do not define standards or contain protocol specifications. Rather, they address more general topics, provide insight into Internet conventions, answer commonly asked questions, contain background or historical information, or provide resource information such as bibliographies or descriptions of software. Some FYIs are addressed specifically to new users.

Because FYIs are also RFCs, they are listed along with all the other RFCs in the RFC Index. However, the file fyi/fyi-index.txt on the NIC host lists only the FYIs. Each index notes both the FYI number and the RFC number of each FYI. You can obtain the FYI Index online by FTPing it or by requesting it through the SERVICE@NIC.DDN.MIL mail service. See Section 5.1.2 for FTP guidelines and Section 6.3.5 for directions on retrieving information via SERVICE.

NIC Contacts Files

Often users need to communicate with the official Point of Contact (POC) responsible for a specific network or domain. While this information is available via the WHOIS program on the NIC host, as described in Section 6.3.1, the NIC also provides files that contain compilations of the contacts for domains and networks. These files are updated weekly and provide a central resource for useful domain and network POC information.

- netinfo/network-contacts.txt lists all assigned networks by number and lists the name of the network, plus the name, phone number, and electronic mailbox for each POC.

- netinfo/domain-contacts.txt is organized by domain name and lists the name, phone number, and electronic mailbox for each domain POC.

With the network information sources and contacts just outlined and the tools introduced in the previous section, you are now ready to explore the network on your own.

APPENDIX B. COMMONLY ASKED QUESTIONS

Here are answers to some of the questions most commonly asked by users. The selections were made from questions addressed to the DDN Network Information Center. (See Sections 6.1 for NIC network and U.S. mail addresses.)

1. I want to send mail to my colleague, John Smith. What is his network mailbox?

   Answer:
   The NIC provides an online program called WHOIS (or NICNAME) that contains the names, addresses, phone numbers, and online mailboxes of many network users. Since some Host Administrators install this program on their host, you should ask him/her if it is available locally. Alternatively, you may make a TELNET connection to NIC.DDN.MIL and use the WHOIS program running on the NIC host. (Login to NIC.DDN.MIL is not required.) The WHOIS program may also be accessed via electronic mail. Send a message to SERVICE@NIC.DDN.MIL and include the word WHOIS and the item you wish to search for in the subject line of your message. You will receive an answer overnight. For more information on using SERVICE, see Section 6.3.5.

2. This TAC phone number doesn't work. What should I do?

   Answer:
   The Network Information Center can try to access the TAC from its site to determine if the problem is in the TAC or if it relates to your equipment or the procedure you are using. If the problem is the TAC, we can give you phone numbers for other TACs. We can help you coordinate with the MILNET Monitoring Center to report the TAC problem.

3. I will be traveling and need to log in to read my mail. How can I find a TAC phone number to use while I'm on the road?

   Answer:
   You can locate TAC phone numbers in several ways. The back of your TAC card lists many of them. The TACNEWS program available on the NIC.DDN.MIL host has a menu option that will show you the three TACs closest to a phone number you provide. TACNEWS also provides lists of phone numbers for TACs both within and outside the U.S. See Section 6.3.2.1 for an example of TACNEWS usage. In addition, if you call the NIC Help Desk, we will be happy to provide you with phone numbers of TACs.

4. What is the difference between the MILNET and the DDN?

   Answer:
   The MILNET is a wide area network that constitutes one subnetwork of the DDN. The MILNET carries unclassified operational data. It is the segment of the DDN that is connected to the Internet. The other subnetworks of the DDN carry classified information and are standalone networks.

5. What is the difference between the MILNET and the Internet?

Answer:
The Internet is a collection of TCP/IP-based wide area and local area networks that are interconnected by various gateways so that users on one network can communicate to users on any of the other networks. In addition, some non-TCP/IP-based networks, such as BITNET, are accessible to Internet users via electronic mail. These networks are usually not strictly considered a part of "the Internet." The MILNET is a wide area network that is connected to the Internet via connections called the Federal Inter-agency Exchanges (FIXs).

6. I see a connection on my host from a network number I don't recognize. How can I find the number of someone to contact on that network to check on this connection?

Answer:
Every IP network number assigned by the Internet Registry at the NIC has a registered Point of Contact (POC) who is responsible for that network. To find a particular POC, you can look up the number of the network via the NIC's WHOIS program. Search only on the network portion of the number and type the local portions as zeroes. (See Section 8.4 for a brief explanation of network addressing. See Section 6.3.1 for how to use WHOIS.) In addition, the NIC provides a publicly accessible, regularly updated file that lists all the POCs for each network number assigned. The file is `netinfo/network-contacts.txt`. The POC information is listed by network number.

7. How do I get a TAC card?

Answer:
Before you can get a TAC card, you must have an account on a host. Then the Host Administrator of a MILNET host (that is, a host whose address is on network 26) must approve a TAC card for you. See Section 4 for a more complete explanation of TAC cards and TAC usage.

8. What is an RFC?

Answer:
As RFC 1177 [8] explains, the Request for Comments documents (RFCs) are working notes of the Internet research and development community. A document in this series may be on essentially any topic related to computer communication, and may consist of anything from a meeting report to the specification of a standard. Most RFCs are descriptions of network protocols or services, often giving detailed procedures and formats. These RFCs generally provide information in sufficient technical detail to enable developers to create implementations. Other RFCs report on the results of policy studies or summarize the work of technical committees or workshops. Currently, all Internet standards are published as RFCs, but not all RFCs are standards. RFCs are publicly available on the NIC.DDN.MIL host. Indexes of RFCs organized by number (in reverse order with the most current RFC at the top), by author, or by title are available from the NIC as well. Hardcopies are available from SRI International in Menlo Park, CA (the former NIC).

9. May I be registered in the WHOIS database?

Answer:
Any TAC user must be registered with the NIC. In addition, any other MILNET user can be added to the WHOIS database if he has a working network mailbox. Information regarding a registered user,

such as his address and network mailbox, is visible via the WHOIS program. Thus, WHOIS acts as a "white pages" directory of network users, enabling other users to ascertain where to send mail to them, either electronically or via the U.S. postal service. To register in the database, fill out the template provided in Section 6.2.1 (or the version currently approved and located in the NIC `templates` directory) and return it online to `REGISTRAR@NIC.DDN.MIL`. The NIC depends on users to send updated information whenever their addresses or mailboxes change.

This page has been left blank intentionally.

INDEX