DataGeneral

Customer Documentation

Managing and Operating the XODIAC™ Network Management System

Managing and Operating the XODIAC™ Network Management System (AOS and AOS/VS)

093-000260-02

For the latest enhancements, cautions, documentation changes, and other information on this product, please see the Release Notice (085-series) supplied with the software.

Ordering No. 093-000260

Revision 02, February 1986

NOTICE

Managing and Operating the XODIAC™ Network Management System
(AOS and AOS/VS)
093-000260-02

Revision History:

Original Release – February 1980
First Revision – October 1981
Addendum 086-000073-00 – September 1984
Second revision – February 1986

Effective with:

XODIAC Rev. 5.10
AOS Rev. 7.00
AOS/VS Rev. 6.00

This document has been extensively revised from the previous revision; therefore change indicators have not been used.

Preface

This manual describes how to manage and operate Data General's XODIAC™ Network Management System under AOS and AOS/VS. The manual is for network administrators, managers, and operators who have responsibility for designing, configuring, or maintaining a XODIAC network.

The administration, management, and operation tasks include the following:

- Loading the network tapes into the proper directories.
- Designing a network—deciding what devices, links, local hosts, remote hosts, and processes should be on the network and how they should be configured.
- Generating the local network.
- Changing the network files each time the physical network changes.
- Changing network parameters as problems occur so that the network operates as efficiently as possible.
- Bringing up and taking down the network.
- Bringing up each network process, monitoring its performance, and terminating it when necessary.
- Assigning select users access privileges to network hosts.
- Devising methods of protecting the integrity of the files both on your system and on the remote hosts to which your system is connected.
- Understanding and interpreting the system log file.
- Troubleshooting problems that may occur on the network.
- Backing up and restoring files over the network.

This manual is organized as follows:

Chapter 1	Introduces Data General's XODIAC Network Management System, describes each of the network agents, and tells how to display on-line help.
Chapter 2	Tells how to set up the XODIAC software on your system.
Chapter 3	Discusses system security and suggests how you can protect the network by using ACLs, user profiles, and the XODIAC Routing Analyser.
Chapter 4	Describes how to run NETGEN to create a network specification file and how to generate a network.
Chapter 5	Describes how to use NETGEN to configure specific controllers.
Chapter 6	Presents a sample network and demonstrates how you can configure it.

Chapter 7	Describes the XODIAC Routing Analyzer (XRA), and tells how to use it to route data on a large network.
Chapter 8	Describes how to control the network, using the network operating process, NETOP. Tells how to bring the network up and down and gives suggestions about handling network problems.
Chapter 9	Describes the commands for controlling X25, the transport service for AOS systems.
Chapter 10	Describes the commands for controlling XTS, the transport service for AOS/VS systems.
Chapter 11	Describes the commands for controlling the Resource Management Agent (RMA).
Chapter 12	Describes the commands for controlling the File Transfer Agent (FTA).
Chapter 13	Describes the commands for controlling the Virtual Terminal Agent (VTA).
Chapter 14	Tells how to back up and restore files over the network.
Appendix A	Shows the parameters that the system log file uses for X.25 information.
Appendix B	Describes how to use the NTRACE program to display the results of a network packet trace.
Appendix C	Suggests resolutions for common network problems.

Related Manuals

In addition to this manual, the following Data General manuals may be helpful:

AOS and AOS/VS User's Handbook has reference information on CLI commands.

Advanced Operating System (AOS) Programmer's Manual (93-000120) and *Advanced Operating System/Virtual Storage (AOS/VS) Programmer's Manual,* Volume 1, *System Concepts* (93-000335) explain operating system concepts.

AOS/VS INFOS® System User's Manual (093-000299) has information on RIA, the Remote INFOS Agent.

Command Line Interpreter (CLI) User's Manual (AOS and AOS/VS) (093-000122) describes how to communicate with AOS and AOS/VS, using the CLI.

Data General/Database Management System (DG/DBMS) Reference Manual (093-000163) has information on RDA, the Remote Database Agent.

How to Generate and Run AOS (093-000217) tells how to generate and operate the AOS operating system.

How to Generate and Run AOS/VS (093-000247) tells how to generate and operate the AOS/VS operating system.

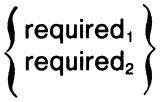
Programming with the XODIAC™ Network Management System (AOS and AOS/VS) (093-000175) describes the X.25 protocol and its relationship to the XODIAC Network Management System.

Using the XODIAC Network Management System (AOS and AOS/VS) (093-000178) explains how to use the XODIAC agent processes.

Reader, Please Note

The following conventions are used in this manual:

COMMAND required *[optional]* ...

Where	Means
COMMAND	You must enter the command (or its accepted abbreviation) as shown.
required	You must enter some argument (such as a filename). Sometimes, we use:  which means you must enter one of the arguments. Don't enter the braces; they only set off the choice.
[optional]	You have the option of entering this argument. Don't enter the brackets; they only set off what's optional.
...	You may repeat the preceding entry or entries. The explanation will tell you exactly what you may repeat.

Additionally we use certain symbols in special ways:

Symbol	Means
⤸	Press the NEW LINE or carriage return (CR) key on your terminal's keyboard.
)	is the CLI prompt.

All numbers are decimal unless we indicate otherwise.

Finally, in examples we use

THIS TYPEFACE TO SHOW YOUR ENTRY ⤸
THIS TYPEFACE FOR SYSTEM QUERIES AND RESPONSES

End of Preface

Contents

Chapter 1 - Introduction

Chapter 2 - Loading the Network Software

Chapter 3 - System Security

Chapter 4 - The Network Generation (NETGEN) Program

Chapter 5 - Configuring Specific Controllers and Other Communications Media

Chapter 6 - A Sample NETGEN Session

Chapter 7 - Using the XODIAC Routing Analyzer (XRA)

Chapter 8 - Controlling Network Processes

Chapter 9 - Using NETOP with X25

Chapter 10 - Using NETOP with XTS

Chapter 11 - Using NETOP with RMA

Chapter 12 - Using NETOP with FTA

Chapter 13 - Using NETOP with SVTA

Chapter 14 - Using XODIAC to Load Software and Back Up Files

Appendix A - SYSLOG Formats for Accounting Information

Appendix B - The NTRACE Program

Appendix C - Network Problems

Tables

Table

Illustrations

Figure

Chapter 1
Introduction

This chapter gives a brief introduction to the XODIAC™ Network Management System and particularly to the manager and operator interfaces documented in this manual.

The Composition of the XODIAC™ Network Management System

The XODIAC Network Management System is a set of software products that lets interconnected systems exchange data and share resources. The products can be divided into three groups: the XODIAC transport service, the XODIAC agents, and the XODIAC management utilities. The following sections describe these groups.

The XODIAC Transport Service

The function of a transport service is to establish and maintain a connection between two remote hosts. It is also responsible for packaging user data into packets, and for sending and receiving the packets across the network.

XODIAC's transport service is an implementation of the international standard access protocol known as X.25. Under AOS, the transport service is provided by the X25 process. Under AOS/VS, it is part of the XODIAC Transport Service (XTS) process. In addition, AOS/VS supports Routing XTS, which can accept a packet from one host and forward it to its proper destination. The AOS and AOS/VS products are fully compatible.

For more information on Data General's X.25 implementation, including the programming interfaces to X.25, see *Programming with the XODIAC™ Network Management System.*

The XODIAC Agents

The XODIAC agents are processes that provide network services to the user. The agents all have interactive interfaces that provide immediate access to network services. In addition, some of the agents have programming interfaces. The agents are as follows:

Agent	Service Provided
Virtual Terminal Agent (VTA)	Lets you log on to a remote AOS or AOS/VS system, as if your terminal were directly connected to the remote system.
File Transfer Agent (FTA)	Lets you transfer files efficiently between your local system and a remote AOS or AOS/VS system.
Resource Management Agent (RMA)	Lets you access files, queues, devices, and processes on a remote AOS or AOS/VS system.
X.29/Host Packet Assembler/Disassembler (X.29/Host PAD)	Lets you log on to a remote AOS or AOS/VS system through a public data network.
Remote INFOS II Agent (RIA)	Lets you access remote INFOS® II files across a network.
Remote Database Agent (RDA)	Lets you access a remote DG/DBMS database across a network.

For information on the interactive interfaces to VTA, FTA, RMA, and X.29/Host PAD, see *Using the XODIAC™* Network Management System. For information on the programming interfaces to FTA and RMA, see *Programming with the XODIAC™* Network Management System. For information on RIA, see the *AOS/VS INFOS® II System User's Manual.* For information on RDA, see the *Data General/Database Management System (DG/DBMS) Reference Manual.*

The XODIAC Management Utilities

The XODIAC management utilities provide interactive interfaces for configuring, creating, and controlling a XODIAC network. This manual documents the XODIAC management utilities. They are as follows:

Utility	Function
Network Generation Program (NETGEN)	Configures and generates a new network, and changes an existing network. NETGEN is a menu-driven utility that prompts you to supply information describing your host's network hardware and software. NETGEN then translates your input into a form that the XODIAC software can use to read the parameters you have set.
Network Operator Process (NETOP)	Creates, controls, and terminates the XODIAC processes (that is the transport service process and the agent processes). You issue NETOP commands from the CLI.
XODIAC Routing Analyzer (XRA)	Generates and updates routing tables for the entire network. XRA is a menu-driven utility. Its use is optional, but it can be helpful in configuring correct and efficient routing paths for a large network.

Chapters 4 through 6 describe NETGEN. Chapter 7 describes XRA. Chapters 8 through 13 describe NETOP.

Manager and Operator Tasks

The XODIAC management utilities, documented in this manual, help perform the tasks of starting and maintaining a network. These tasks break down into three areas of responsibility:

Job Title	Utility	Responsibilities
Network adminstrator	XRA	Global responsibility for planning the entire network: • Understand the topology of the entire network, that is, how the hosts, devices, and links relate to each other. • Run XRA to generate routing tables for the network. • Provide consistent global parameters to the managers of individual systems.
System manager	NETGEN	Local responsibility for generating a single system: • Understand the devices and links connected to this host. • Decide what users should have access to the network. • Run NETGEN to configure the local system's software and hardware for the XODIAC network. Use the global parameters supplied by the network administrator, and make decisions about the strictly local parameters. • Use NETGEN to make whatever configuration changes become necessary.
System operator	NETOP	Local responsibility for keeping a local system running: • Understand the local devices, links, and network processes. • Bring the network up and down. • When necessary, use NETOP to bring individual XODIAC processes up and down. • Inform the system manager or network administrator of any local changes that could affect the whole network. • Perform troubleshooting operations when network problems arise.

The rest of the manual explains how to perform these tasks.

Getting Help

XODIAC has an on-line help facility. To get the list of topics, type

```
) NHELP ↵
```

For help on a particular topic, type NHELP, followed by the name of the topic. For example, for information on NETOP, enter the command:

```
) NHELP NETOP ↵
```

A brief, explanatory message will appear.

End of Chapter

Chapter 2
Loading the Network Software

This chapter explains how to load tapes containing X25 (AOS) or XTS (AOS/VS) and XODIAC Network Management software into your computer. It also tells you how to create links to the network files. (To load from another medium, such as diskettes, follow the directions in the proper Release Notice.)

The CLI manuals listed in the Preface of this manual have more information on the CLI commands and access control privileges that appear in this chapter.

Loading the Network Tapes

When you purchased the XODIAC Network Management System, you received two tapes: the X25 or XTS release tape and the XODIAC release tape, containing the XODIAC functional agents. You must load the X25 or XTS tape first.

To load the network tapes, take the following steps:

1. Give yourself Write access to directory :NET by issuing the following commands:

   ```
   ) SUPERUSER ON ⤸
   *) DIR : ⤸
   *) ACL  NET  OP,OWARE,  +,RE ⤸
   ```

   Initially, AOS and AOS/VS create the network directory (:NET) with no access control list (ACL). To load the network tape, you must have Write access to :NET. First, turn on the Superuser privilege, which you need in order to change the ACLs in :NET. Now, use the DIRECTORY command to move to the root directory. Use the ACL command to give OP Owner, Write, Append, Write, and Execute access to :NET, and Read and Execute access to everyone else.

2. Mount the X25 or XTS release tape on a system tape drive, and then move to the directory, :NET and load the tape by issuing the following commands:

   ```
   *) DIR  :NET ⤸

   *) LOAD/V/R  @magnetic-tape-unit-n ⤸
   ```

   Loading the X25 or XTS tape creates a subdirectory structure — :NET:NETGEN, :NET:UTIL, :NET:HELP, and :NET:LOGFILES. Table 2-1 lists each subdirectory and what it contains.

Table 2-1. The Subdirectories of :NET

Subdirectory	What It Contains
:NET:NETGEN	The X25 or XTS generation program, NETGEN, and sample network specification files.
:NET:UTIL	User-executable programs, CLI macros, and the network error message files, NETERMES.OB, and XTS_ERMES.OB. You must incorporate the error message files into the system ERMES file to get correct error messages.
:NET:HELP	The help files that the NHELP macro displays.
:NET:LOGFILES	The log files. NETOP puts log files for network processes into this directory if you enable logging for them.

3. Mount the XODIAC tape, and then issue the following CLI commands that move to the :NET directory and load the tape:

   ```
   *) DIR  :NET ⤸
   *) LOAD/V/R  @magnetic-tape-unit:n ⤸
   ```

   This command loads the files on the XODIAC tape, displaying their names on your terminal. The files on this tape include the network help files and the latest XODIAC Release Notice.

The release notice has a complete list of XODIAC files and other useful information about managing network software. The release notice filename has the format

XODIAC<rev_no>.RN

where <rev_no> is the current XODIAC revision number. For example, for XODIAC revision number 5.00, the release notice has the filename, XODIAC500.RN.

Creating Links to the Network

Once you've loaded the network tapes, you can create links in :UTIL to some of the network files. By using a link, you can avoid entering full pathnames every time you use network files or macros.

You will find it useful to create links in :UTIL to all of the files in :NET:UTIL. To create a link from :UTIL to a network file, use the following CLI format:

```
CREATE/LINK  pathname  resolution-pathname
```

For example, on an AOS system, if you want to access a macro in :NET:UTIL called CX25.CLI from your working directory without including the full pathname, you can create a link to it in :UTIL. Since :UTIL is on everyone's search list, the system automatically looks there, finds the link that tells it where the macro really is, and then goes to :NET:UTIL to find and execute it.

To create this link, first invoke the Superuser privilege to get Write access to :UTIL. Set the current directory to :UTIL and use the CREATE command, as follows:

```
) SUPERUSER ON ⤸
*) DIR :UTIL ⤸
*) CREATE/LINK  CX25.CLI  :NET:UTIL:CX25.CLI ⤸
```

The link allows you to access :NET:UTIL:CX25.CLI by simply typing the name of the CX25 macro.

End of Chapter

Chapter 3
System Security

You can make your network more secure by controlling access to files, directories, hosts, and other network resources. To control network privileges, you can use the following methods:

- use NETGEN sessions to control ACLs on remote HST files
- use the CLI to reset the ACLs for the directories :NET and :NET:UTIL
- use the PREDITOR program to control user network privileges
- control network access through the XODIAC Routing Analyzer

Setting ACLs on Network Files

You can set ACLs on network configuration files to specify what users can use the network resources. You can set these ACLs either during your NETGEN session or by using the CLI ACL command. Using NETGEN, however, gives the ACLs greater longevity: whenever you run NETGEN, ACLs on the network files revert to those assigned by the NETGEN specification file.

Chapter 4 explains NETGEN; the CLI manuals listed in the Preface explain ACLs.

Setting ACLs with NETGEN

When you configure local and remote hosts and network processes, NETGEN prompts you for access control lists (ACL) and puts the ACLs in the network specification file. For example, to add a remote host, you fill in the following screen:

```
XODIAC Network Configuration Process -- Add Remote Host Configuration


Remote Host Name (an AOS filename):

Remote Host Name is:

Host ID (None, 1-32762):          Hostfile ACL (an AOS ACL): + RE
```

The ACLs that you enter determine the local user privileges to the remote host file. The default grants all users Read and Execute access.

You can accept this default or be more restrictive. For example, to give yourself (OP) and Tam all available privileges and everyone else Read and Execute access, you can enter the following:

Hostfile ACL (an AOS ACL): OP OWARE, TAM OWARE, + RE ⤸

NETGEN records these answers in the network specification file. To change the network specification file, you use the NETGEN Change option.

Setting ACLs with the CLI

To change the ACLs on network files and directories, you can use the CLI ACL command. This command lets you specify access rights to each network file and, consequently, a user's access to the network. Since this command does not update the network specification file, whenever you run NETGEN these ACLs revert to those assigned in the specification file. When the network comes down, the ACLs to network files revert to the network spec file specifications.

Changing the ACLs on the Network Directory

Bringing down the network does not affect changes that you have made to limit a user's access to the :NET directory. Most network files reside in the :NET directory. A user must have access to :NET in order to use the network. For example, the following command prevents Tam from using the network.

```
) ACL  :NET  TAM,,OP,WARE,+,RE ⤸
```

The double commas indicate that TAM has no access to :NET. Tam cannot use network files and cannot, therefore, use the network itself. The operator gets Write, Append, Read and Execute access and all other users (+) get Read and Execute access.

Changing the ACLs on Network Program Files

To deny someone access to certain functions, but not to the whole network, use the ACL command to change the ACLs of individual XODIAC program files. You may want to set the ACLs on the following files to OP, OWARE:

RMA.PR	FTA.ST
RMA.ST	NETOP.PR
SVTA.PR	NETOP.ST
SVTA.ST	NETOP.OL (AOS only)
FTA.PR	

The initial ACL of the network files is OP OWARE, + RE.

Table 3-1 shows what happens when you set the ACLs on various network files.

Table 3-1. The Effect of ACLs on Network Files

Network File	What the ACL Controls
PVC files	Which users on that host use which permanent virtual connections to other hosts.
NPN files	Which users on that host can communicate with which remote processes.
HST files	Which users can communicate with which remote hosts.
RMA files	Which local processes can use RMA to access remote resources.

For example, to allow a user named Lee to use everything but NETOP, you enter the following command line:

```
) ACL  :NET:NETOP.PR  LEE,,OP OWARE, + RE ⤸
```

This command line prevents Lee from using NETOP, gives the operator all privileges, and gives everyone else Read and Execute privileges.

The following commands give only the operator access to the specified programs:

```
) ACL  :NET:RMA.(PR,ST)  OP,OWARE ⤸
) ACL  :NET:SVTA.(PR,ST)  OP,OWARE ⤸
) ACL  :NET:FTA.(PR,ST,OL)  OP,OWARE ⤸
) ACL  :NET:NETOP.(PR,ST,OL)  OP,OWARE ⤸
) ACL  :NET:UTIL:UVTA.(PR,ST)  OP,OWARE ⤸
) ACL  :NET:UTIL:UFTA.(PR,ST,OL)  OP,OWARE ⤸
```

Note that files with the extension .OL appear only under AOS.

Controlling Network Access Using PREDITOR

Another way of controlling access to the network is through PREDITOR. The PREDITOR utility creates and edits user profiles that determine user privileges. Three PREDITOR questions affect a user's network privileges:

USE VIRTUAL CONSOLE?

To allow a user to use VTA to log on to a virtual console, answer Y.

ACCESS LOCAL RESOURCES FROM REMOTE MACHINES?

Answer Y to allow a remote user to access files and devices, such as tapes and printers, on your system. For remote resource access, the user must have a profile with the same username and password on both systems.

MODEM?

To allow a user to log on to your system from a modem, answer Y.

The user profile contains certain other privileges that can affect network security. They are

Privilege	What It Does
Change Username	Allows the user to change his/her username, perhaps to a privileged name like OP.
Superprocess	Allows the user to issue process control commands against any process. With this privilege a user can block a process, change process priority, become resident, or terminate any process, including the master CLI. Terminating the master CLI brings down the system.
Superuser	Allows the user to bypass all file access controls. With this privilege, a user can get access to any file on the system.

Remember that someone with Superuser or Superprocess privileges plus the network privileges could combine the privileges to explore your system from a remote site.

Controlling Network Access with the XODIAC Routing Analyzer

If your network uses the AOS/VS XRA program, you can restrict access to certain hosts. XRA divides a network into service areas, or groups of hosts. Hosts in one service area can communicate with hosts in foreign (i.e., other) service areas.

If you are the network administrator for a service area, you give a list of your area's hosts to managers of other service areas. The other service areas use the list to reach your hosts. Foreign hosts can communicate only with the hosts on the list. If any of your hosts is absent from your list, foreign hosts will not know that it exists. In compiling the list for each foreign service area, you can therefore control that area's access to your hosts.

Details about XRA appear in Chapter 7.

Using RMA Under the Username OP

RMA requires that a user have the same username/password pair on the local and remote system. For username OP or any privileged username, this can be a security risk. A user on one system who knows the username/password pair of an operator can access all files on both systems. When using RMA from a large, central system to a small, local system, you can protect the files on the central system in two ways:

1. Keep different OP passwords on the local and on the remote system. When you want to use RMA, use the OP username but change the OP password to that used on the remote system. When you have finished using RMA, change the local password again to maintain security.

2. Create a special profile with the same username/password on both systems. The profiles on neither system should be privileged. When you create a back up directory, give Write, Append, Read, and Execute privileges to the operator of the local system. This allows the local operator to back up files from the local to the remote system.

End of Chapter

Chapter 4
The Network Generation (NETGEN) Program

The XODIAC Network Generation (NETGEN) program is an interactive, menu-driven utility. As a system manager, you use NETGEN to describe your own system and its connections to other systems in the network. NETGEN then packages this information as a set of configuration files that the XODIAC software can use to manage communications between your system and remote systems.

This chapter describes how to use NETGEN and covers these topics:

- an overview of NETGEN and the XODIAC network components it defines
- general directions for using NETGEN
- detailed directions for adding and changing network components

In addition, Chapters 5 and 6 also discuss NETGEN:

- Chapter 5 describes the steps in adding specific controllers and other communications devices to a XODIAC network. Chapter 4 describes devices in general; Chapter 5 describes specific devices.
- Chapter 6 gives a sample NETGEN session for configuring a network.

Chapter 4 is a prerequisite for Chapters 5 and 6.

The Specification File and Configuration Files

Using NETGEN is a two-step process:

1. Creating a *specification file.*

   As you define a network component, NETGEN displays a series of menus that prompt you for information about the component. NETGEN stores your responses in a specification file. The specification file is your definition of your system's position in a XODIAC network.

   When you change an existing network by adding or deleting a component, you must use NETGEN to edit the specification file.

2. Generating the *configuration files* from your specification file.

   Once you have created a specification file, you direct NETGEN to generate configuration files. NETGEN translates the specification file's information into a form that the XODIAC software can use, and it stores the information in the configuration files. The files are always in the :NET directory. There is one configuration file for each XODIAC component that your system can use.

   Whenever you make a change to the specification file, you must generate a new set of configuration files. If you don't, the XODIAC software will be using outdated information.

The kinds of configuration files correspond to the various components of a XODIAC network. The components are as follows:

- your *local host* (that is, your system)
- physical *devices* that are connected to your host and that can transmit and receive data
- software *links* that define how your host puts data onto a device
- *remote hosts* with which your local host can communicate over the links
- *network process names* that identify remote processes accessible from your local host

The following paragraphs discuss these XODIAC components.

Your system is your *local host.* In defining your local host, you assign the name by which other systems in the network can identify you.

Physical *devices* are pieces of hardware that let your host communicate with another host. There are many different kinds of devices, each with its own set of capabilities. When you define a device, you assign it a name and tell XODIAC what kind of device it is.

Links are devices as you define them to the XODIAC software. XODIAC must know certain facts about a device: for example, what communications protocol the host at the other end of the device is using; how many packets the host should send out without receiving an acknowledgement from the remote host; how large the data packets it sends out can be. You use NETGEN to set these parameters. The values you assign are known collectively as a link, which can be defined as a software abstraction of a physical device. Each link corresponds to a single device, but a single device may have more than one link defined on it.

When you define a link, you specify the maximum number of switched and permanent connections for the link. When two hosts communicate, they use a *virtual connection.* If they must establish the connection at the beginning of their communication session, the connection is a *switched virtual connection* or SVC. When the session begins, the SVC comes into existence. When the two hosts finish their session, they clear the connection, which disappears. It is also possible to define a *permanent virtual connection* (PVC) between two hosts. A

PVC always exists, whether or not it is in use. When you define a link, you can also create and name PVCs for the link.

Remote hosts are the other hosts in the network. Your local XODIAC software needs to know the name of each remote host and the link to use to reach the host. You use NETGEN to provide this information. You can also define parallel paths to a remote host: that is, if the primary link to a remote host is for some reason unusable, you can specify additional links that XODIAC can use for direct access to the host.

Network process names (NPN) are global names by which processes can be called from remote hosts. Communications between remote hosts essentially consist of communications between processes on the two hosts. For example, when you use the XODIAC Virtual Terminal Agent (VTA) to log on a remote host, you direct a local VTA process to establish a switched virtual connection with the complementary VTA process on the remote host. In addition to the standard XODIAC processes, a user can create a process (from a user-created program) that communicates with another user-created process on a remote host. Each process on your host that can be called from a remote host must have a *network process name* by which it is known to remote hosts. In addition, there must also be a network process name for each remote process that the processes on your host might want to call.

You use NETGEN to define all of these components. NETGEN initially stores the information in your specification file. It then generates the configuration files for use by the XODIAC software. There is a different kind of configuration file for each network component. Table 4-1 summarizes the types and contents of the different kinds of configuration files.

Table 4-1. XODIAC Configuration Files

File Type	Information
HST	Local or remote host Your :NET directory contains one HST file for your local host and one HST file for each remote host that your host can call. The name of the HST file is usually the host name followed by a dollar sign: for example, the host HOSTA usually has an HST file named HOSTA$.
RMA	Local or remote host The XODIAC Resource Management Agent (RMA) requires a special identifier for hosts. The RMA file contains this identifier. There is usually one RMA file for each HST file. The name of the RMA file is usually the same as the host name.
DCF	Physical device For each device connected to your host, NETGEN creates a device configuration file (DCF). The file has the name you assign to the device.
LCF	Link For each link that you define on a device, NETGEN creates a link configuration file (LCF). The file has the name you assign to the link.
PVC	Permanent virtual connection When you define a link, you also define the link's permanent virtual connections (if any). NETGEN creates a PVC file for each permanent virtual connection and gives it the name you assigned to the connection. Note that there are no configuration files for switched virtual connections (SVCs), because these come into existence only when two processes begin a communications session.
NPN	Network process name NETGEN automatically creates an NPN file for the standard XODIAC processes: for example, a file named VTA for the Virtual Terminal Agent, and one named FTA for the File Transfer Agent. You can define additional NPN files for user-created processes. You assign the filename by which remote hosts can identify the process.

Using NETGEN

This section describes various aspects of using NETGEN:

- navigating the NETGEN menu tree
- viewing the specification file
- responding to NETGEN's questions
- invoking NETGEN
- outlines of typical NETGEN sessions

The NETGEN Menu Tree

The NETGEN interface is a series of menus, which form an upside-down tree structure as shown in Figure 4-1. The higher menus ask you which NETGEN task you want to perform. Depending on your response, NETGEN displays the

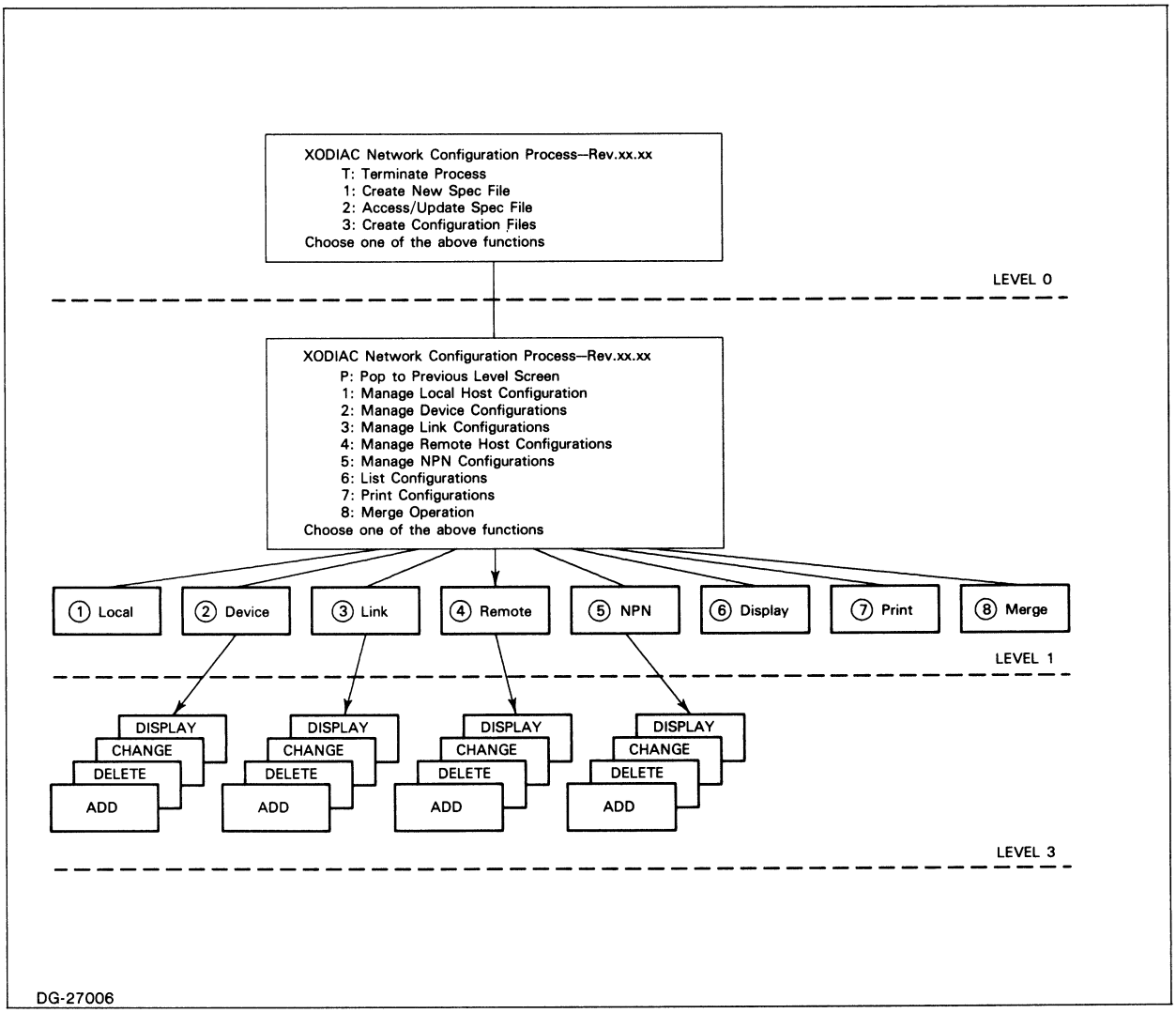


Figure 4-1. NETGEN Menu Levels

The highest NETGEN menu asks what general task you want to perform. The options are as follows:

Menu Item	What It Does
T : Terminate Process	Terminates the NETGEN process and returns you to the CLI.
1 : Create New Spec File	Creates a new specification file. NETGEN prompts you for the name of the file, which must not already exist. You choose this option when you want to create a new definition for your host's connection to the XODIAC network.
2 : Access/Update Spec File	Opens an existing specification file, which you can then view or edit. NETGEN prompts you for the name of the file. It then asks you for the name of the new specification file, and displays the existing file's name as a default. If you accept the default, NETGEN applies your editing changes to the current file. If you provide a different filename, NETGEN does not change the existing file, but instead creates a new specification file to include your editing changes. The current revision of NETGEN may not be compatible with the revision you used to create the specification file. If this occurs, you can convert the file to be compatible with the new revision. When you choose this option and specify the filename, NETGEN tells you that the revisions are incompatible. Simply specify a new filename as the new file. NETGEN performs the necessary conversion, and the new file is now compatible with the new NETGEN revision.

3 : Create Configuration Files	Generates the configuration files from your specification file. NETGEN prompts you for the name of the specification file it is to use. If configuration files already exist in :NET, NETGEN deletes them and creates new ones based on the specification file you indicate.

If you choose option 1 or 2, NETGEN displays its next level of menu, which asks what task you want to perform. The options are as follows:

Menu Item	**What It Does**
P : Pop to Previous Level Screen	Returns to the next higher level of NETGEN menus.
1 : Manage Local Host Configuration	Lets you add, change, delete, or display information about your local host.
2 : Manage Device Configurations	Lets you add, change, delete, or display information about a physical device.
3 : Manage Link Configurations	Lets you add, change, delete, or display information about a link.
4 : Manage Remote Host Configurations	Lets you add, change, delete, or display information about a remote host.
5 : Manage NPN Configurations	Lets you add, change, delete, or display information about a network process name.
6 : List Configurations	Lets you list all components of a particular type.
7 : Print Configurations	Lets you create a printable version of the specification file.
8 : Merge Operation	Lets you import definitions of the remote hosts by merging a file provided by the network manager with your local specification file.

When you select an option, NETGEN displays the next lower menu to obtain additional information about the task you want to perform.

Options 1 through 5 and option 8 are covered later in this chapter under "Steps for Using NETGEN." The next section discusses options 6 and 7.

Viewing the Specification File

The information in the specification file is machine-readable. You cannot view the file's contents directly with the CLI command TYPE. Instead, all access to the file must be through NETGEN, as described in this section.

You can view items in the specification file during a NETGEN session. The option to "List Configurations" lists all items of a certain kind. If you choose this option, NETGEN asks what kind of component you want, and then displays the list of names, plus some additional information.

In addition, each "Manage Configurations" option (for example, "Manage Link Configurations") gives you the option of displaying the current definition of a specific component of that kind. If you choose this option, NETGEN asks for the name of the component and then displays the information.

The option to "Print Configurations" creates a printable version of the entire specification file. If you choose this option, NETGEN prompts you for the pathname where you want the file created. You can specify a disk file. You can also specify @LPT, which causes NETGEN to send the printable file to the line-printer queue.

Responding to NETGEN's Questions

The higher NETGEN menus display a list of options and ask for your choice. You type the number or letter corresponding to your choice and then press NEW LINE.

The lower NETGEN menus request more complex information. You must enter a name, an address, or some other piece of information. Enter the value and press NEW LINE. Some values must conform to a particular format: for example, some station addresses must contain exactly 12 hexadecimal digits, and some other addresses must contain between 2 and 15 decimal digits. The NETGEN menus usually display the format requirement as part of the prompt. If the value you enter does not conform, NETGEN rejects the value, issues an error message, and does not move to the next field until you enter a valid value.

NETGEN often supplies a default value with its prompt. If you are adding a new item, the default values are those that seem most universally usable. If you are changing an existing definition, the default values are the current values, that is, those provided in the previous NETGEN session. If a question has a default value, NETGEN displays it in the space provided for your response. To accept the default, press NEW LINE. To supply your own value, type over the default value and then press NEW LINE.

To leave a menu before completing it, press ESC. This action returns you to the main NETGEN menu. It also aborts the tasks you were performing and clears any values that you have already entered for the menu. For example, if you are adding a link and, in the middle of the link definition menu, you press ESC, NETGEN does not configure the link based on the values you have already provided.

Invoking NETGEN

To invoke NETGEN, use this CLI format line:

XEQ NETGEN*[/RECREATE=specification-file-pathname]*

The /RECREATE switch is equivalent to the "Create Configuration Files" option on the first NETGEN menu. The switch lets you generate the configuration files in batch mode, rather than interactively. The switch value names the specification file to be used in generating the configuration files. This switch is especially useful if your specification file is large, because generating the configuration files for a large network can be time-consuming.

Typical NETGEN Sessions

This section gives an overview of the steps involved in using NETGEN. Detailed instructions appear later under "Adding and Changing Network Components" and in Chapter 5.

This section shows two typical NETGEN sessions for creating a new set of configuration files. The difference is in the way you define the remote hosts. The first way is to define each remote host separately using the option to "Manage Remote Host Configurations."

The second way assumes that your network uses the XODIAC Routing Analyzer (XRA), which is described in Chapter 7. XRA is a utility that helps a network manager design a large network. One manager has the centralized authority for running XRA for the entire network, or at least for a large subsection of the network. This manager provides a *local view specification file* to the system manager of each local host. The file contains directions for getting from the local host to every remote host in the network. When you receive this local view specification file from the central manager, you use the NETGEN option "Merge Operation" to merge the file with your specification file. This single step enters the definitions for all the remote hosts.

If your network does not use XRA, follow these steps:

1. Invoke NETGEN.
2. Select option 1, "Create New Spec File," from the first menu, and enter a name for the specification file.
3. Create a specification file by adding the XODIAC components in the order they appear on the next menu:

   - your local host
   - devices
   - links
   - remote hosts
   - network process names

   NETGEN requires you to configure a device before you configure any link defined on the device. It also requires you to configure a link before you configure any hosts that use the link.

4. Return to the highest menu and select option 3, "Create Configuration Files." If you already have a XODIAC network running, you must first bring it down (see Chapter 8) before creating new configuration files. Bringing the network down ensures that NETGEN replaces the old files with new ones. Note that you can create the configuration files in batch mode.

5. Bring the network up (see Chapter 8). The XODIAC software now uses the specifications you have just defined.

If your network uses XRA, follow these steps:

1. Invoke NETGEN.

2. Select option 1, "Create New Spec File," from the first menu, and enter a name for the specification file.

3. Create a *basic* specification file. A basic file contains all the configurations except the remote hosts. In other words, add these components in the order they appear on the next menu:

   - your local host
   - devices
   - links
   - network process names

   NETGEN requires you to configure a device before you configure any link defined on the device. It also requires you to configure a link before you configure any hosts that use the link.

4. Make sure that your central network manager has sent you the local view specification file for your host. Select the option "Merge Operation" and give the name of the local view specification file. NETGEN imports the file's contents into your specification file.

5. Return to the highest menu and select option 3, "Create Configuration Files." If you already have a XODIAC network running, you must first bring it down (see Chapter 8) before creating new configuration files. Bringing the network down ensures that NETGEN replaces the old files with new ones. Note that you can create the configuration files in batch mode.

6. Bring the network up (see Chapter 8). The XODIAC software now uses the specifications you have just defined.

Adding and Changing Network Components

This section discusses the questions NETGEN asks when you select one of the "Manage Configurations" options and add or change a network component. In response to NETGEN's values, you provide values that define the component. This section gives some guidelines for the values.

This section gives a thorough description of local hosts, remote hosts, and network process names. Its description of devices and links is more general, because the questions NETGEN asks vary greatly depending on the type of device you are adding. This section therefore discusses only those parameters that are common to several different device types. For details on each device type, see Chapter 5.

Configuring Your Local Host

You must define your own host to the network by giving the name and identifier by which other hosts can call your host. When you configure your host, NETGEN requests the following information:

Information	Reply Guidelines
Local host name	A host name can be any valid AOS or AOS/VS filename, with a maximum length of 10 characters. Remote hosts use this host name to call your host. The name must therefore be unique throughout the network, and all remote systems must know your host by this name.
ACL	The access control list (ACL) applies to the HST and RMA files for your local host. It determines what local users can have access to the host. You should be conservative in granting access. The default ACL is + RE, which grants all users the minimum privilege they need to use the files. Chapter 3 discusses ACLs.
Host ID	The host identifier is an integer in the range 1–127 on AOS and 1–32767 on AOS/VS. The number must be unique among all the host identifiers that you assign on your system. The host identifier is optional. However, RMA uses the host identifier and cannot function without it.

Configuring Devices

A device is a piece of hardware that physically connects your host to a remote host. XODIAC supports many different types of devices: synchronous controllers, local area network (LAN) controllers, and others. This section covers some of the parameters that are common to several types. The questions that NETGEN asks depend on the type of device you are adding. For details about specific types, see Chapter 5.

When you configure a device, NETGEN requests the following information:

Information	Guidelines
Device name	A device name is a valid AOS or AOS/VS filename not longer than 16 characters. The device name must be unique among all the devices configured in this specification file. The device name should begin with an alphabetic character to avoid confusion for NETOP commands that can take either a device name or a number as an argument. A convenient naming convention is to append _DCF to the name of the controller. For example, an ISC can be named ISC_DCF.
Device type	NETGEN displays a list of the valid device types. Note that AOS and AOS/VS support different device types. Enter the type of the device you are adding.
Device code	Most device types require a device code, which is one to three octal digits. Your local host's hardware and operating system use this code to identify the device, so the code must be unique among all the devices on your system. NETGEN displays as a default the number that Data General puts on the communications board for this type of device. The field engineer who installs the board may retain the default or may provide a different value.
Do you wish to specify the station address?	LAN controllers require a station address, which the the remote hosts use to specify your host's position on the LAN. The address must therefore be unique across the LAN. Each board that supports a LAN has a unique value on it. By default, NETGEN uses this value as the station address. To accept the default, answer N to NETGEN's question. If you use the default, you must retain this value as the address, even if you later replace the board, because the other hosts on the LAN know your host by this address.

If your LAN has its own addressing system, you can override the default by answering Y to NETGEN's question. A station address consists of 12 hexadecimal digits. NETGEN displays the first 6 digits, which are Data General's vendor code. You cannot change this part of the station address. You enter the final 6 hexadecimal digits. The station address must be unique across the LAN, and all other hosts must know you by this address. A central network administrator should therefore assign all station addresses.

Run X25 on this controller? (AOS/VS only)

XTS, the AOS/VS transport service, lets you run the X.25 portion of its program on an intelligent controller rather than on the CPU on the host. In this way, you can off-load the connection management work onto the controller. If the intelligent controller you are configuring supports this option, NETGEN asks whether you want to run X.25 on the controller.

Configuring Links

A link is a device as seen by the XODIAC software. When you configure a link, you set the parameters that XODIAC is to use when it puts data on or takes data from a device. You usually configure one link for each device (or for each line if the device supports multiple lines). It is possible to configure more than one link per device or line, perhaps giving different parameters to the links. At any one time, however, you can enable only one link per device or line.

The NETGEN menus for configuring links vary more widely than for any other XODIAC component. You associate a link with a specific device, and the type of the device determines what questions NETGEN asks about the link. This section covers only those questions that are common to several sets of the link menus. For details about adding links that are associated with specific device types, see Chapter 5.

Under AOS/VS, some links can support either the X.25 protocol or the Transmission Control Protocol/Internet Protocol (TCP/IP), or both. If the device associated with this link can support either protocol, NETGEN asks "Configure this link for X25 (Y/N)." Because you are configuring a XODIAC network, answer Y. (If you answer N, the prompts pertaining to X25 disappear.) After you answer the X25 questions, NETGEN asks "Configure this link for TCP/IP (Y/N)." If you want to configure the link for TCP/IP as well, answer Y and consult *Managing and Operating AOS/VS Internet* (093-000400) for the relevant NETGEN questions.

Some link values must be consistent with the values that other hosts set. For example, hosts that communicate with each other must use the same maximum packet size. They must also specify the same number of permanent virtual connections (PVCs) and the same maximum number of concurrent switched virtual connections (SVCs). The parameter descriptions in Chapter 5 state what values must be consistent.

The consistency requirement is as follows:

- Two hosts in a point-to-point connection over a synchronous link must specify the same value for certain link parameters.
- All the hosts on a local area network must specify the same value for certain link parameters.
- A host connected to a public data network (PDN) over a synchronous link must follow the PDN's conventions in specifying certain link parameters.

For these parameters, a central network administrator should set the values to ensure that they are consistent among all the hosts.

NETGEN asks the following questions about any link you configure, regardless of the associated device type:

Information	**Guidelines**
Link name	A link name is a valid AOS or AOS/VS filename not longer than 16 characters. The link name must be unique among all the links configured in this specification file. The link name should begin with an alphabetic character to avoid confusion for NETOP commands that can take either a link name or a number as an argument. A convenient naming convention is to append _LCF to the name of the associated controller. For example, an ISC link can be named ISC_LCF.
Device name	This is the name of the device that you want associated with this link. You must already have configured the device. When you enter the name of an existing device, NETGEN displays the device type and the questions relevant to that type.
Local host address	A host address consists of 2 to 15 decimal digits. Currently, these addresses are meaningful only on a PDN, where it is interpreted as a DTE (data terminating equipment) address. If you are on a PDN, use the number supplied by the PDN administrator.

Even if you are not on a PDN, NETGEN requires an address. Consult your network administrator for a valid value. The address may be used in the future.

Transmit retry count

This value sets the maximum number of times X.25 should retry a failed transmission. If an error occurs while X.25 is transmitting data, it automatically retries the transmission, until it succeeds or it exhausts the retry count you specify here. The value must be between 0 (do not retry) and 99.

If you receive frequent error messages stating that the retry count is exhausted, you can double the current value, and then lower it in small steps until you reach an acceptable performance level. If the value is too high, X.25 may waste time attempting retries when transmission is for some reason impossible.

Maximum packet size

This value is the maximum size, in bytes, for packets transmitted on this link. X.25 will not construct packets larger than the size you specify. NETGEN displays the valid values for each particular type of link. Enter one of the displayed values. If your major use for the link is to transfer files, a larger packet size is more efficient.

# of PVC's
# of SVC's

NETGEN asks for the number of permanent virtual connections (PVCs) you want to specify, and for the maximum number of concurrent switched virtual connections (SVCs) that you want to permit.

If you set either number to a value greater than zero (the default), some device types require a starting number for the virtual connections. A valid starting number is a decimal integer between 0 and 4095. If you request one or more PVCs, the default PVC starting number is 1; the PVCs are numbered sequentially from the starting number. If you request one or more SVCs, the default SVC starting number is the highest PVC number plus 1.

If you request one or more PVCs, NETGEN asks for additional information about each PVC:

PVC name

A PVC name is a valid AOS or AOS/VS filename of up to 16 characters. This name must be unique among all the PVCs on your local host (not only the PVCs on this link). NETGEN creates a PVC file with this name.

Host address	The host address is meaningful only on a PDN, where you supply the number that identifies the remote host to which this PVC is to be connected. Even if you are not on a PDN, NETGEN requires an address.
Station address	If you are on a LAN, NETGEN requests the station address (12 hexadecimal digits) of the remote host. Get this address from the network administrator.
PVC ACL	Enter the access control list (ACL) for the PVC file. The default ACL is + RE. This ACL controls what local users can use the PVC.

The following table describes information that only certain types of links require. The descriptions in Chapter 5 indicate whether a particular link requires this information.

Information	**Guidelines**
Network type	A synchronous link can connect you to a PDN or to another Data General host. If you are connected to a PDN, you enter the type of PDN from the choices that NETGEN displays (or enter OTHER). If you are connected to another DG host, you enter DATA GENERAL as the network type.
DTE or DCE	The X.25 protocol originally defined the interface connecting a user's equipment to a PDN. It distinguished between the data terminal equipment (DTE) and the data circuit equipment (DCE). The DTE is the user's equipment; the DCE is the point of connection to the PDN. Data General's implementation of X.25 relaxes the distinction, but the terminology persists to comply with the protocol. NETGEN therefore asks this question for synchronous links. If you specified a PDN for "Network type," NETGEN automatically assigns you the DTE role. In a point-to-point connection, you assign one host the DTE role and the other the DCE role. The assignment is arbitrary except in one case. If this is an asynchronous link between your ECLIPSE® MV/Family host and a remote DESKTOP GENERATION® host that is running AOS XODIAC PREGEN, your MV/Family host must specify DCE, because XODIAC PREGEN automatically chooses the DTE role.

Connect retry count

This value sets the maximum number of times X.25 should try to establish a virtual connection with a remote host. If X.25 fails to establish a connection, it automatically tries again, until it succeeds or it exhausts the retry count you specify here. The value must be between 0 (do not retry) and 99. Unless there are known problems on this link, it is usually best to keep the retry count low. Otherwise, X.25 may waste time attempting to establish a connection when a connection is for some reason impossible.

Packet window size
Frame window size

A packet is the unit of data transmission at the network level. A frame is the unit of data transmission at the link level. The packet window size is the maximum number of packets that you can send without receiving an acknowledgement from the destination host. The frame window size is the maximum number of frames that you can send without receiving an acknowledgement from the next host in the route to the destination host.

A low window size can slow performance by forcing X25 to wait for acknowledgements. If the link or receiving host is slow, you may improve performance by raising the window size.

Transmit time-out

This value sets the time-out period. When X.25 sends a frame over a link, it waits for an acknowledgement from the next host in the route. If it does not receive an acknowledgement within this time-out period, it retries the transmission.

NETGEN displays the valid values. A value of –1, if shown, means wait forever (infinite time-out). A value of 0, if shown, means do not wait. A value greater than 0 means wait the specified number of seconds.

When you start X25 or XTS, it automatically enables two *loopback links* named LOOPBACK0 and LOOPBACK1. These links let a single host put data onto a link and then receive it from the link. The loopback feature lets you test networking on a single host without requiring a physical link to a remote host. Under AOS, you cannot disable these links. Under both AOS and AOS/VS, you cannot change their host addresses, which are as follows:

Link	Local Host Address	Remote Host Address
LOOPBACK0	1234567890	9876543210
LOOPBACK1	9876543210	1234567890

Configuring Remote Hosts

A remote host is any other host in your network with which you want to communicate. Your host may be directly connected to the remote host by a

physical device, or the connection may be *routed.* A routed connection has several intermediate hosts between the local host and the destination remote host. Each intermediate host must be an AOS/VS system running Routing XTS or X25_LMGR.

The way you configure remote hosts depends on whether your central network administrator uses the XODIAC Routing Analyzer (XRA):

- If your network uses XRA, you do not use NETGEN to configure remote hosts. Instead, the network administrator provides a local view specification file that contains routing information for your host. Use the NETGEN option "Merge Operation," described in this chapter, to merge the file with your host's NETGEN specification file.
- If your network does not use XRA, you must use NETGEN to configure each remote host individually. Follow the directions in this section.

In configuring a remote host, you must tell XODIAC the path (that is, the link) it should use to reach the host. For a direct connection, this path is the link associated with the physical device that connected your host with the remote host. For a routed connection, this path is the link to the next host in the route to the destination host. In specifying the routed paths, you must carefully map out the entire network. You must take particular care to avoid cycles, that is, paths that go into infinite loops. Note that XRA produces routes that are guaranteed not to contain cycles.

NETGEN lets you specify parallel paths to a remote host. That is, after you describe a primary path, you can also describe up to four more parallel paths. If one path is for some reason unusable, the XODIAC software can select the second path; if that one is also out of order, it can take the third, and so on, up to the fifth path.

The paths are numbered from 1 to 5 in order of priority, with 1 being the highest priority. Using the "Change Remote Host Configuration" option, you can insert or delete a path. If you delete a path, the rest of the configured paths move up one step in priority. If you insert a path, the rest of the paths move down one step. Therefore, to change the priority of a path, you must first delete it and then reinsert it in its new position.

As you configure each path, NETGEN first asks if you want to configure it for any PMGR switched line. This option is for configuring a modem on an asynchronous line between an MV/Family host and a DESKTOP GENERATION host. Answer Y only for this configuration. In all other cases, answer N. Chapter 5 tells how to configure a DESKTOP GENERATION host.

On an AOS/VS host, a connection to a remote host may use either the X.25 protocol or the TCP/IP protocol, or both. When you configure a host, NETGEN asks "Use X25 transport (Y/N)." Because you are configuring a XODIAC network, answer Y. NETGEN then asks "Use TCP/IP transport (Y/N)." If you want to use TCP/IP in addition to X.25, answer Y and consult *Managing and Operating AOS/VS Internet* (093-000400).

When you configure a remote host, NETGEN requests the following information:

Information	Reply Guidelines
Remote host filename	This is a valid AOS or AOS/VS filename with a maximum length of 10 characters. NETGEN creates an HST file whose name is this filename with a dollar sign appended. (Do not enter the dollar sign as part of the filename.) A local user specifies this filename when calling the remote host. The file contains the name that X.25 uses to identify the remote host (you specify the host name in answer to the next NETGEN question). You usually use the same name for the file and the host. You can, however, configure the same remote host twice, using different filenames. Each filename would be associated with a different link. You can call the remote host through either filename. In this way, you can control which link the call uses.
Remote name	A host name is a valid AOS or AOS/VS filename with a maximum length of 10 characters. See the previous entry for the relationship between the remote host name and the remote host filename.
Host ID	The host identifier is an integer in the range 1–127 on AOS and 1–32767 on AOS/VS. The host identifier must be unique among all the host identifiers that you assign. The host identifier is optional. However, RMA uses the host identifier. If you omit it, local users cannot use RMA to reach the remote host.
Hostfile ACL	The access control list (ACL) applies to the remote host's HST and RMA files in your local :NET directory. It determines what local users can have access to the remote host. The default ACL is + RE, which grants all users the minimum privilege they need to use the files. Chapter 3 discusses ACLs.

After asking these questions, NETGEN asks about paths to the remote host. It displays a path number. To add that path, or to change or display it if it already exists, press NEW LINE. Otherwise, specify the number of the path you want. Once you select a path number, NETGEN asks for the following information for each path:

Information	Reply Guidelines
Do you wish to configure path(n) for any PMGR switched line.	This question applies only to an asynchronous line between an MV/Family host and a DESKTOP GENERATION host. See the discussion above.

Link name

This is the link to be used for this path to the remote host. The link must already have been configured. If you enter a valid link name, NETGEN displays the type of the associated device.

Host address

A network address consists of 2 to 15 decimal digits. The address is meaningful only on a PDN. If you are on a PDN, get the address of the remote host from the PDN administrator. Even if you are not on a PDN, NETGEN requires a host address.

Station address

If the link you specify is for a LAN, NETGEN requests the station address of the remote host. The address consists of 12 hexadecimal digits. Get the address from the central network administrator.

Configuring Network Process Names (NPNs)

A network process name (NPN) identifies a process on your host that remote users can use or a process on a remote host that local users can use. Configuring a network process name creates a file of type NPN in your :NET directory.

NETGEN automatically configures a number of NPNs for XODIAC and other Data General software. For example, it configures VTA, FTA, and RMA. For a list of the automatically configured NPNs, use the NETGEN option "List Configurations," followed by the "List NPNs" option.

A programmer can use the XODIAC X.25 interface to create a process that accepts requests from remote users. Before the process is usable, you must use NETGEN to define an NPN file in your local :NET directory. An NPN file must also exist in the remote host's :NET directory.

In configuring an NPN, you specify both an NPN filename and the contents of the file. If both hosts are Data General systems, the file contains the process name, which is usually the same as the filename.

However, if a Data General system is communicating with a host running a non-Data General implementation of X.25, the remote host may not understand the Data General format for the process name. In this case, you explicitly specify a *user data area* as the contents of the NPN file. A user data area consists of from 0 to 32 pairs of hexadecimal digits, formatted according to the CCITT standards that the remote host expects. Also, you can use the user data area to select X.25 options that are not part of the standard Data General interface.

Users refer to the process by the NPN filename. To establish a connection between the local and remote processes, X.25 puts the contents of the NPN file into call packets. The process identifiers in the packets from the local and remote processes must match exactly. If they do not, X.25 does not establish the connection.

When you configure an NPN, NETGEN requests the following information:

Information	Reply Guidelines
NPN-type entry name	Enter a valid AOS or AOS/VS filename for the process' NPN file. Users refer to the process (for example, to request the services of a remote serving process) by the NPN filename.
Do you wish to specify the User Data Area	If you want the NPN file to contain other X.25 options beyond the process name, answer Y. NETGEN then asks for the user data area in 0 to 32 pairs of hexadecimal digits. If you answer N, NETGEN asks for the process name, as shown in the next entry.
Network Process Name	Enter a 0 to 4 byte process name. The network process name is case-sensitive: that is, "VTA" and "vta" do not match. Note that X.25 requires an exact match between the process name specified by the local and remote processes before it establishes a connection. The process name is usually the same as the filename.
Access Control List	The access control list (ACL) determines what local users can use this process. The default ACL is + RE, which grants all users the minimum privilege they need to use the NPN file. Chapter 3 discusses ACLs.

Merging Remote Host Information from an XRA File

If your network uses the XODIAC Routing Analyzer (XRA), you do not explicitly configure the remote hosts. Instead, the central network administrator provides you with a *local view specification file* that describes the routing from your host. You use the NETGEN option "Merge Operation" to import this information into your host's specification file.

You merge the local view specification file into a *basic* specification file. A basic file contains the configurations for all network components *except* the remote hosts. To create a basic file, use NETGEN to configure your local host, the devices, the links, and the network process names.

You must begin with a basic specification file. If you use a specification file that already contains remote host configurations, the NETGEN merge operation successfully overwrites the existing information with any new information about the hosts. However, it does not delete any hosts configured in your old specification file but missing from the local view specification file. Your file could therefore contain configurations for hosts that the central network administrator has deleted from the network. In addition, the merge operation executes more quickly on a basic file.

When you choose the "Merge Operation" option, NETGEN asks for the following information:

Information	Reply Guidelines
Local View Specfile Name	Enter the pathname of the local view specification file. The filename is usually hostname.LVS, where hostname is the name of your host.
Do you wish to have Host ID's assigned for merged hosts?	If you answer Y, NETGEN begins at the highest permitted host identifier (127 for AOS, 32767 for AOS/VS) and goes down through the numbers until it finds the next unassigned number. It assigns this number to a host, and then finds the next unassigned number for the next host. If you answer N, NETGEN does not assign host identifiers. You can explicitly assign them by changing the individual remote host configurations. Host identifiers are optional. However, RMA uses host identifiers. If you do not assign host identifiers, local users cannot use RMA to reach remote hosts.
Do you wish to overwrite the remote host information, for already existing hosts, with that from the local view specfile?	If you answer Y, NETGEN automatically overwrites an existing host configuration with the new information contained in the local view specification file. If you answer N, NETGEN asks you to verify the information before it overwrites an existing configuration.

End of Chapter

Chapter 5
Configuring Specific Controllers and Other Communications Media

This chapter gives step-by-step directions for using NETGEN to configure specific controllers and other communications media. There is a separate section for each kind of controller. The section describes the device, link, and remote host screens that NETGEN displays for the controller, and provides guidelines for answering NETGEN's questions.

For more general comments on the NETGEN fields discussed in this chapter, see Chapter 4.

The description of a NETGEN field sometimes gives a range of valid values. Note that this range is the set of values that NETGEN accepts, not the practical maximum that the XODIAC software can support. The actual maximum depends on your specific configuration and may differ from the values given here and on the NETGEN screens. The most recent XTS or X25 release notice contains the actual maximum values.

XODIAC supports the controllers and communications media listed in Table 5-1. The table groups the controllers by category and, for each controller, shows its NETGEN code, full name, and model number (where applicable). The individual sections in this chapter give more information about each controller.

Some controllers can communicate directly with other controllers that are in the same category but are of different types:

- A synchronous controller can communicate directly with any other synchronous controller.
- A baseband LAN controller can communicate directly with any other baseband LAN controller.

The other controllers can communicate directly only with another controller of their own kind. For example, an MCA can communicate directly only with another MCA. If two controllers cannot communicate directly with each other, they can be connected through a routing host.

Table 5-1. Controllers and Other Communications Media

Code	Name	Model
	Synchronous Controllers (Point-to-Point or PDN Connection)	
ISC	Intelligent Synchronous Controller (ISC/2)	4380*
	Intelligent Synchronous Microcontroller (ISMC/2)	4530
	Multicommunications Processor (MCP-1)	4543
LSC	L-Bus Synchronous Controller	4561
DCU	Data Control Unit (DCU/200)†	4254
	* On an MV/4000 DC, the model number for an ISC/2 is 4395.	
	† The DCU is not recommended for new installations, except where a single CPU must support a large number of lines.	
	Baseband LAN Controllers (Ethernet/IEEE 802.3 Protocols)	
ILC	Intelligent LAN Controller	4532
LLC	L-Bus LAN Controller	4562
ICB	Integrated Control Board	N/A
DILC	DS/7700 Integrated LAN Controller	N/A
ILAN	Interlan NI4010A*	N/A
M802	802.3 Microcontroller	4529
	* The Interlan NI4010A is not recommended for new installations; the ILC represents newer technology.	
	Broadband LAN Controller (Ethernet/IEEE 802.3 Protocol)	
IBC	Intelligent Broadband Controller	4555
	Data General Proprietary LAN Controllers*	
MCA	Multiprocessor Communications Adapter	4206
	Radial Multiprocessor Communications Subsystem	5899
NBS	Network Bus System	4460
	* These controllers are not recommended for new installations; the industry standard LANs in the previous two categories are preferred.	
	Miscellaneous Communications Media	
PMGR_ASYNC	Asynchronous line*	N/A
SNA	SNA Backbone	31283
	* The PMGR_ASYNC line is intended to connect an MV/Family host to a DESKTOP GENERATION host.	

802.3 Microcontroller (M802) (AOS only)

An 802.3 Microcontroller (M802) is a communications controller board for DESKTOP GENERATION, S/20, C/30, and CS/100B systems. It supports the IEEE 802.3 and Ethernet® protocols for local area networks.

Configuring the M802 Device

From the main NETGEN menu, select option 2, "Manage Device Configurations." Then select option 1, "Add Device Configuration." NETGEN requests the following information:

Device Information	Reply Guidelines
Device Name	Assign a device name (1 to 16 AOS filename characters).
Device Type	Enter M802.
Do you wish to specify the M802 Station Address?	To accept the default address, enter N. To override the default, enter Y; NETGEN asks the following question: *M802 Station Address in 12 Hexadecimal Digits* — NETGEN displays the Data General vendor code as the first 6 digits. You enter 6 more hexadecimal digits. A remote host uses the station address to identify your local host's position on the LAN. It must be unique across the LAN. Each M802 board has a unique value that NETGEN uses as the default station address. If you use the default, you must retain this initial address even if you later replace the board, because remote hosts know your host by this address. If your LAN has its own addressing system, you can override the default and enter the address provided by the central network administrator.
Device code	Enter an octal value between 1 and 77. The code must be unique among all the devices on your system. The default M802 code is 45. Your field engineer may provide a different value.

Configuring an M802 Link

After you have configured the M802 device, configure a link on the device. From the main NETGEN menu, select option 3, "Manage Link Configurations." Then select option 1, "Add Link Configuration." NETGEN requests the following information:

Link Information	Reply Guidelines
Link Name	Assign a link name (1 to 16 AOS filename characters).
Device Name	Enter the name of the previously configured M802 device. NETGEN responds by displaying the device type, M802.
Local Host Address	Enter the address of your host (2 to 14 decimal digits). The central network administrator should provide all host addresses.
Transmit retry count	Enter a value between 0 and 99. The default is 4. The value sets the number of times X.25 should automatically reattempt a failed data transmission. The value 0 means do not retry. Once the link is in use, if you receive frequent error messages that the retry count is exhausted, try doubling the current value and then lowering it until you reach an acceptable performance level. A value that is too high can cause X.25 to keep reattempting an impossible transmission.
Max Packet Size	Enter 512 (the default) or 1024. This value sets the maximum size, in bytes, for data packets transmitted on this link. If the major use for the link is file transfer, a larger packet size is more efficient. All hosts on the LAN must specify the same maximum. A central network administrator should set this value.
# PVC's	Enter a value, between 0 (the default) and 64, for the number of permanent virtual connections (PVCs) you want. All hosts on the LAN must specify the same number of PVCs. A central network administrator should set this value. If you specify one or more PVCs, NETGEN also requests the following information:

	PVC name	Assign a PVC name (1 to 16 AOS filename characters).
	Host Address	Enter the address of the remote host to which this PVC is to be connected.
	M802 Station Address	Enter the station address of the remote host.
	PVC ACL	Enter the ACL for the PVC file. The default is + RE. The ACL controls what local users can use the PVC.
# SVC's		Enter a value, between 0 (the default) and 126, for the maximum number of concurrent switched virtual connections (SVCs) you want to permit. All hosts on the LAN must specify the same number of SVCs. A central network administrator should set this value.

Configuring an M802 Path to a Remote Host

After you have configured an M802 link, you can use it as a path to a remote host. Add the remote host, as described under "Configuring Remote Hosts" in Chapter 4. When you reach the question about paths, NETGEN requests the following information:

Path Information	Reply Guidelines
Path n	NETGEN displays a path number. Enter the number corresponding to the priority you want to give to the M802 path.
Do you wish to configure path(n) for any PMGR switched line?	Enter N (the default).
Link name	Enter the name of the M802 link that you have already configured. NETGEN responds by displaying the link type, M802.
M802 Station Address in 12 Hexadecimal Digits	Enter the station address of the remote host.
Host Address	Enter the address of the remote host.

Asynchronous Line to a DESKTOP GENERATION Host (PMGR_ASYNC)

NETGEN provides the device type PMGR_ASYNC to let you configure an asynchronous connection between an ECLIPSE MV/Family host and a DESKTOP GENERATION host. A DESKTOP host can run AOS XODIAC PREGEN, a user-friendly subset of the XODIAC and X.25 products. This section describes how to use XODIAC PREGEN and AOS/VS NETGEN to configure an asynchronous line.

Overview

On the MV/Family host, you use NETGEN to configure the asynchronous line. You define a device of type PMGR_ASYNC. PMGR_ASYNC is a virtual device, not an actual piece of hardware like the controllers that NETGEN configures. The PMGR_ASYNC virtual device permits use of the PMGR process, which manages the system's console lines. When you configure a PMGR_ASYNC device, you reserve a certain number of PMGR's console lines for use as asynchronous communications lines. PMGR continues to manage these as if they were console lines.

After configuring a PMGR_ASYNC device — that is, after reserving a number of PMGR lines — you configure each line as an asynchronous link. You identify each line by its PMGR console number. The PMGR_ASYNC link is like the other links that NETGEN configures.

On the DESKTOP host, you use the CONFIGURE.CLI macro to configure both AOS and XODIAC PREGEN. The macro does not distinguish between devices and links. It simply asks if you want to reserve a line for communications. If you answer Y, it asks for further information about the line.

You can configure an asynchronous line as a dedicated line or a switched line. A switched line is a dial-up modem connection. When the remote DESKTOP host requests a connection, it can use any available asynchronous line on the MV/Family host. The line assignment is dynamic and cannot be made during the NETGEN session.

On the DESKTOP host, the CONFIGURE.CLI macro asks you if the line is connected by a modem. If you answer Y, it asks for the modem rate; if N, it asks for the line rate.

On the MV/Family host, you first configure the switched lines as PMGR_ASYNC links. You then configure the remote host that will be connected to you by a switched line. After you give the host name and identifier, NETGEN asks you to configure the first or primary path to the remote host. It asks, *Do you wish to configure path(1) for any PMGR switched line?* Answer Y. NETGEN does not ask any further questions for this path. (You should not configure any parallel paths to this remote host.) NETGEN stores #ANY as the name of Path(1). This means that when the remote host requests a connection, PMGR will assign any available asynchronous line.

AOS XODIAC PREGEN automatically selects certain values for the link configuration. Because these values must be consistent on both hosts, the

NETGEN configuration on the MV/Family host must specify the following values:

- If the line is dedicated, the maximum packet size must be 512.
- If the line is switched, the maximum packet size must be 128.
- The number of SVCs must be 10.
- The number of PVCs must be 0.
- The DESKTOP host must take the DTE role. The MV/Family host must take the DCE role.
- On the DESKTOP host, CONFIGURE.CLI asks for your system's local ID. On the MV/Family host, the NETGEN Add Remote Host Configuration screen asks for the remote host's ID. If the asynchronous line is switched, these two numbers must match exactly.
- On the MV/Family host, you use VSGEN to define the console line. You should accept default values for parameters such as parity and number of stop bits.

A DESKTOP system can run standard AOS XODIAC, as well as XODIAC PREGEN. If it runs standard XODIAC, you use NETGEN to configure the communications line. Depending on the available controller, you can connect the system to a LAN, a PDN, or another Data General system. You can also define a PMGR_ASYNC device and link for an asynchronous connection. In such a connection, you are not restricted to the values just listed. Both hosts, however, must specify the same value for the parameters, and one must be assigned the DTE role and the other the DCE role.

If you have defined the asynchronous line in VSGEN and have enabled it through EXEC, you must disable the console number associated with the line before you enable the PMGR_ASYNC link.

The following sections describe the steps for connecting a DESKTOP system to an MV/Family system over an asynchronous line. It first describes the AOS PREGEN session (that is, the CONFIGURE.CLI macro dialogue) on the DESKTOP host, and then the complementary NETGEN session on the MV/Family host.

Configuring a DESKTOP GENERATION Computer with XODIAC PREGEN

To use XODIAC PREGEN to configure a DESKTOP host, follow these steps:

1. Install the system software and start up your system, as described in *Using AOS on DESKTOP GENERATION Systems.*
2. Install your XODIAC software, as described in *Using AOS on DESKTOP GENERATION Systems.*

3. Before you bring up EXEC, execute the CONFIGURE.CLI macro. Reply to the CONFIGURE.CLI macro prompts as suggested in the following paragraphs.

4. Execute the UP.CLI macro to bring up your network. The network is now configured.

When you execute the CONFIGURE macro, it prompts for configuration information. Some of the information concerns AOS and is described in the chapter "Installing AOS for the First Time" in *Using AOS on DESKTOP GENERATION Systems*. The following questions are specific to XODIAC:

DO YOU WANT TO RECONFIGURE?

Answer Y. You are adding new software to the system and must add new parameters to the configuration.

CONFIGURE now asks for more information about the model type of the system. These prompts are discussed in *Using AOS on DESKTOP GENERATION Systems*. It then asks the following questions.

Do you want to reserve line 0 for communications?

Enter Y, to configure the line for the asynchronous multiplexor that you need for communications.

Is line n connected via a modem?

If you are going to use a modem, answer Y. The line must be prepared for modem support, and a field engineer must configure your controller for this use.

If you answer Y, CONFIGURE asks about the modem rate:

What is the baud rate of the modem? {300 1200 2400 4800 9600}

Enter the exact baud rate allowed by your modem. Check the user's guide for your modem.

If you answer N, CONFIGURE assumes the line is dedicated and asks about the line rate:

What is the baud rate of the line? {300 1200 2400 4800 9600}

When you first configure the line, accept the default, 4800.

CONFIGURE now asks for information about issues unrelated to XODIAC.

If you indicate that you want some user's terminals on the system, CONFIGURE asks if you want a modem for each terminal. Depending on your answer, it asks the baud rate of the modem or line.

CONFIGURE now asks the following questions:

Would you like to reconfigure XODIAC?

Enter Y.

Please specify your system's local hostname

Enter the name of the local host, which can be up to 10 characters long.

Please specify your system's local ID

Enter a number between 10 and 127. The number must be unique among all the hosts with which the MV/Family host communicates. The MV/Family host will use this number to generate a unique address for the DESKTOP GENERATION host. A central network administrator should assign all host IDs.

Please specify the remote system's hostname

Enter the name of the remote MV/Family host.

After you enter the name of the remote host, CONFIGURE displays the message *SYSTEM DEFINITION IS COMPLETE.*

Configuring the Asynchronous Line on the MV/Family Host

The following sections describe how to use AOS/VS NETGEN to configure an asynchronous line from an MV/Family host to a DESKTOP GENERATION host that has used XODIAC PREGEN. The values shown match the values that XODIAC PREGEN automatically selects. If the remote DESKTOP GENERATION host uses standard AOS NETGEN, not XODIAC PREGEN, the restrictions do not apply.

Configuring the PMGR_ASYNC Device

From the main NETGEN menu, select option 2, "Manage Device Configurations." Then select option 1, "Add Device Configuration." NETGEN requests the following information:

Device Information	Reply Guidelines
Device Name	Assign a device name (1 to 16 AOS filename characters).
Device Type	Enter PMGR_ASYNC.
Maximum Number of Lines	Enter a value, between 1 (the default) and 50, for the number of console lines that you want to reserve for asynchronous communications. You must configure each of these lines as a separate link.

Configuring a PMGR_ASYNC Link

After you have configured the PMGR_ASYNC device, configure a link on the device. From the main NETGEN menu, select option 3, "Manage Link Configurations." Then select option 1, "Add Link Configuration." NETGEN requests the following information:

Link Information	Reply Guidelines
Link Name	Assign a link name (1 to 16 AOS filename characters).
Device Name	Enter the name of the previously configured PMGR_ASYNC device. NETGEN responds by displaying the device type, PMGR_ASYNC.
PMGR Console Number	Enter a value between 2 and 258. This is the number that PMGR has assigned to the console line (@CONn) on which you want to configure the PMGR_ASYNC link.
Local Host Address	Enter the address of your host (2 to 15 decimal digits). A central network administrator should provide all host addresses.
Transmit timeout	Enter a value between 2 and 180. The default is 5. This value sets the number of seconds X.25 waits for the next host in a route to acknowledge a data transmission. If the time-out period expires, X.25 retries the transmission.
Max Packet Size	If the asynchronous line is dedicated, enter 512 (the default). If the line is switched, enter 128. XODIAC PREGEN uses these values, which must be the same on both hosts.
DTE or DCE	Enter DCE (the default). The X.25 protocol defines the DTE as the data terminal equipment (the user's equipment) and the DCE as the data circuit-terminating equipment (the connection to the PDN). Data General's X.25 implementation can also connect two hosts in a point-to-point connection. The DESKTOP GENERATION host must be the DTE, and the MV/Family host must be the DCE.
# PVC's	Enter 0 (the default). XODIAC PREGEN does not support permanent virtual connections.
# SVC's	Enter 10. This is the number of concurrent switched virtual connections (SVCs) you want to permit. XODIAC PREGEN uses 10, and the value must be the same on both hosts.

Configuring a PMGR_ASYNC Path to a Remote Host

After you have configured a PMGR_ASYNC link, you can use it as a path to the remote DESKTOP GENERATION host. You can configure a dedicated or switched path. NETGEN requests the following information:

Path Information	Reply Guidelines
Remote Host Filename	Enter an AOS filename, with a maximum length of 10 characters. NETGEN creates an HST file whose name is this filename with a dollar sign appended. A local user specifies this filename to call the remote host. The file contains the name that X.25 uses to identify the remote host.
Use X25 transport?	Enter Y (the default).
Use TCP/IP transport?	Enter N (the default).
Remote Name	Enter an AOS filename, with a maximum length of 10 characters. This is the name that X.25 uses to identify the remote host. This name must match the name that the DESKTOP host specifies as its local host name in the CONFIGURE.CLI dialog.
Host ID	Enter the host ID. This number must match the number that the DESKTOP host specifies as its local ID in the CONFIGURE.CLI dialog.
Hostfile ACL	Enter the ACL for the HST and RMA files. The default is + RE. The ACL controls what local users can have access to the remote host.
Path 1	NETGEN displays path number 1. Press NEW LINE to indicate that you want to configure the primary path.
Do you wish to configure path(n) for any PMGR switched line?	If you want to access this host over a dial-up asynchronous line, answer Y. NETGEN does not ask any further questions about this path. If you want the path to be a dedicated asynchronous line, answer N (the default). NETGEN asks the following questions: *Link name* — Enter the name of the PMGR_ASYNC link that you have already configured. NETGEN responds by displaying the link type,PMGR_ASYNC. *Host Address* — Enter the address of the remote host.

Data Control Unit DCU/200

The Data Control Unit DCU/200 controls communications line multiplexors in parallel with the main processor. A DCU/200 can form a complete communications subsystem when configured with the following multiplexors and interfaces:

Item	Code	Model Number
Synchronous line multiplexors	SLM-1	4264
	SLM-2	4263
Bit-synchronous line multiplexors	BLM-1	4248
	BLM-4	4249
Bit-synchronous interfaces	BSI-1	4348
	BSI-4	4349
Character synchronous interfaces	CSI-1	4346
	CSI-2	4345

Under AOS/VS, you can use NETGEN to set certain parameters that, under AOS, are set during the AOSGEN session. These parameters relate to the data channel mapping for the DCU lines.

Configuring the DCU Device

From the main NETGEN menu, select option 2, "Manage Device Configurations." Then select option 1, "Add Device Configuration." NETGEN requests the following information:

Device Information	Reply Guidelines
Device Name	Assign a device name (1 to 16 AOS filename characters).
Device Type	Enter DCU.
Device code (AOS/VS only)	Enter an octal value between 1 and 77. The code must be unique among all the devices on your system. The default DCU code is 40. Your field engineer may provide a different value.
DCU Program Name (AOS/VS only)	Enter the pathname to the AOS/VS program file for the DCU protocol. The default is LAPB.PR (Balanced Link Access Protocol). Accept the default unless you know that you use another DCU protocol, such as LAP.PR (Link Access Protocol).

Under AOS/VS, you must explicitly configure each DCU line. NETGEN displays each line number from 0 to 7 and asks if you want to configure this line. The default is N. If you type Y, NETGEN asks for the following information for the line:

Line Information (AOS/VS only)	Reply Guidelines
Data Channel Map	Enter A, B, C, or D. The DCU uses this channel to access the host's memory. Disk and tape drives use A and B, and the host CPU often uses D. The DCU default channel is C.
# of Map Slots	Enter a value between 3 and 24. This value determines the host's buffer size for storing data from the link associated with this line. The default is 5. If you use a large packet size, you may want to assign more map slots. The total number of map slots on one DCU cannot exceed 27.

Configuring a DCU Link

After you have configured the DCU device, configure a link on the device. You configure a separate link for each DCU line that you want to use.

From the main NETGEN menu, select option 3, "Manage Link Configurations." Then select option 1, "Add Link Configuration." NETGEN requests the following information:

Link Information	Reply Guidelines
Link Name	Assign a link name (1 to 16 AOS filename characters).
Device Name	Enter the name of the previously configured DCU device. NETGEN responds by displaying the device type, DCU.
Network Type	If you are on a PDN, enter the type of PDN from the list that NETGEN displays; if your type is not on the list, enter OTHER. If you are not on a PDN, enter DATA GENERAL (the default).
Line #	Under AOS, enter a number between 0 and 31. Under AOS/VS, enter the number of a line you configured on the DCU device screen (that is, you answered Y when NETGEN asked *Config* for this line). The lines are numbered from 0 to 7. You must have configured the line before you use its number here.
Protocol Type	Enter LAP (Link Access Protocol) or LAPB (Balanced Link Access Protocol). The default is LAPB. The protocol type should be the same as the value you specified for DCU program name on the DCU device screen.

DTE or DCE

Enter DTE or DCE. The default is DTE. NETGEN asks this question only if you answered DATA GENERAL or OTHER for Network Type. If you specified a PDN, NETGEN automatically chooses DTE.

The X.25 protocol defines the DTE as the data terminal equipment (the user's equipment) and the DCE as the data circuit-terminating equipment (the connection to the PDN). Data General's X.25 implementation can also connect two hosts in a point-to-point connection. If you did not specify a PDN, you arbitrarily assign one host the DCE role and the other the DTE role.

Local Host Address

Enter the address of your host (2 to 14 decimal digits). The PDN administrator or central network administrator should provide all host addresses.

Sequence Numbering Modulus

Enter 8 (the default) or 128. The value determines the numbering system for the packets transmitted on the link. If you need to permit a large number of outstanding frames, use 128 rather than 8.

Connect retry count (AOS/VS only)

Enter a value between 0 and 99. The default is 10. The value sets the number of times X.25 should automatically reattempt to establish a connection with a remote host. The value 0 means do not retry.

Unless there are known problems on the link, it is usually best to set a low retry count, to keep X.25 from repeatedly trying to establish an impossible connection.

Transmit retry count

Enter a value between 0 and 99. The default is 10. The value sets the number of times X.25 should automatically reattempt a failed data transmission. The value 0 means do not retry.

Once the link is in use, if you receive frequent error messages that the retry count is exhausted, try doubling the current value and then lowering it until you reach an acceptable performance level. A value that is too high can cause X.25 to keep reattempting an impossible transmission.

Transmit timeout

Enter –1 or a value between 0 and 3600. The default is 3. This value sets the number of seconds X.25 waits for the next host in a route to acknowledge a data transmission. If the time-out period expires, X.25 retries the transmission.

The value –1 means wait forever (infinite time-out). The value 0 means do not wait. Neither of these values is recommended.

Use the following formula to compute the time-out period for your system:

First compute t, the time required to transmit a single frame. Use p (the value you specify as Max Packet Size on this screen) and r (the rate of transmission in bits per second).

$$t = \frac{(p \times 8)}{r}$$

On a full-duplex line, the time-out period should be the ceiling of

$$2t + 1$$

On a half-duplex line, you must also use w (the value you specify as Frame Window Size on this screen). The time-out period should be the ceiling of

$$[(w + 1) \times t] + 1$$

Enable timeout

Enter –1 or a value between 0 and 3600. The default is 30. This value sets the number of seconds X.25 waits before giving up an attempt to connect with a local modem. A value of –1 means wait forever (infinite time-out). A value of 0 means do not wait. It is usually best to keep this value between 5 and 40.

Frame Window Size

Enter a value between 1 and 7. The default is 7. A frame is the link level unit of data transmission. This value sets the maximum number of frames that X.25 can send without receiving an acknowledgement from the next host in the route.

On a PDN, you enter the window size set by the administrator. In a point-to-point connection, both hosts must specify the same window size.

A small window size can slow performance by forcing X.25 to wait for acknowledgements. If the link or remote host is slow, you can improve performance by raising the window size.

Packet Window Size

Enter a value between 1 and 7. The default is 2. A packet is the network level unit of data transmission. This value sets the maximum number of packets that X.25 can send without receiving an acknowledgement from the destination host. See the comment on *Frame Window Size.*

On a PDN, you enter the window size set by the administrator. In a point-to-point connection, both hosts must specify the same window size.

Max Packet Size

Enter one of these values: 32, 64, 128 (the default), 256, 512, 1024. This value sets the maximum size, in bytes, for data packets transmitted on this link. If the major use for the link is file transfer, a larger packet size is more efficient.

Max Packet Size (cont.)

On a PDN, you enter the maximum set by the administrator. In a point-to-point connection, both hosts must specify the same maximum.

 # PVC's

Enter a value in the following range:

0–64 (AOS)
0–250 (AOS/VS)

The default is 0. This is the number of permanent virtual connections (PVCs) you want.

On a PDN, you enter the number set by the administrator. In a point-to-point connection, both hosts must specify the same number of PVCs.

If you specify one or more PVCs, NETGEN asks the following question:

Start PVC # :

NETGEN begins numbering PVCs at this number, which must be between 1 (the default) and 4095. On a PDN, enter the number reserved for your host's PVCs. In a point-to-point connection, both hosts must specify the same starting number.

If you specify one or more PVCs, NETGEN also requests the following information:

PVC name	Assign a PVC name (1 to 16 AOS filename characters).
Host Address	Enter the address of the remote host on this PVC.
PVC ACL	Enter the ACL for the PVC file. The default is + RE. The ACL controls what local users can use the PVC.

 # SVC's

Enter a value in the following range:

0–126 (AOS)
0–250 (AOS/VS)

The default is 0. This is the maximum number of concurrent switched virtual connections (SVCs) you want to permit.

On a PDN, enter the number set by the administrator. In a point-to-point connection, both hosts must specify the same number of SVCs.

If you specify one or more SVCs, NETGEN asks the following question:

Start SVC # :

NETGEN begins numbering SVCs at this number, which must be between the highest PVC number plus 1 (the default) and 4095. On a PDN, enter the number reserved for your host's SVCs. In a point-to-point connection, both hosts must specify the same starting number.

Configuring a DCU Path to a Remote Host

After you have configured a DCU link, you can use it as a path to a remote host. Add the remote host, as described under "Configuring Remote Hosts" in Chapter 4. When you reach the question about paths, NETGEN requests the following information:

Path Information	Reply Guidelines
Path n	NETGEN displays a path number. Enter the number corresponding to the priority you want to give to the DCU path.
Do you wish to configure path(n) for any PMGR switched line?	Enter N (the default).
Link name	Enter the name of the DCU link that you have already configured. NETGEN responds by displaying the link type, DCU, and the network type.
Host Address	Enter the address of the remote host.

DS/7700 Integrated LAN Controller (DILC) (AOS/VS only)

The DS/7700 Integrated Local Area Network Controller (DILC) is part of a multiple-device controller that supports the IEEE 802.3 and Ethernet protocols for local area networks. The DILC is an integral component of the DS/7700 series of workstations and cannot be ordered separately. The DILC makes use of the DS/7700's high-speed, memory-mapped I-Bus.

Configuring the DILC Device

From the main NETGEN menu, select option 2, "Manage Device Configurations." Then select option 1, "Add Device Configuration." NETGEN requests the following information:

Device Information	Reply Guidelines
Device Name	Assign a device name (1 to 16 AOS filename characters).
Device Type	Enter DILC.
Do you wish to specify the DILC Station Address?	To accept the default address, enter N. To override the default, enter Y; NETGEN asks the following question: *DILC Station Address in 12 Hexadecimal Digits* — NETGEN displays the Data General vendor code as the first 6 digits. You enter 6 more hexadecimal digits. A remote host uses the station address to identify your local host's position on this LAN. It must be unique across the LAN. Each DILC board has a unique value that NETGEN uses as the default station address. If you use the default, you must retain this initial address even if you later replace the board, because remote hosts know your host by this address. If your network has its own addressing system, you can override the default and enter the address provided by the central network administrator.
Device code	Enter an octal value between 1 and 677. The code must be unique among all the devices on your system. The default DILC code is 56. Your field engineer may provide a different value.

Configuring a DILC Link

After you have configured the DILC device, configure a link on the device. From the main NETGEN menu, select option 3, "Manage Link Configurations." Then select option 1, "Add Link Configuration." NETGEN requests the following information:

Link Information	Reply Guidelines
Link Name	Assign a link name (1 to 16 AOS filename characters).
Device Name	Enter the name of the previously configured DILC device. NETGEN responds by displaying the device type, DILC.
Local Host Address	Enter the address of your host (2 to 15 decimal digits). The central network administrator should provide all host addresses.
Transmit retry count	Enter a value between 0 and 99. The default is 4. The value sets the number of times X.25 should automatically reattempt a failed data transmission. The value 0 means do not retry. Once the link is in use, if you receive frequent error messages that the retry count is exhausted, try doubling the current value and then lowering it until you reach an acceptable performance level. A value that is too high can cause X.25 to keep reattempting an impossible transmission.
Max Packet Size	Enter 512 (the default) or 1024. This value sets the maximum size, in bytes, for data packets transmitted on this link. If the major use for the link is file transfer, a larger packet size is more efficient. All hosts on the LAN must specify the same maximum. A central network administrator should set this value.
# PVC's	Enter a value, between 0 (the default) and 250, for the number of permanent virtual connections (PVCs) you want. All hosts on the LAN must specify the same number of PVCs. A central network administrator should set this value. If you specify one or more PVCs, NETGEN also requests the following information:

PVC name	Assign a PVC name (1 to 16 AOS filename characters).
Host Address	Enter the address of the remote host to which this PVC is to be connected.
DILC Station Address	Enter the station address of the remote host.

	PVC ACL	Enter the ACL for the PVC file. The default is + RE. The ACL controls what local users can use the PVC.
# SVC's	Enter a value, between 0 (the default) and 512, for the number of concurrent switched virtual connections (SVCs) you want to permit. All hosts on the LAN must specify the same number of SVCs. A central network administrator should set this value.	

Configuring a DILC Path to a Remote Host

After you have configured a DILC link, you can use it as a path to a remote host. Add the remote host, as described under "Configuring Remote Hosts" in Chapter 4. When you reach the question about paths, NETGEN requests the following information:

Path Information	Reply Guidelines
Path n	NETGEN displays a path number. Enter the number corresponding to the priority you want to give to the DILC path.
Do you wish to configure path(n) for any PMGR switched line?	Enter N (the default).
Link name	Enter the name of the DILC link that you have already configured. NETGEN responds by displaying the link type, DILC.
DILC Station Address in 12 Hexadecimal Digits	Enter the station address of the remote host.
Host Address	Enter the address of the remote host.

Integrated Control Board (ICB) (AOS/VS only)

The Integrated Control Board (ICB) is part of a multiple-device controller that supports the IEEE 802.3 and Ethernet protocols for local area networks. The ICB is an integral component of the ECLIPSE MV/4000® SC and DS 4000-series computer and cannot be ordered separately.

Configuring the ICB Device

From the main NETGEN menu, select option 2, "Manage Device Configurations." Then select option 1, "Add Device Configuration." NETGEN requests the following information:

Device Information	Reply Guidelines
Device Name	Assign a device name (1 to 16 AOS filename characters).
Device Type	Enter ICB.
Do you wish to specify the ICB Station Address?	To accept the default address, enter N. To override the default, enter Y; NETGEN asks the following question:

ICB Station Address in 12 Hexadecimal Digits	NETGEN displays the Data General vendor code as the first 6 digits. You enter 6 more hexadecimal digits.

A remote host uses the station address to identify your local host's position on this LAN. It must be unique across the LAN.

Each ICB has a unique value that NETGEN uses as the default station address. If you use the default, you must retain this initial address even if you later replace the board, because remote hosts know your host by this address. If your LAN has its own addressing system, you can override the default and enter the address provided by the central network administrator.

Configuring an ICB Link

After you have configured the ICB device, configure a link on the device. From the main NETGEN menu, select option 3, "Manage Link Configurations." Then select option 1, "Add Link Configuration." NETGEN requests the following information:

Link Information	Reply Guidelines
Link Name	Assign a link name (1 to 16 AOS filename characters).
Device Name	Enter the name of the previously configured ICB device. NETGEN responds by displaying the device type, ICB.
Configure this link for X25?	Enter Y.
Local Host Address	Enter the address of your host (2 to 15 decimal digits). The central network administrator should provide all host addresses.
Transmit retry count	Enter a value between 0 and 99. The default is 4. This value sets the number of times X.25 should automatically reattempt a failed data transmission. The value 0 means do not retry. Once the link is in use, if you receive frequent error messages that the retry count is exhausted, try doubling the current value and then lowering it until you reach an acceptable performance level. A value that is too high can cause X.25 to keep reattempting an impossible transmission.
Max Packet Size	Enter 512 (the default) or 1024. This value sets the maximum size, in bytes, for data packets transmitted on this link. If the major use for the link is file transfer, a larger packet size is more efficient. All hosts on the LAN must specify the same maximum. A central network administrator should set this value.
# PVC's	Enter a value, between 0 (the default) and 250, for the number of permanent virtual connections (PVCs) you want. All hosts on the LAN must specify the same number of PVCs. A central network administrator should set this value.

If you specify one or more PVCs, NETGEN also requests the following information:

PVC name	Assign a PVC name (1 to 16 AOS filename characters).
Host Address	Enter the address of the remote host to which this PVC is to be connected.
ICB Station Address	Enter the station address of the remote host.
PVC ACL	Enter the ACL for the PVC file. The default is + RE. The ACL controls what local users can use the PVC.

 # SVC's

Enter a value, between 0 (the default) and 512, for the number of concurrent switched virtual connections (SVCs) you want to permit.

All hosts on the LAN must specify the same number of SVCs. A central network administrator should set this value.

Configure this link for TCP/IP?

If you want this link to support only X.25 and XODIAC, enter N (the default). If you want it to support TCP/IP and Internet as well, enter Y; NETGEN prompts for further information. See the AOS/VS Internet documentation.

Configuring an ICB Path to a Remote Host

After you have configured an ICB link, you can use it as a path to a remote host. Add the remote host, as described under "Configuring Remote Hosts" in Chapter 4. When you reach the question about paths, NETGEN requests the following information:

Path Information	Reply Guidelines
Path n	NETGEN displays a path number. Enter the number corresponding to the priority you want to give to the ICB path.
Do you wish to configure path(n) for any PMGR switched line?	Enter N (the default).
Link name	Enter the name of the ICB link that you have already configured. NETGEN responds by displaying the link type, ICB.
ICB Station Address in 12 Hexadecimal Digits	Enter the station address of the remote host.
Host Address	Enter the address of the remote host.

Intelligent Broadband Controller (IBC) (AOS/VS only)

An Intelligent Broadband Controller (IBC) provides a connection between Data General ECLIPSE MV/Family systems and the Ungerman-Bass Net/One broadband local area network. The IBC supports the IEEE 802.3 standard and is compatible with the Ethernet specification at the data link layer.

Because the IBC is intelligent, you can run the X.25 portion of XTS on the controller rather than in main CPU memory.

Configuring the IBC Device

From the main NETGEN menu, select option 2, "Manage Device Configurations." Then select option 1, "Add Device Configuration." NETGEN requests the following information:

Device Information	Reply Guidelines
Device Name	Assign a device name (1 to 16 AOS filename characters).
Device Type	Enter IBC.
Run X25 on this controller?	Enter Y if you want to run X.25 on the controller. Enter N (the default) if you want to run X.25 on the main CPU.
Do you wish to specify the IBC Station Address?	To accept the default address, enter N. To override the default, enter Y; NETGEN asks the following question:
	IBC Station Address in 12 Hexadecimal Digits — NETGEN displays the Data General vendor code as the Digits first 6 digits. You enter 6 more hexadecimal digits.
	The station address identifies your host's position on this LAN. It must be unique across the LAN.
	Each IBC board has a unique value that NETGEN uses as the default station address. If you use the default, you must retain this initial address even if you later replace the board, because remote hosts know your host by this address. If your LAN has its own addressing system, you can override the default and enter the address provided by the central network administrator.
Device code	Enter an octal value between 1 and 677. The code must be unique among all the devices on your system. The default IBC code is 60. Your field engineer may provide a different value.

Configuring an IBC Link

After you have configured the IBC device, configure a link on the device. From the main NETGEN menu, select option 3, "Manage Link Configurations." Then

select option 1, "Add Link Configuration." NETGEN requests the following information:

Link Information	Reply Guidelines
Link Name	Assign a link name (1 to 16 AOS filename characters).
Device Name	Enter the name of the previously configured IBC device. NETGEN responds by displaying the device type, IBC.
Local Host Address	Enter the address of your host (2 to 15 decimal digits). The central network administrator should provide all host addresses.
Transmit retry count	Enter a value between 0 and 99. The default is 4. This value sets the number of times X.25 should automatically reattempt a failed data transmission. The value 0 means do not retry. Once the link is in use, if you receive frequent error messages that the retry count is exhausted, try doubling the current value and then lowering it until you reach an acceptable performance level. A value that is too high can cause X.25 to keep reattempting an impossible transmission.
Max packet size	Enter 512 (the default) or 1024. This value is the maximum size, in bytes, for data packets transmitted on this link. If the major use for the link is file transfer, a larger packet size is more efficient. All hosts on the LAN must specify the same maximum. A central network administrator should set this value.
# PVC's	Enter a value, between 0 (the default) and 250, for the number of permanent virtual connections (PVCs) you want. All hosts on the LAN must specify the same number of PVCs. A central network administrator should set this value. For each PVC you specify, NETGEN also requests the following information: *PVC name* — Assign a PVC name (1 to 16 AOS filename characters). *Host Address* — Enter the address of the remote host to which this PVC is to be connected. *IBC Station Address* — Enter the station address of the remote host.

PVC ACL	Enter the ACL for the PVC file. The default is + RE. The ACL controls what local users can use the PVC.
# SVC's	Enter a value, between 0 (the default) and 512, for the maximum number of concurrent switched virtual connections (SVCs) you want to permit. All hosts on the LAN must specify the same number of SVCs. A central network administrator should set this value.

Configuring an IBC Path to a Remote Host

After you have configured the IBC link, you can use it as a path to a remote host. Add the remote host, as described under "Configuring Remote Hosts" in Chapter 4. When you reach the question about paths, NETGEN requests the following information about the IBC link:

Path Information	Reply Guidelines
Path n	NETGEN displays a path number. Enter the number corresponding to the priority you want to give to the IBC path.
Do you wish to configure path(n) for any PMGR switched line?	Enter N (the default).
Link name	Enter the name of the IBC link that you have already configured. NETGEN responds by displaying the link type, IBC.
IBC Station Address in 12 Hexadecimal Digits	Enter the station address of the remote host.
Host Address	Enter the address of the remote host.

Intelligent LAN Controller (ILC) (AOS/VS only)

The Intelligent Local Area Network Controller (ILC) is the 802.3 board for MV/Family systems. It supports the Ethernet and IEEE 802.3 protocols. The ILC contains an microECLIPSE processor for increased performance.

In configuring an ILC, note the following options:

- You can run the X.25 portion of XTS on the controller rather than in main CPU memory.
- This section tells how to configure an ILC link for use by X.25 and XODIAC. In addition, you can configure the same link for use by TCP/IP and Internet. TCP/IP communications software is supported under both AOS/VS and DG/UX™.

Configuring the ILC Device

From the main NETGEN menu, select option 2, "Manage Device Configurations." Then select option 1, "Add Device Configuration." NETGEN requests the following information:

Device Information	Reply Guidelines
Device Name	Assign a device name (1 to 16 AOS filename characters).
Device Type	Enter ILC.
Run X25 on this controller?	Enter Y if you want to run X.25 on the controller. Enter N (the default) if you want to run X.25 on the main CPU.
Do you wish to specify the ILC Station Address?	To accept the default address, enter N. To override the default, enter Y; NETGEN asks the following question:
	ILC Station Address in 12 Hexadecimal Digits — NETGEN displays the Data General vendor code as the first 6 digits. You enter 6 more hexadecimal digits.

Do you wish to specify the ILC Station Address? (cont.)	A remote host uses the station address to identify your local host's position on the LAN. It must be unique across the LAN. Each ILC board has a unique value that NETGEN uses as the default station address. If you use the default, you must retain this initial address even if you later replace the board, because remote hosts know your host by this address. If your LAN has its own addressing system, you can override the default and enter the address provided by the central network administrator.
Device code	Enter an octal value between 1 and 677. The code must be unique among all the devices on your system. The default ILC code is 60. Your field engineer may provide a different value.

Configuring an ILC Link

After you have configured the ILC device, configure a link on the device. From the main NETGEN menu, select option 3, "Manage Link Configurations." Then select option 1, "Add Link Configuration." NETGEN requests the following information:

Link Information	**Reply Guidelines**
Link Name	Assign a link name (1 to 16 AOS filename characters).
Device Name	Enter the name of the previously configured ILC device. NETGEN responds by displaying the device type, ILC.
Configure this link for X25?	Enter Y.
Local Host Address	Enter the address of your host (2 to 15 decimal digits). The central network administrator should provide all host addresses.
Transmit retry count	Enter a value between 0 and 99. The default is 4. The value sets the number of times X.25 should automatically reattempt a failed data transmission. The value 0 means do not retry. Once the link is in use, if you receive frequent error messages that the retry count is exhausted, try doubling the current value and then lowering it until you reach an acceptable performance level. A value that is too high can cause X.25 to keep reattempting an impossible transmission.
Max Packet Size	Enter 512 (the default) or 1024. This value sets the maximum size, in bytes, for data packets transmitted on this link. If the major use for the link is file transfer, a larger packet size is more efficient.

All hosts on the LAN must specify the same maximum. A central network administrator should set this value.

 # PVC's

Enter a value, between 0 (the default) and 250, for the number of permanent virtual connections (PVCs) you want.

All hosts on the LAN must specify the same number of PVCs. A central network administrator should set this value.

If you specify one or more PVCs, NETGEN also requests the following information:

PVC name	Assign a PVC name (1 to 16 AOS filename characters).
Host Address	Enter the address of the remote host to which this PVC is to be connected.
ILC Station Address	Enter the station address of the remote host.
PVC ACL	Enter the ACL for the PVC file. The default is + RE. The ACL controls what local users can use the PVC.

 # SVC's

Enter a value, between 0 (the default) and 512, for the maximum number of concurrent switched virtual connections (SVCs) you want to permit.

All hosts on the LAN must specify the same number of SVCs. A central network administrator should set this value.

Configure this link for TCP/IP?

If you want this link to support only X.25 and XODIAC, enter N (the default). If you want it to support TCP/IP and Internet as well, enter Y; NETGEN prompts you for further information. See the AOS/VS Internet documentation.

Configuring an ILC Path to a Remote Host

After you have configured an ILC link, you can use it as a path to a remote host. Add the remote host, as described under "Configuring Remote Hosts" in Chapter 4. When you reach the question about paths, NETGEN requests the following information:

Path Information	Reply Guidelines
Path n	NETGEN displays a path number. Enter the number corresponding to the priority you want to give to the ILC path.
Do you wish to configure path(n) for any PMGR switched line?	Enter N (the default).
Link name	Enter the name of the ILC link that you have already configured. NETGEN responds by displaying the link type, ILC.
ILC Station Address in 12 Hexadecimal Digits	Enter the station address of the remote host.
Host Address	Enter the address of the remote host.

Intelligent Synchronous Controller (ISC/2 and ISMC/2)

You can use NETGEN to configure the following Data General Intelligent Synchronous Controllers:

- Intelligent Synchronous Controller (ISC/2), for AOS and AOS/VS systems
- Intelligent Synchronous Microcontroller (ISMC/2), for DESKTOP GENERATION systems

Both controllers are single-board, front-end processors. The ISC includes a microECLIPSE™ processor and two bit- or byte-synchronous communications lines. In synchronous mode, an ISC line can support the binary synchronous, SDLC, or HDLC protocols.

In configuring an ISC, note the following options:

- When you configure the ISC link, you can set certain parameters, which in other controllers are set in the hardware. These parameters relate to framing and clocking.
- Under AOS/VS, you can run the X.25 portion of XTS on the controller rather than in main CPU memory.

Configuring the ISC Device

From the main NETGEN menu, select option 2, "Manage Device Configurations." Then select option 1, "Add Device Configuration." NETGEN requests the following information:

Device Information	Reply Guidelines
Device Name	Assign a device name (1 to 16 AOS filename characters).
Device Type	Enter ISC.
Run X25 on this controller? (AOS/VS only)	Enter Y if you want to run X.25 on the controller. Enter N (the default) if you want to run X.25 on the main CPU.
Device code (AOS/VS only)	Enter an octal value in the range 1 to 677. The code must be unique among all the devices on your system. The default ISC code is 25. Your field engineer may provide a different value.

Configuring an ISC Link

After you have configured the ISC device, configure a link on the device. You configure a separate link for each ISC line that you want to use.

From the main NETGEN menu, select option 3, "Manage Link Configurations." Then select option 1, "Add Link Configuration." NETGEN requests the following information:

Link Information	Reply Guidelines
Link Name	Assign a link name (1 to 16 AOS filename characters).
Device Name	Enter the name of the previously configured ISC device. NETGEN responds by displaying the device type, ISC.
Network Type	If you are on a PDN, enter the type of PDN from the list that NETGEN displays; if your type is not on the list, enter OTHER. If you are not on a PDN, enter DATA GENERAL (the default).
Line #	Under AOS, enter a number between 0 and 15. Under AOS/VS, enter 0 or 1.
Protocol Type	Enter LAP (Link Access Protocol) or LAPB (Balanced Link Access Protocol). The default is LAPB. Accept the default unless you know that your link uses LAP.
DTE or DCE	Enter DTE or DCE. The default is DTE. NETGEN asks this question only if you answered DATA GENERAL or OTHER for Network Type. If you specified a PDN, NETGEN automatically chooses DTE. The X.25 protocol defines the DTE as the data terminal equipment (the user's equipment) and the DCE as the data circuit-terminating equipment (the connection to the PDN). Data General's X.25 implementation can also connect two hosts in a point-to-point connection. If you did not specify a PDN, you arbitrarily assign one host the DCE role and the other the DTE role.
Local Host Address	Enter the address of your host (2 to 15 decimal digits). The PDN administrator or central network administrator should provide all host addresses.
Sequence Numbering Modulus	Enter 8 (the default) or 128. The value determines the system used to number the packets transmitted on the link. If you need to permit a larger number of outstanding frames, use 128 rather than 8.
Connect retry count	Enter a value between 0 and 99. The default is 10. The value sets the number of times X.25 should automatically reattempt to establish a connection with a remote host. The value 0 means do not retry. Unless there are known problems on the link, it is usually best to set a low retry count, to keep X.25 from repeatedly trying to establish an impossible connection.

Transmit retry count

Enter a value between 0 and 99. The default is 10. The value sets the number of times X.25 should automatically reattempt a failed data transmission. The value 0 means do not retry.

Once the link is in use, if you receive frequent error messages that the retry count is exhausted, try doubling the current value and then lowering it until you reach an acceptable performance level. A value that is too high can cause X.25 to keep reattempting an impossible transmission.

Transmit timeout

Enter –1 or a value between 0 and 3600. The default is 3. This value sets the number of seconds X.25 waits for the next host in a route to acknowledge a data transmission. If the time-out period expires, X.25 retries the transmission.

The value –1 means wait forever (infinite time-out). The value 0 means do not wait. Neither of these values is recommended.

Use the following formula to compute the time-out period for your system:

First compute t, the time required to transmit a single frame. Use p (the value you specify as Max Packet Size on this screen) and r (the rate of transmission in bits per second, which you either specify as Internal Clock Rate on this screen or take from the external modem).

$$t = \frac{(p \times 8)}{r}$$

On a full-duplex line, the time-out period should be the ceiling of

$$2t + 1$$

On a half-duplex line, you must also use w (the value you specify as Frame Window Size on this screen). The time-out period should be the ceiling of

$$[(w + 1) \times t] + 1$$

Enable timeout

Enter –1 or a value between 0 and 3600. The default is 30. This value sets the number of seconds X.25 waits before giving up an attempt to connect with a local modem. A value of –1 means wait forever (infinite time-out). A value of 0 means do not wait. It is usually best to keep this value between 5 and 40.

Frame Window Size

Enter a value between 1 and 7. The default is 7. A frame is the link level unit of data transmission. This value sets the maximum number of frames that X.25 can send without receiving an acknowledgement from the next host in the route.

Frame Window Size (cont.)

On a PDN, you enter the window size set by the administrator. In a point-to-point connection, both hosts must specify the same window size.

A small window size can slow performance by forcing X.25 to wait for acknowledgements. If the link or remote host is slow, you can improve performance by raising the window size.

Packet Window Size

Enter a value between 1 and 7. The default is 2. A packet is the network level unit of data transmission. This value sets the maximum number of packets that X.25 can send without receiving an acknowledgement from the destination host. See the comment on Frame Window Size.

On a PDN, you enter the window size set by the administrator. In a point-to-point connection, both hosts must specify the same window size.

Max Packet Size

Enter one of these values: 32, 64, 128 (the default), 256, 512, 1024. This value sets the maximum size, in bytes, for data packets transmitted on this link. If the major use for the link is file transfer, a larger packet size is more efficient.

On a PDN, you enter the maximum set by the administrator. In a point-to-point connection, both hosts must specify the same maximum.

Framing Type

Enter HDLC (High-level Data Link Control, the default) or BSC (Byte Synchronous Control). HDLC is for bit-synchronous framing and is compatible with existing BLM or BSI boards. BSC is for byte synchronous framing and is compatible with existing SLM or CSI boards.

On a PDN, you enter the framing type set by the administrator. In a point-to-point connection, both hosts must specify the same framing type.

If you answer HDLC, NETGEN also asks about HDLC encoding and full- or half-duplex. If you answer BSC, NETGEN does not ask these questions.

HDLC Encoding

Enter NRZ (nonreturn to zero, direct encoding) or NRZI (nonreturn to zero, inverted encoding). The parameter sets the method of representing zeros and ones. The default is NRZ. Certain kinds of modems require NRZI.

NETGEN asks this question only if you entered HDLC for Framing Type.

On a PDN, you enter the encoding type set by the administrator. In a point-to-point connection, both hosts must specify the same encoding type.

Note that even if a modem requires NRZI, it cannot extract clock values from the data stream. This parameter sets only the encoding type, not the clock rate.

Clocking
(AOS/VS only)

If you will use a modem or external clock, enter EXTERNAL (the default). If you want to generate clock signals from the board, enter INTERNAL; NETGEN asks the following question:

Internal Clock Rate

Enter one of these values: 300, 600, 1200, 2400, 4800, 9600 (the default), 19.2K, 38.4K. This value is the clock rate, in bits per second. (The K indicates kilobits per second.)

If you have configured both ISC lines for HDLC framing, the total clock rate must not exceed 38.4 kilobits per second.

If you have configured both ISC lines for BSC framing, the total clock rate must not exceed 19.2 kilobits per second.

FULL or HALF duplex
(AOS/VS only)

Enter FULL (the default) or HALF, based on the kind of modem you are using. NETGEN asks this question only if you entered HDLC for Framing Type.

On a PDN, you enter the duplex type set by the administrator. In a point-to-point connection, both hosts must specify the same duplex type.

 # PVC's

Enter a value in the following range:

0–64 (AOS)
0–250 (AOS/VS)

The default is 0. This is the number of permanent virtual connections (PVCs) you want.

On a PDN, you enter the number set by the administrator. In a point-to-point connection, both hosts must specify the same number of PVCs.

If you specify one or more PVCs, NETGEN asks the following question:

Start PVC # :

NETGEN begins numbering PVCs at this number, which must be between 1 (the default) and 4095. On a PDN, you enter the number reserved for your host's PVCs. In a point-to-point connection, both hosts must specify the same starting number.

If you specify one or more PVCs, NETGEN also requests the following information:

PVC name	Assign a PVC name (1 to 16 AOS filename characters).
Host Address	Enter the address of the remote host to which this PVC is to be connected.
PVC ACL	Enter the ACL for the PVC file. The default is + RE. The ACL controls what local users can use the PVC.

 # SVC's

Enter a value in the following range:

0–126 (AOS)
0–512 (AOS/VS)

The default is 0. This is the number of concurrent switched virtual connections (SVCs) you want to permit.

On a PDN, you enter the number set by the administrator. In a point-to-point connection, both hosts must specify the same number of SVCs.

If you specify one or more SVCs, NETGEN asks the following question:

Start SVC # :

NETGEN begins numbering SVCs at this number, which must be between the highest PVC number plus 1 (the default) and 4095. On a PDN, you enter the number reserved for your host's SVCs. In a point-to-point connection, both hosts must specify the same starting number.

Configuring an ISC Path to a Remote Host

After you have configured an ISC link, you can use it as a path to a remote host. Add the remote host, as described under "Configuring Remote Hosts" in Chapter 4. When you reach the question about paths, NETGEN requests the following information:

Path Information	Reply Guidelines
Path n	NETGEN displays a path number. Enter the number corresponding to the priority you want to give to the ISC path.
Do you wish to configure path(n) for any PMGR switched line?	Enter N (the default).
Link name	Enter the name of the ISC link that you have already configured. NETGEN responds by displaying the link type, ISC, and the network type.
Host Address	Enter the address of the remote host.

Interlan NI4010A (ILAN) (AOS/VS only)

The Interlan NI4010A Data General Ethernet/IEEE 802 Communications Controller lets MV/Family systems connect to an Ethernet or IEEE 802.3 local area network. The Interlan NI4010A board and controller are manufactured and marketed by Interlan Inc.

Configuring the ILAN Device

From the main NETGEN menu, select option 2, "Manage Device Configurations." Then select option 1, "Add Device Configuration." NETGEN requests the following information:

Device Information	Reply Guidelines
Device Name	Assign a device name (1 to 16 AOS filename characters).
Device Type	Enter ILAN.
Do you wish to specify the ILAN Station Address?	To accept the default address, enter N. To override the default, enter Y; NETGEN asks the following question: *ILAN Station Address in 12 Hexadecimal Digits* — NETGEN displays the Data General vendor code as the first 6 digits. You enter 6 more hexadecimal digits. A remote host uses the station address to identify your local host's position on this LAN. It must be unique across the LAN. Each ILAN board has a unique value that NETGEN uses as the default station address. If you use the default, you must retain this initial address even if you later replace the board, because remote hosts know your host by this address. If your LAN has its own addressing system, you can override the default and enter the address provided by the central network administrator.
Device code	Enter an octal value between 1 and 677. The code must be unique among all the devices on your system. The default ILAN code is 46. Your field engineer may provide a different value.

Configuring an ILAN Link

After you have configured the ILAN device, configure a link on the device. From the main NETGEN menu, select option 3, "Manage Link Configurations." Then select option 1, "Add Link Configuration." NETGEN requests the following information:

Link Information	Reply Guidelines
Link Name	Assign a link name (1 to 16 AOS filename characters).
Device Name	Enter the name of the previously configured ILAN device. NETGEN responds by displaying the device type, ILAN.
Local Host Address	Enter the address of your host (2 to 15 decimal digits). The central network administrator should provide all host addresses.
Transmit retry count	Enter a value between 0 and 99. The default is 4. The value sets the number of times X.25 should automatically reattempt a failed data transmission. The value 0 means do not retry. Once the link is in use, if you receive frequent error messages that the retry count is exhausted, try doubling the current value and then lowering it until you reach an acceptable performance level. A value that is too high can cause X.25 to keep reattempting an impossible transmission.
Max Packet Size	Enter 512 (the default) or 1024. This value sets the maximum size, in bytes, for data packets transmitted on this link. If the major use for the link is file transfer, a larger packet size is more efficient. All hosts on the LAN must specify the same maximum. A central network administrator should set this value.
# PVC's	Enter a value, between 0 (the default) and 250, for the number of permanent virtual connections (PVCs) you want. All hosts on the LAN must specify the same number of PVCs. A central network administrator should set this value. If you specify one or more PVCs, NETGEN also requests the following information: *PVC name* — Assign a PVC name (1 to 16 AOS filename characters). *Host Address* — Enter the address of the remote host to which this PVC is to be connected. *ILAN Station Address* — Enter the station address of the remote host.

PVC ACL	Enter the ACL for the PVC file. The default is + RE. The ACL controls what local users can use the PVC.
# SVC's	Enter a value, between 0 (the default) and 512, for the number of concurrent switched virtual connections (SVCs) you want to permit. All hosts on the LAN must specify the same number of SVCs. A central network administrator should set this value.

Configuring an ILAN Path to a Remote Host

After you have configured an ILAN link, you can use it as a path to a remote host. Add the remote host, as described under "Configuring Remote Hosts" in Chapter 4. When you reach the question about paths, NETGEN requests the following information:

Path Information	Reply Guidelines
Path n	NETGEN displays a path number. Enter the number corresponding to the priority you want to give to the ILAN path.
Do you wish to configure path(n) for any PMGR switched line?	Enter N (the default).
Link name	Enter the name of the ILAN link that you have already configured. NETGEN responds by displaying the link type, ILAN.
ILAN Station Address in 12 Hexadecimal Digits	Enter the station address of the remote host.
Host Address	Enter the address of the remote host.

L-Bus LAN Controller (LLC) (AOS/VS only)

An L-Bus Local Area Network Controller (LLC) is the 802.3 board for ECLIPSE MV/2000 DC and DS systems. It supports the IEEE 802.3 and Ethernet protocols for local area networks. The LLC has its own memory that is addressable by X.25. It makes use of the memory-mapped L-Bus technology of the MV/2000 series.

Configuring the LLC Device

From the main NETGEN menu, select option 2, "Manage Device Configurations." Then select option 1, "Add Device Configuration." NETGEN requests the following information:

Device Information	Reply Guidelines
Device Name	Assign a device name (1 to 16 AOS filename characters).
Device Type	Enter LLC.
Do you wish to specify the LLC Station Address?	To accept the default address, enter N. To override the default, enter Y; NETGEN asks the following question: *LLC Station Address in 12 Hexadecimal Digits* — NETGEN displays the Data General vendor code as the first 6 digits. You enter 6 more hexadecimal digits. A remote host uses the station address to identify your local host's position on the LAN. It must be unique across the LAN. Each LLC board has a unique value that NETGEN uses as the default station address. If you use the default, you must retain this initial address even if you later replace the board, because remote hosts know your host by this address. If your LAN has its own addressing system, you can override the default and enter the address provided by the central network administrator.
Device code	Enter an octal value between 1 and 677. The code must be unique among all the devices on your system. The default LLC code is 74. Your field engineer may provide a different value.

Configuring an LLC Link

After you have configured the LLC device, configure a link on the device. From the main NETGEN menu, select option 3, "Manage Link Configurations." Then select option 1, "Add Link Configuration." NETGEN requests the following information:

Link Information	Reply Guidelines
Link Name	Assign a link name (1 to 16 AOS filename characters).
Device Name	Enter the name of the previously configured LLC device. NETGEN responds by displaying the device type, LLC.
Local Host Address	Enter the address of your host (2 to 15 decimal digits). The central network administrator should provide all host addresses.
Transmit retry count	Enter a value between 0 and 99. The default is 4. The value sets the number of times X.25 should automatically reattempt a failed data transmission. The value 0 means do not retry. Once the link is in use, if you receive frequent error messages that the retry count is exhausted, try doubling the current value and then lowering it until you reach an acceptable performance level. A value that is too high can cause X.25 to keep reattempting an impossible transmission.
Max Packet Size	Enter 512 (the default) or 1024. This value sets the maximum size, in bytes, for data packets transmitted on this link. If the major use for the link is file transfer, a larger packet size is more efficient. All hosts on the LAN must specify the same maximum. A central network administrator should set this value.
# PVC's	Enter a value, between 0 (the default) and 250, for the number of permanent virtual connections (PVCs) you want. All hosts on the LAN must specify the same number of PVCs. A central network administrator should set this value. If you specify one or more PVCs, NETGEN also requests the following information: *PVC name* — Assign a PVC name (1 to 16 AOS filename characters). *Host Address* — Enter the address of the remote host to which this PVC is to be connected. *LLC Station Address in 12 Hexadecimal Digits* — Enter the station address of the remote host.

	PVC ACL	Enter the ACL for the PVC file. The default is + RE. The ACL controls what local users can use the PVC.
# SVC's	Enter a value, between 0 (the default) and 512, for the maximum number of concurrent switched virtual connections (SVCs) you want to permit. All hosts on the LAN must specify the same number of SVCs. A central network administrator should set this value.	

Configuring an LLC Path to a Remote Host

After you have configured an LLC link, you can use it as a path to a remote host. Add the remote host, as described under "Configuring Remote Hosts" in Chapter 4. When you reach the question about paths, NETGEN requests the following information:

Path Information	Reply Guidelines
Path n	NETGEN displays a path number. Enter the number corresponding to the priority you want to give to the LLC path.
Do you wish to configure path(n) for any PMGR switched line?	Enter N (the default).
Link name	Enter the name of the LLC link that you have already configured. NETGEN responds by displaying the link type, LLC.
LLC Station Address in 12 Hexadecimal Digits	Enter the station address of the remote host.
Host Address	Enter the address of the remote host.

L-Bus Synchronous Controller (LSC) (AOS/VS only)

The L-Bus Synchronous Controller is a single-board intelligent controller for ECLIPSE MV/2000 DC and DS systems. It includes a microECLIPSE processor and two bit- or byte-synchronous communications lines.

In configuring an LSC, note the following options:

- When you configure the LSC link, you can set certain parameters, which in other controllers are set in the hardware. These parameters relate to framing and clocking.
- You can run the X.25 portion of XTS on the controller rather than in main CPU memory.

Configuring the LSC Device

From the main NETGEN menu, select option 2, "Manage Device Configurations." Then select option 1, "Add Device Configuration." NETGEN requests the following information:

Device Information	Reply Guidelines
Device Name	Assign a device name (1 to 16 AOS filename characters).
Device Type	Enter LSC.
Run X25 on this controller?	Enter Y if you want to run X.25 on the controller. Enter N (the default) if you want to run X.25 on the main CPU.
Device code	Enter an octal value in the range 1 to 677. The code must be unique among all the devices on your system. The default LSC code is 31. Your field engineer may provide a different value.

Configuring an LSC Link

After you have configured the LSC device, configure a link on the device. You configure a separate link for each LSC line that you want to use.

From the main NETGEN menu, select option 3, "Manage Link Configurations." Then select option 1, "Add Link Configuration." NETGEN requests the following information:

Link Information	Reply Guidelines
Link Name	Assign a link name (1 to 16 AOS filename characters).
Device Name	Enter the name of the previously configured LSC device. NETGEN responds by displaying the device type, LSC.

Network Type

If you are on a PDN, enter the type of PDN from the list that NETGEN displays; if your type is not on the list, enter OTHER. If you are not on a PDN, enter DATA GENERAL (the default).

Line #

Enter 0 or 1.

Protocol Type

Enter LAP (Link Access Protocol) or LAPB (Balanced Link Access Protocol). The default is LAPB. Accept the default unless you know that your link uses LAP.

DTE or DCE

Enter DTE or DCE. The default is DTE. NETGEN asks this question only if you answered DATA GENERAL or OTHER for Network Type. If you specified a PDN, NETGEN automatically chooses DTE.

The X.25 protocol defines the DTE as the data terminal equipment (the user's equipment) and the DCE as the data circuit-terminating equipment (the connection to the PDN). Data General's X.25 implementation can also connect two hosts in a point-to-point connection. If you did not specify a PDN, you arbitrarily assign one host the DCE role and the other the DTE role.

Local Host Address

Enter the address of your host (2 to 15 decimal digits). The PDN administrator or central network administrator should provide all host addresses.

Sequence Numbering Modulus

Enter 8 (the default) or 128. The value determines the system used to number the packets transmitted on the link. If you need to permit a large number of outstanding frames, use 128 rather than 8.

Connect retry count

Enter a value between 0 and 99. The default is 10. The value sets the number of times X.25 should automatically reattempt to establish a connection with a remote host. The value 0 means do not retry.

Unless there are known problems on the link, it is usually best to set a low retry count, to keep X.25 from repeatedly trying to establish an impossible connection.

Transmit retry count

Enter a value between 0 and 99. The default is 10. The value sets the number of times X.25 should automatically reattempt a failed data transmission. The value 0 means do not retry.

Once the link is in use, if you receive frequent error messages that the retry count is exhausted, try doubling the current value and then lowering it until you reach an acceptable performance level. A value that is too high can cause X.25 to keep reattempting an impossible transmission.

Transmit timeout

Enter –1 or a value between 0 and 3600. The default is 3. This value sets the number of seconds X.25 waits for the next host in a route to acknowledge a data transmission. If the time-out period expires, X.25 retries the transmission.

The value –1 means wait forever (infinite time-out). The value 0 means do not wait. Neither of these values is recommended.

Use the following formula to compute the time-out period for your system:

First compute t, the time required to transmit a single frame. Use p (the value you specify as Max Packet Size on this screen) and r (the rate of transmission in bits per second, which you either specify as Internal Clock Rate on this screen or take from the external modem).

$$t = \frac{(p \times 8)}{r}$$

On a full-duplex line, the time-out period should be the ceiling of

$$2t + 1$$

On a half-duplex line, you must also use w (the value you specify as Frame Window Size on this screen). The time-out period should be the ceiling of

$$[(w + 1) \times t] + 1$$

Enable timeout

Enter –1 or a value between 0 and 3600. The default is 30. This value sets the number of seconds X.25 waits before giving up an attempt to connect with a local modem. A value of –1 means wait forever (infinite time-out). A value of 0 means do not wait. It is usually best to keep this value between 5 and 40.

Frame Window Size

Enter a value between 1 and 7. The default is 7. A frame is the link level unit of data transmission. This value sets the maximum number of frames that X.25 can send without receiving an acknowledgement from the next host in the route.

On a PDN, you enter the window size set by the administrator. In a point-to-point connection, both hosts must specify the same window size.

A small window size can slow performance by forcing X.25 to wait for acknowledgements. If the link or remote host is slow, you can improve performance by raising the window size.

Packet Window Size

Enter a value between 1 and 7. The default is 2. A packet is the network level unit of data transmission. This value sets the maximum number of packets that X.25 can send without receiving an acknowledgement from the destination host. See the comment on Frame Window Size.

On a PDN, you enter the window size set by the administrator. In a point-to-point connection, both hosts must specify the same window size.

Max Packet Size

Enter one of these values: 32, 64, 128 (the default), 256, 512, 1024. This value sets the maximum size, in bytes, for data packets transmitted on this link. If the major use for the link is file transfer, a larger packet size is more efficient.

On a PDN, you enter the maximum set by the administrator. In a point-to-point connection, both hosts must specify the same maximum.

Framing Type

Enter HDLC (High-level Data Link Control, the default) or BSC (Byte Synchronous Control). HDLC is for bit-synchronous framing and is compatible with existing BLM or BSI boards. BSC is for byte-synchronous framing and is compatible with existing SLM or CSI boards.

On a PDN, you enter the framing type set by the administrator. In a point-to-point connection, both hosts must specify the same framing type.

If you answer HDLC, NETGEN also asks about HDLC encoding and full- or half-duplex. If you answer BSC, NETGEN does not ask these questions.

HDLC Encoding

Enter NRZ (nonreturn to zero, direct encoding) or NRZI (nonreturn to zero, inverted encoding). The parameter sets the method of representing zeros and ones. The default is NRZ. Certain kinds of modems require NRZI.

NETGEN asks this question only if you entered HDLC for Framing Type.

On a PDN, you enter the encoding type set by the administrator. In a point-to-point connection, both hosts must specify the same encoding type.

Note that even if a modem requires NRZI, it cannot extract clock values from the data stream. This parameter sets only the encoding type, not the clock rate.

Clocking

If you will use a modem or external clock, enter EXTERNAL (the default). If you want to generate clock signals from the board, enter INTERNAL; NETGEN asks the following question:

Internal Clock Rate

Enter one of these values: 300, 600, 1200, 2400, 4800, 9600 (the default), 19.2K, 38.4K. This value is the clock rate, in bits per second. (The K indicates kilobits per second.)

If you have configured both LSC lines for HDLC framing, the total clock rate must not exceed 38.4 kilobits per second.

If you have configured both LSC lines for BSC framing, the total clock rate must not exceed 19.2 kilobits per second.

FULL or HALF duplex

Enter FULL (the default) or HALF, based on the kind of modem you are using. NETGEN asks this question only if you entered HDLC for Framing Type.

On a PDN, you enter the duplex type set by the administrator. In a point-to-point connection, both hosts must specify the same duplex type.

 # PVC's

Enter a value, between 0 (the default) and 250, for the number of permanent virtual connections (PVCs) you want.

On a PDN, you enter the number set by the administrator. In a point-to-point connection, both hosts must specify the same number of PVCs.

If you specify one or more PVCs, NETGEN asks the following question:

Start PVC # :

NETGEN begins numbering PVCs at this number, which must be between 1 (the default) and 4095. On a PDN, you enter the number reserved for your host's PVCs. In a point-to-point connection, both hosts must specify the same starting number.

If you specify one or more PVCs, NETGEN also requests the following information:

PVC name

Assign a PVC name (1 to 16 AOS filename characters).

	Host Address	Enter the address of the remote host to which this PVC is to be connected.
	PVC ACL	Enter the ACL for the PVC file. The default is + RE. The ACL controls what local users can use the PVC.
# SVC's		Enter a value, between 0 (the default) and 512, for the number of concurrent switched virtual connections (SVCs) you want to permit. On a PDN, you enter the number set by the administrator. In a point-to-point connection, both hosts must specify the same number of SVCs. If you specify one or more SVCs, NETGEN asks the following question: *Start SVC # :* NETGEN begins numbering SVCs at this number, which must be between the highest PVC number plus 1 (the default) and 4095. On a PDN, you enter the number reserved for your host's SVCs. In a point-to-point connection, both hosts must specify the same starting number.

Configuring an LSC Path to a Remote Host

After you have configured an LSC link, you can use it as a path to a remote host. Add the remote host, as described under "Configuring Remote Hosts" in Chapter 4. When you reach the question about paths, NETGEN requests the following information:

Path Information	Reply Guidelines
Path n	NETGEN displays a path number. Enter the number corresponding to the priority you want to give to the LSC path.
Do you wish to configure path(n) for any PMGR switched line?	Enter N (the default).
Link name	Enter the name of the LSC link that you have already configured. NETGEN responds by displaying the link type, LSC, and the network type.
Host Address	Enter the address of the remote host.

Multi-Communications Processor (MCP1) (AOS/VS only)

A Multi-Communications Processor (MCP1) is a general purpose, intelligent communications board. Originally designed as part of the ECLIPSE MV/4000 SC system, it is now available as a separate product for any MV/Family system. The MCP1 consists of a two-line intelligent synchronous controller, an eight-line intelligent asynchronous controller, and a data channel/line printer controller interface. NETGEN lets you configure the MCP1 as an intelligent synchronous controller.

Note that NETGEN does not have a separate device type for MCP1. Instead, you configure it as if it were an ISC but provide values appropriate to an MCP1.

In configuring an MCP1, note the following options:

- When you configure the ISC link, you can set certain parameters, which in other controllers are set in the hardware. These parameters relate to framing and clocking.
- You can run the X.25 portion of XTS on the controller rather than in main CPU memory.

Configuring the MCP1 Device

From the main NETGEN menu, select option 2, "Manage Device Configurations." Then select option 1, "Add Device Configuration." NETGEN requests the following information:

Device Information	Reply Guidelines
Device Name	Assign a device name (1 to 16 AOS filename characters).
Device Type	Enter ISC. NETGEN does not have a separate category for an MCP1.
Run X25 on this controller?	Enter Y if you want to run X.25 on the controller. Enter N (the default) if you want to run X.25 on the main CPU.
Device code	Enter an octal value between 1 and 677. The code must be unique among all the devices on your system. The default ISC code does not apply to an MCP1. Your field engineer can provide the correct value.

Configuring an MCP1 Link

After you have configured the MCP1 device, configure a link on the device. From the main NETGEN menu, select option 3, "Manage Link Configurations." Then select option 1, "Add Link Configuration." NETGEN requests the following information:

Link Information	Reply Guidelines
Link Name	Assign a link name (1 to 16 AOS filename characters).
Device Name	Enter the name of the previously configured MCP1 device. NETGEN responds by displaying the device type, ISC.
Network Type	If you are on a PDN, enter the type of PDN from the list that NETGEN displays; if your type is not on the list, enter OTHER. If you are not on a PDN, enter DATA GENERAL (the default).
Line #	Enter 0 or 1.
Protocol Type	Enter LAP (Link Access Protocol) or LAPB (Balanced Link Access Protocol). The default is LAPB. Accept the default unless you know that your link uses LAP.
DTE or DCE	Enter DTE or DCE. The default is DTE. The X.25 protocol defines the DTE as the data terminal equipment (the user's equipment) and the DCE as the data circuit-terminating equipment (the connection to the PDN). Data General's X.25 implementation can also connect two hosts in a point-to-point connection. If you did not specify a PDN, you arbitrarily assign one host the DCE role and the other the DTE role.
Local Host Address	Enter the address of your host (2 to 15 decimal digits). The PDN administrator or central network administrator should provide all host addresses.
Sequence Numbering Modulus	Enter 8 (the default) or 128. The value determines the system used to number the packets transmitted on the link. If you need to permit a large number of outstanding frames, use 128 as the modulus.
Connect retry count	Enter a value between 0 and 99. The default is 10. The value sets the number of times X.25 should automatically reattempt to establish a connection with a remote host. The value 0 means do not retry. Unless there are known problems on the link, it is usually best to set a low retry count, to keep X.25 from repeatedly trying to establish an impossible connection.
Transmit retry count	Enter a value between 0 and 99. The default is 10. The value sets the number of times X.25 should automatically reattempt a failed data transmission. The value 0 means do not retry.

Transmit retry count (cont.)

Once the link is in use, if you receive frequent error messages that the retry count is exhausted, try doubling the current value and then lowering it until you reach an acceptable performance level. A value that is too high can cause X.25 to keep reattempting an impossible transmission.

Transmit timeout

Enter –1 or a value between 0 and 3600. The default is 3. This value sets the number of seconds X.25 waits for the next host in a route to acknowledge a data transmission. If the time-out period expires, X.25 retries the transmission.

The value –1 means wait forever (infinite time-out). The value 0 means do not wait. Neither of these values is recommended.

Use the following formula to compute the time-out period for your system:

First compute t, the time required to transmit a single frame. Use p (the value you specify as Max Packet Size on this screen) and r (the rate of transmission in bits per second, which you either specify as Internal Clock Rate on this screen or take from the external modem).

$$t = \frac{(p \times 8)}{r}$$

On a full-duplex line, the time-out period should be the ceiling of

$$2t + 1$$

On a half-duplex line, you must also use w (the value you specify as Frame Window Size on this screen). The time-out period should be the ceiling of

$$[(w + 1) \times t] + 1$$

Enable timeout

Enter –1 or a value between 0 and 3600. The default is 30. This value sets the number of seconds X.25 waits before giving up an attempt to connect with a local modem. A value of –1 means wait forever (infinite time-out). A value of 0 means do not wait. It is usually best to keep this value between 5 and 40.

Frame Window Size

Enter a value between 1 and 7. The default is 7. A frame is the link level unit of data transmission. This value sets the maximum number of frames that X.25 can send without receiving an acknowledgement from the next host in the route.

On a PDN, you enter the window size set by the administrator. In a point-to-point connection, both hosts must specify the same window size.

A small window size can slow performance by forcing X.25 to wait for acknowledgements. If the link or remote host is slow, you can improve performance by raising the window size.

Packet Window Size

Enter a value between 1 and 7. The default is 2. A packet is the network level unit of data transmission. This value sets the maximum number of packets that X.25 can send without receiving an acknowledgement from the destination host. See the comment on Frame Window Size.

On a PDN, you enter the window size set by the administrator. In a point-to-point connection, both hosts must specify the same window size.

Max Packet Size

Enter one of these values: 32, 64, 128 (the default), 256, 512, 1024. This value sets the maximum size, in bytes, for data packets transmitted on this link. If the major use for the link is file transfer, a larger packet size is more efficient.

On a PDN, you enter the maximum set by the administrator. In a point-to-point connection, both hosts must specify the same maximum.

Framing Type

Enter HDLC (High-level Data Link Control, the default) or BSC (Byte Synchronous Control). HDLC is for bit-synchronous framing and is compatible with existing BLM or BSI boards. BSC is for byte-synchronous framing and is compatible with existing SLM or CSI boards.

On a PDN, you enter the framing type set by the administrator. In a point-to-point connection, both hosts must specify the same framing type.

If you answer HDLC, NETGEN also asks about HDLC encoding and full- or half-duplex. If you answer BSC, NETGEN does not ask these questions.

HDLC Encoding

Enter NRZ (nonreturn to zero, direct encoding) or NRZI (nonreturn to zero, inverted encoding). The parameter sets the method of representing zeros and ones. The default is NRZ. Certain kinds of modems require NRZI.

NETGEN asks this question only if you entered HDLC for Framing Type.

On a PDN, you enter the encoding type set by the administrator. In a point-to-point connection, both hosts must specify the same encoding type.

Note that even if a modem requires NRZI, it cannot extract clock values from the data stream. This parameter sets only the encoding type, not the clock rate.

Clocking

If you will use a modem or external clock, enter EXTERNAL (the default). If you want to generate clock signals from the board, enter INTERNAL; NETGEN asks the following question:

Internal Clock Rate

Enter one of these values: 300, 600, 1200, 2400, 4800, 9600 (the default), 19.2K, 38.4K. This value is the clock rate, in bits per second. (The K indicates kilobits per second.)

If you have configured both MCP1 lines for HDLC framing, the total clock rate must not exceed 38.4 kilobits per second.

If you have configured both MCP1 lines for BSC framing, the total clock rate must not exceed 19.2 kilobits per second.

FULL or HALF duplex

Enter FULL (the default) or HALF, based on the kind of modem you are using. NETGEN asks this question only if you entered HDLC for Framing Type.

On a PDN, you enter the duplex type set by the administrator. In a point-to-point connection, both hosts must specify the same duplex type.

 # PVC's

Enter a value, between 0 (the default) and 250, for the number of permanent virtual connections (PVCs) you want.

On a PDN, you enter the number set by the administrator. In a point-to-point connection, both hosts must specify the same number of PVCs.

If you specify one or more PVCs, NETGEN asks the following question:

Start PVC # :

NETGEN begins numbering PVCs at this value, which must be between 1 (the default) and 4095. On a PDN, you enter the number reserved for your host's PVCs. In a point-to-point connection, both hosts must specify the same starting number.

If you specify one or more PVCs, NETGEN also requests the following information:

	PVC name	Assign a PVC name (1 to 16 AOS filename characters).
	Host Address	Enter the address of the remote host to which this PVC is to be connected.
	PVC ACL	Enter the ACL for the PVC file. The default is + RE. The ACL controls what local users can use the PVC.
# SVC's		Enter a value, between 0 (the default) and 512, for the number of concurrent switched virtual connections (SVCs) you want to permit. On a PDN, you enter the number set by the administrator. In a point-to-point connection, both hosts must specify the same number of SVCs. If you specify one or more SVCs, NETGEN asks the following question: *Start SVC # :* NETGEN begins numbering SVCs at this value, which must be between the highest PVC number plus 1 (the default) and 4095. On a PDN, you enter the number reserved for your host's SVCs. In a point-to-point connection, both hosts must specify the same starting number.

Configuring an MCP1 Path to a Remote Host

After you have configured an MCP1 link, you can use it as a path to a remote host. Add the remote host, as described under "Configuring Remote Hosts" in Chapter 4. When you reach the question about paths, NETGEN requests the following information:

Path Information	Reply Guidelines
Path n	NETGEN displays a path number. Enter the number corresponding to the priority you want to give to the MCP1 path.
Do you wish to configure path(n) for any PMGR switched line?	Enter N (the default).
Link name	Enter the name of the MCP1 link that you have already configured. NETGEN responds by displaying the link type, ISC, and the network type.
Host Address	Enter the address of the remote host.

Multiprocessor Communications Adapter (MCA)

A Multiprocessor Communications Adapter (MCA) is a Data General proprietary local area network that supports up to 15 hosts.

You can also use the NETGEN screens for an MCA to configure a Radial Multiprocessor Communications Subsystem (RMCS). The RMCS uses radial topology, while the MCA uses bus topology, but the two are identical in terms of NETGEN configuration.

Configuring the MCA Device

From the main NETGEN menu, select option 2, "Manage Device Configurations." Then select option 1, "Add Device Configuration." NETGEN requests the following information:

Device Information	Reply Guidelines
Device Name	Assign a device name (1 to 16 AOS filename characters).
Device Type	Enter MCA.
MCA Device	Enter MCA or MCA1. In SYSGEN, you define each MCA as the primary device (MCA) or as the secondary device (MCA1).

Configuring an MCA Link

After you have configured the MCA device, configure a link on the device. From the main NETGEN menu, select option 3, "Manage Link Configurations." Then select option 1, "Add Link Configuration." NETGEN requests the following information:

Link Information	Reply Guidelines
Link Name	Assign a link name (1 to 16 AOS filename characters).
Device Name	Enter the name of the previously configured MCA device. NETGEN responds by displaying the device type, MCA.
Local Host Address	Enter the address of your host (2 to 15 decimal digits). A central network administrator should provide all host addresses.
Transmit retry count	Enter a value between 0 and 99. The default is 2. The value sets the number of times X.25 should automatically reattempt a failed data transmission. The value 0 means do not retry. Once the link is in use, if you receive frequent error messages that the retry count is exhausted, try doubling the current value and then lowering it until you reach an acceptable performance level. A value that is too high can cause X.25 to keep reattempting an impossible transmission.

Packet Window Size

Enter a value between 1 and 7. The default is 2. A packet is the network level unit of data transmission. This value sets the maximum number of packets that X.25 can send without receiving an acknowledgement from the destination host.

All hosts on the MCA must specify the same window size.

A small window size can slow performance by forcing X.25 to wait for acknowledgements. If the link or remote host is slow, you can improve performance by raising the window size.

Frame Window Size (AOS/VS only)

Enter a value between 1 and 7. The default is 7. A frame is the link level unit of data transmission. This value sets the maximum number of frames that X.25 can send without receiving an acknowledgement from the next host in the route. See the comment on Packet Window Size.

All hosts on the MCA must specify the same window size.

Max Packet Size

Enter one of these values: 32, 64, 128 (the default), 256, 512, 1024. This value sets the maximum size, in bytes, for data packets transmitted on this link. If the major use for the link is file transfer, a larger packet size is more efficient.

All hosts on the MCA must specify the same maximum.

 # PVC's

Enter a value in the following range:

0–64 (AOS)
0–250 (AOS/VS)

The default is 0. This is the number of permanent virtual connections (PVCs) you want.

All hosts on the MCA must specify the same number of PVCs.

If you specify one or more PVCs, NETGEN also requests the following information:

PVC name

Assign a PVC name (1 to 16 AOS filename characters).

Host Address

Enter the address of the remote host to which this PVC is to be connected.

Unit Number

Enter a value between 1 and 15. This number is the station address of the remote host on this MCA.

PVC ACL	Enter the ACL for the PVC file. The ACL is + RE. The ACL controls what local users can use the PVC.
# SVC's	Enter a value in the following range: 0–126 (AOS) 0–512 (AOS/VS) The default is 0. This is the number of concurrent switched virtual connections (SVCs) you want to permit. All hosts on the MCA must specify the same number of SVCs.

Configuring an MCA Path to a Remote Host

After you have configured an MCA link, you can use it as a path to a remote host. Add the remote host, as described under "Configuring Remote Hosts" in Chapter 4. When you reach the question about paths, NETGEN requests the following information:

Path Information	Reply Guidelines
Path n	NETGEN displays a path number. Enter the number corresponding to the priority you want to give to the MCA path.
Do you wish to configure path(n) for any PMGR switched line?	Enter N (the default).
Link name	Enter the name of the MCA link that you have already configured. NETGEN responds by displaying the link type, MCA.
MCA Unit Number	Enter a value between 1 and 15. This number is the station address of the remote host on this link.
Host Address	Enter the address of the remote host.

Network Bus System (NBS)

A Network Bus System (NBS) is a Data General proprietary local area network that can support up to 32 hosts.

Configuring the NBS Device

From the main NETGEN menu, select option 2, "Manage Device Configurations." Then select option 1, "Add Device Configuration." NETGEN requests the following information:

Device Information	Reply Guidelines
Device Name	Assign a device name (1 to 16 AOS filename characters).
Device Type	Enter NBS.
Device code	Enter an octal value in the following range: 1–76 (AOS) 1–77 (AOS/VS) The code must be unique among all the devices on your system. The default NBS code is 30. Your field engineer may provide a different value.

Configuring an NBS Link

After you have configured the NBS device, configure a link on the device. From the main NETGEN menu, select option 3, "Manage Link Configurations." Then select option 1, "Add Link Configuration." NETGEN requests the following information:

Link Information	Reply Guidelines
Link Name	Assign a link name (1 to 16 AOS filename characters).
Device Name	Enter the name of the previously configured NBS device. NETGEN responds by displaying the device type, NBS.
Local Host Address	Enter the address of your host (2 to 15 decimal digits). A central network administrator should provide all host addresses.
Transmit retry count	Enter a value between 0 and 99. The default is 2. The value sets the number of times X.25 should automatically reattempt a failed data transmission. The value 0 means do not retry. Once the link is in use, if you receive frequent error messages that the retry count is exhausted, try doubling the current value and then lowering it until you reach an acceptable performance level. A value that is too high can cause X.25 to keep reattempting an impossible transmission.

 # PVC's

Enter a value in the following range:

0–64 (AOS)
0–250 (AOS/VS)

The default is 0. This is the number of permanent virtual connections (PVCs) you want.

All hosts on an NBS must specify the same number of PVCs.

If you specify one or more PVCs, NETGEN also requests the following information:

PVC name	Assign a PVC name (1 to 16 AOS filename characters).
Host Address	Enter the address of the remote host to which this PVC is to be connected.
Unit Number	Enter a value between 1 and 32. This number is the station address of the remote host on this NBS link.
PVC ACL	Enter the ACL for the PVC file. The default is + RE. The ACL controls what local users can use the PVC.

 # SVC's

Enter a value in the following range:

0–126 (AOS)
0–512 (AOS/VS)

The default is 0. This is the number of concurrent switched virtual connections (SVCs) you want to permit.

All hosts on an NBS must specify the same number of SVCs.

Configuring an NBS Path to a Remote Host

After you have configured an NBS link, you can use it as a path to a remote host. Add the remote host, as described under "Configuring Remote Hosts" in Chapter 4. When you reach the question about paths, NETGEN requests the following information:

Path Information	Reply Guidelines
Path n	NETGEN displays a path number. Enter the number corresponding to the priority you want to give to the NBS path.
Do you wish to configure path(n) for any PMGR switched line?	Enter N (the default).
Link name	Enter the name of the NBS link that you have already configured. NETGEN responds by displaying the link type, NBS.
NBS Unit Number	Enter a value between 1 and 32. This number is the station address of the remote host on this link.
Host Address	Enter the address of the remote host.

SNA Backbone (AOS/VS only)

SNA Backbone provides XODIAC services over an SNA network. SNA is IBM's Systems Network Architecture. SNA Backbone works in conjunction with DG/SNA to allow XTS to run over the SNA network. This section presents an overview of SNA Backbone and then describes how to use NETGEN to configure a link.

This discussion assumes a familiarity with SNA and DG/SNA. See the *DG/SNA Reference Manual* (093-000282), the *DG/SNA Operator's Guide* (093-000283), and the DG/SNA Release Notice.

Overview

The Data General hosts that use SNA Backbone are connected to the SNA network by SDLC links. The links are connected to an IBM 37x5 front-end controller that is running IBM's Network Routing Facility (NRF). Figure 5-1 shows a simplified version of the SNA network.

All connections are through the NRF. When two Data General hosts want to communicate over the SNA network, each maintains its own LU-LU session with the NRF. The NRF routes packets from one session to the other. The two LU-LU sessions function as a single XTS virtual connection.

The NRF performs routing by referring to a table of all LUs on its network. Each LU is assigned an index entry into the table. The NRF maintains the mapping between the index entry and the actual location of the LU.

An SNA Backbone link is an LU and has an NRF table index entry. When you use NETGEN to configure an SNA Backbone link for your host, you specify the index entry for the link. This value effectively identifies your host, since the SNA Backbone link is the path to your host. When you configure a path to a remote host, you specify the index entry that has been assigned to the remote host's SNA Backbone link; again, this value effectively identifies the remote host.

When a user wants to call the remote host, he or she uses the host name, not the index entry. For example, in Figure 5-1, a user on HOSTA enters the UVTA command CALL HOSTB. XODIAC maintains the mapping between the host name and the NRF table index entry. In turn, NRF maintains the mapping between the index entry and the location of the remote host on the SNA network.

To X.25, the SNA network appears like any other link-level service. In this way, the SNA network is invisible to the XODIAC or X.25 user. When the SNA Backbone link is enabled, the XTS process connects to the DG/SNA process as a customer. The DG/SNA process must therefore be initialized and running before the SNA Backbone link is enabled.

To keep its interface consistent, NETGEN requires you to define SNA Backbone first as a device, then as a link, and finally as a path to a remote host:

Device — Use the Add Device Configuration screen to identify your local DG/SNA process as a controller. DG/SNA appears as a device to NETGEN because, like actual controllers, it mediates between XTS and the physical communications line. When you configure the SNA Backbone device, you also specify the NRF table index entry for your host's link.

Link — Use the Add Link Configuration screen to provide additional information that the NRF needs. As with other links, you also specify the number of SVCs and PVCs you want.

Remote host — Use the Add Remote Host Configuration screen to identify the remote Data General host. You specify the SNA Backbone link to be used as the path to the host. You also specify the NRF table index entry for the remote host's link.

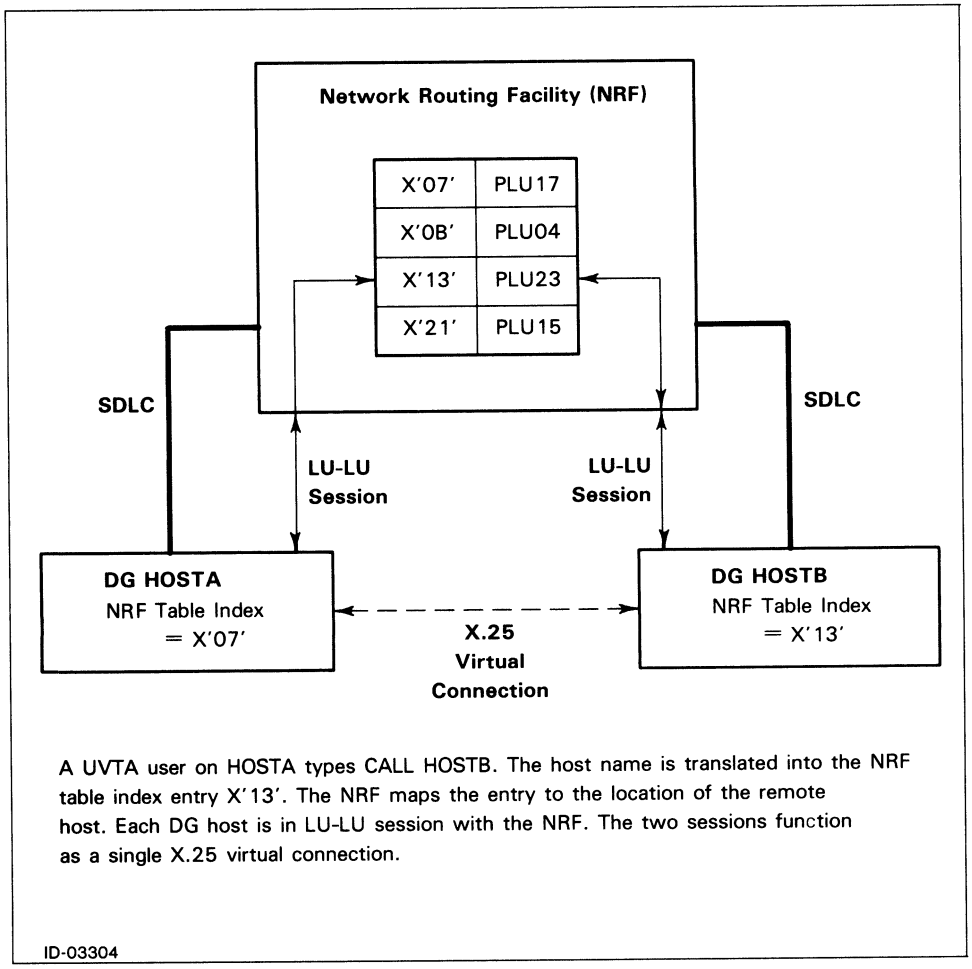


Figure 5-1. SNA Backbone Configuration

The NETGEN values that you enter for an SNA Backbone link should come from a central administrator for the Data General hosts on the SNA network. These values must be consistent across the network and must be understood by the NRF. The IBM administrator provides certain values to the DG administrator, who in turn provides them to each DG system manager. The values are as follows:

- *NRF table index entries.* The IBM administrator assigns a set of entries to the DG administrator. The DG administrator assigns one entry to each SNA Backbone link that is to be configured on the DG hosts. The system managers of each DG host must know what index entry or entries have been assigned to the other remote DG hosts, since NETGEN requires this information in its configuration of remote hosts. Each index entry is a hexadecimal value between 0 and FFFF.

- *Destination primary logical unit identifier.* The NRF requires this PLU for its internal mapping. The IBM administrator provides a set of destination PLUs along with the NRF table index entries. The DG administrator assigns one destination PLU to each SNA Backbone link. The PLUs must be unique, but they do not need to be known across the network. You enter the destination PLU that the DG administrator assigns to your link.

- *Log mode table entry name.* The NRF requires a certain bind image to establish a session. It holds these images in a table, where they are identified by entry names. The IBM administrator must construct the proper bind image, as required by SNA Backbone. (For details, see the Release Notice for SNA Backbone.) The DG administrator must have the proper entry name to identify the image. You enter the name that the DG administrator provides.

In addition, you must also know the following information about your local DG/SNA configuration:

- *DG/SNA process name.* This is either the name given as an argument to the DG/SNA START command or the default name. This name must be a valid AOS filename.

- *Logical user group (LUG) configured for SNA Backbone.* A LUG is a DG/SNA concept, and is not part of IBM SNA. A LUG name must be a valid AOS filename. LUGs are defined in the SNAGEN session. The LUG for SNA Backbone must contain LU numbers defined for this use by the NRF. The IBM administrator should provide these numbers to the DG administrator.

With this information, you can configure an SNA Backbone link, as shown in the next sections.

Configuring the DG/SNA Process as a Device

From the main NETGEN menu, select option 2, "Manage Device Configurations." Then select option 1, "Add Device Configuration." NETGEN requests the following information:

Device Information	Reply Guidelines
Device Name	Assign a device name (1 to 16 AOS filename characters).
Device Type	Enter SNA.
Logical Unit Group	Enter the name of the DG/SNA logical unit group (LUG) for SNA Backbone.
SNA Server Name	Enter the name assigned to the DG/SNA process.
Local NRF Table Index	Enter the NRF table index for your local host's SNA Backbone link. The index is a hexadecimal value between 0 and FFFF. The network administrator supplies this value.

Configuring an SNA Backbone Link

After you have configured the SNA device, configure a link on the device. From the main NETGEN menu, select option 3, "Manage Link Configurations." Then select option 1, "Add Link Configuration." NETGEN requests the following information:

Link Information	Reply Guidelines
Link Name	Assign a link name (1 to 16 AOS filename characters).
Device Name	Enter the name of the previously configured SNA device. NETGEN responds by displaying the device type, SNA.
Mode Table Entry Name	Enter a string of up to 8 characters that specifies the mode table entry name. The network administrator supplies this name.
Destination Logical Unit	Enter the name of the destination primary logical unit that corresponds to your host's SNA Backbone link. The network administrator supplies this name, which contains up to 8 characters.
# PVC's	Enter a value, between 0 (the default) and 250, for the number of permanent virtual connections (PVCs) you want. Hosts that communicate over an SNA link must specify the same number of PVCs.

If you specify one or more PVCs, NETGEN also requests the following information:

PVC name	Assign a PVC name (1 to 16 AOS filename characters).
Remote NRF Table Index	Enter the NRF table index for the remote host to which this PVC is to be connected. The network administrator supplies this value.
PVC ACL	Enter the ACL for the PVC file. The default is + RE. The ACL controls what local users can use the PVC.

 # SVC's

Enter a value, between 0 (the default) and 512, for the number of concurrent switched virtual connections (SVCs) you want to permit.

Hosts that communicate over an SNA link must specify the same number of SVCs.

Configuring an SNA Backbone Path to a Remote Host

After you have configured an SNA link, you can use it as a path to a remote host. Add the remote host, as described under "Configuring Remote Hosts" in Chapter 4. When you reach the question about paths, NETGEN requests the following information:

Path Information	Reply Guidelines
Path n	NETGEN displays a path number. Enter the number corresponding to the priority you want to give to the SNA path.
Do you wish to configure path(n) for any PMGR switched line?	Enter N (the default).
Link name	Enter the name of the SNA Backbone link that you have already configured. NETGEN responds by displaying the link type, SNA.
Remote NRF Table Index	Enter the NRF table index for the remote host. The index is a hexadecimal value between 0 and FFFF. The network administrator provides this value.

End of Chapter

Chapter 6
A Sample NETGEN Session

This chapter contains a sample NETGEN session that configures a simple network. The NETGEN session takes place on host HQ. That is, as network manager on HQ, you are defining the relationship of HQ, the local host, to the other hosts in the XODIAC network. The goal is to connect HQ to the other hosts as follows:

- Use a PMGR asynchronous device to connect HQ to remote host DESK0.
- Use another PMGR asynchronous device to connect HQ to a modem that in turn is connected to remote host DESK1.
- Use an Intelligent Local Area Network Controller (ILC) to connect HQ with remote hosts ADMIN and MFG.
- Because the traffic between HQ and ADMIN is heavy, use an Intelligent Synchronous Controller (ISC) as a parallel path between these hosts.

Figure 6-1 shows the desired network. Note that each host has two or three numbers associated with it. These are addresses or identifiers, as follows:

- One decimal digit = the host identifier, assigned by the network administrator
- Four decimal digits = the host address, assigned by the network administrator
- Twelve hexadecimal digits = the station address, assigned by the field engineer

This session is in two parts. The first configures the hosts with three devices: the ILC and the two PMGR asynchronous devices. The second part adds the ISC as the primary path between HQ and ADMIN and therefore demonstrates how to change an existing configuration.

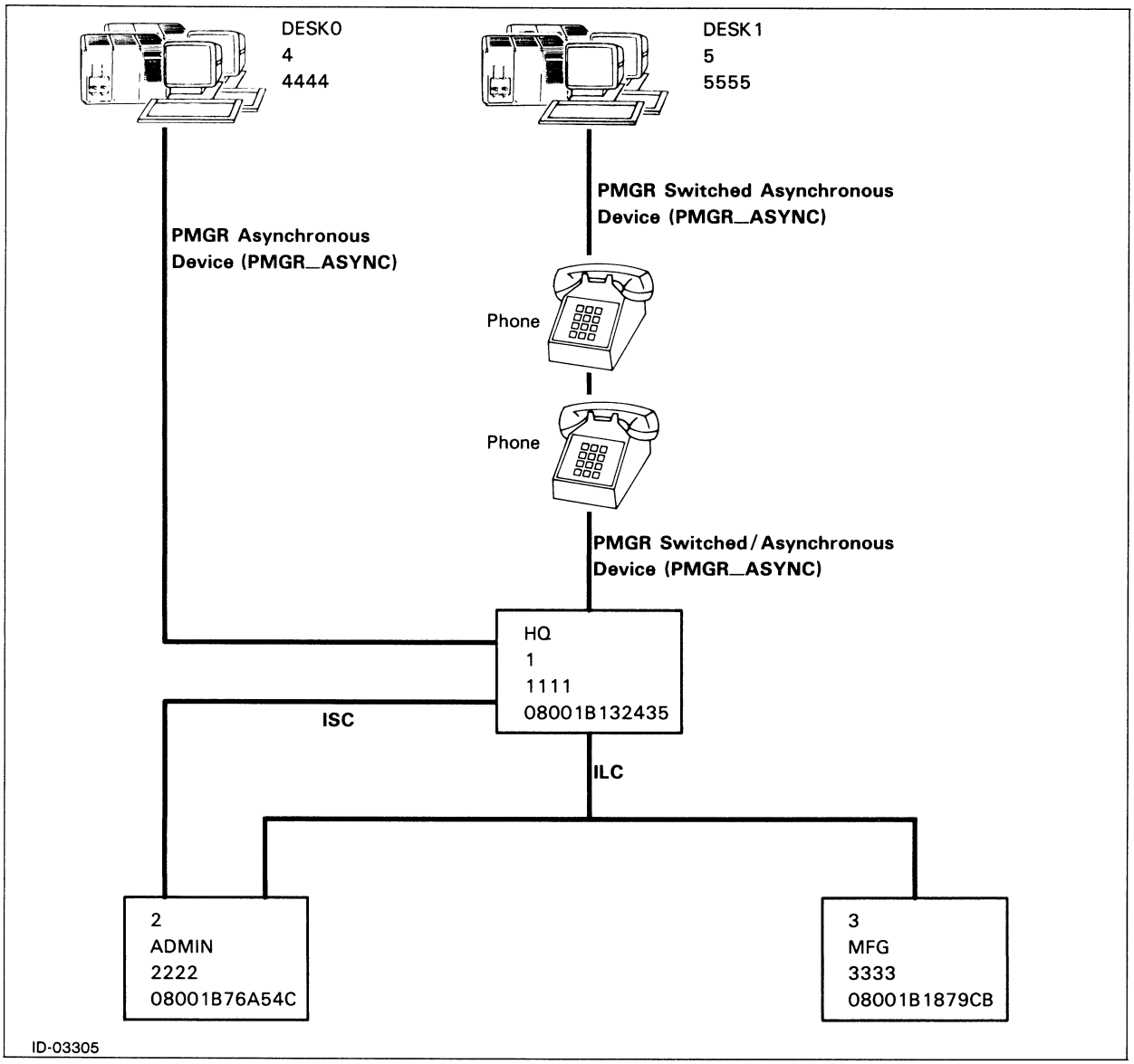


Figure 6-1. A Diagram of Your Network

Beginning the Session

To begin the NETGEN session, execute the NETGEN program. The first NETGEN menu appears, as shown in Figure 6-2. To create a new specification file, enter 1.

```
XODIAC Network Configuration Process -- Rev xx.xx


          T : Terminate Process

          1 : Create New Spec File

          2 : Access/Update Spec File

          3 : Create Configuration Files

    Choose one of the above functions: 1
```

Figure 6-2. Using the First NETGEN Menu

NETGEN asks for the new specification filename. It is useful to make the filenames consistent, for example, by concatenating the host name with the _SPEC suffix:

Enter New Spec File Name : HQ_SPEC ↵

After you press NEW LINE, the main NETGEN menu appears, as shown in Figure 6-3. Configure your network in the order in which the items appear in the menu: local host, devices, links, remote hosts, and NPNs. Because you are creating a new specification, enter a 1 to configure the local host.

```
XODIAC Network Configuration Process -- Rev xx.xx


      P : Pop to Previous Level Screen

      1 : Manage Local Host Configuration

      2 : Manage Device Configurations

      3 : Manage Link Configurations

      4 : Manage Remote Host Configurations

      5 : Manage NPN Configurations

      6 : List Configurations

      7 : Print Configurations

      8 : Merge Operation


Choose one of the above functions : 1
```

Figure 6-3. Using the Main NETGEN Menu

Adding a Local Host

The Change Local Host Info Function screen appears, as shown in Figure 6-4. It requests the host name, the ACL of the local host file, and the host identifier (which is optional, but needed by RMA).

```
XODIAC Network Configuration Process -- Rev xx.xx

Change Local Host Info Function

Note - to leave the current host info unchanged, press only 'new-line'

Local Host Name (an AOS filename):  HQ ↵

ACL (an AOS ACL):  + RE ↵

Host ID (None, 1-32767):  1 ↵
```

Figure 6-4. Dialog for Managing the Local Host

Adding Devices

Once you have configured the local host, you can add the devices to the network. You must configure three devices: an ILC and two PMGR asynchronous devices.

Adding an ILC Device

On the main NETGEN menu (Figure 6-3), choose option 2, Manage Device Configurations. When the screen appears, choose option 1, Add Device Configuration. The Add Device Configuration Menu (Figure 6-5) appears.

To configure an ILC device, provide the name ILC_DCF (the device type plus _DCF, for Device Configuration File). The device type is ILC. To save CPU cycles, you are running X25 on the device rather than on the host. Field Service supplied you with the ILC Station Address of 08001B132435 and the device code of 60. So you answer Y to the question, *Do you wish to specify the ILC Station Address*, and enter the address. You accept the default device code.

```
XODIAC Network Configuration Process -- Add Device Configuration

Device Name :  ILC_DCF ↵

Device Type
(DCU,MCA,NBS,ISC,PMGR_ASYNC,ILAN,ICB,ILC,IBC,SNA,LSC,LLC)
: ILC ↵
Run X25 on this controller:  Y ↵
Do you wish to specify the ILC Station Address(Y/N)?  Y ↵
ILC Station Address in
12 Hexadecimal Digits:  08001B132435 ↵
Device Code (octal)(1-677):  60 ↵
```

Figure 6-5. Dialog for Adding an ILC Device

Adding a PMGR Asynchronous Device (PMGR_ASYNC)

Next, you want to configure the device that supports the connection between HQ and DESK0.

When the Manage Device Configuration menu returns, enter 1 again, to configure another device. NETGEN redisplays the Add Device Configuration menu. This time you enter PMGR_CON9_DCF for the device name and PMGR_ASYNC for the device. You are naming the PMGR asynchronous device for the console number that it represents. NETGEN also prompts you for the maximum number of lines. You plan to have only one line. The relevant fields are as follows:

Device Name : PMGR_CON9_DCF ↵

Device Type
(DCU,MCA,NBS,ISC,PMGR_ASYNC,ILAN,ICB,ILC,IBC,SNA,LSC,LLC)
: PMGR_ASYNC ↵

Maximum Number of Lines (1-50): 1↵

Adding a Second PMGR_ASYNC Device to the Network

The second PMGR asynchronous device connects HQ to the modem. Repeat the process for adding the first PMGR asynchronous device, this time naming the device PMGR_CON2_DCF. The relevant fields are as follows:

Device Name : PMGR_CON2_DCF ↵

Device Type
(DCU,MCA,NBS,ISC,PMGR_ASYNC,ILAN,ICB,ILC,IBC,SNA,LSC,LLC)
: PMGR_ASYNC ↵

Maximum Number of Lines (1-50): 1 ↵

Adding Links

After adding the three devices, you can add the three associated links. Return to the main NETGEN menu, and choose option 3, Manage Link Configurations. When the Link Configuration Menu appears, choose option 1, Add Link Configuration.

Adding an ILC Link

Because you are adding an ILC link, you can call the link ILC_LCF, where LCF stands for Link Configuration File. NETGEN asks you for the name of the device on which you are defining the link. When you enter ILC_DCF, NETGEN checks the previously specified device information and displays the fact that the device type is ILC. It also displays the prompts appropriate to an ILC link, as shown in Figure 6-6.

You are going to use X.25 protocol on this link, so you accept the default Y to the question, *Configure this link for X25.* The network manager assigned the local host address (1111). Since you do not want X.25 to hold up the system

while it continually tries to send data, keep a low retry count. The network manager provides the value of 512 for the maximum packet size and 25 for the number of SVCs; these values must be the same across the LAN. There are no PVCs on this link; consequently, enter 0 for this parameter. You do not use the TCP/IP protocol on your network, so accept the default of N for the prompt.

```
Link Name is :  ILC_LCF ↵

Device Name:  ILC_DCF ↵        Device Type: ILC
Configure this link for X25(Y/N):  Y ↵

Local Host Address (2-15 decimal digits):  1111 ↵

Transmit retry count (0-99) :  4 ↵
Maximum Packet Size (512, 1024) :  512 ↵

# of PVC's :  0 ↵
# of SVC's :  25 ↵
Configure this link for TCP/IP(Y/N): N ↵
```

Figure 6-6. Adding an ILC Link

Adding PMGR Asynchronous Links

Next, you want to configure the PMGR asynchronous links for DESK0 and DESK1. After adding the ILC link, you return to the Manage Link Configuration Menu. Choose option 1 again, "Add Link Configuration." Enter the name of the link, PMGR_CON9_LCF and the device name, PMGR_CON9_DCF. Then enter the information as shown in Figure 6-7. The remote DESKTOP GENERATION host uses XODIAC PREGEN, which selects certain values by default. You must enter matching or complementary values. Because the line will be dedicated, not switched, the maximum packet size must be 512 (the default). The number of PVCs must be zero, and the number of SVCs must be 10. The MV/Family host must take the DCE role, because XODIAC PREGEN chooses the DTE role for the DESKTOP GENERATION host.

```
Link Name is :  PMGR_CON9_LCF ↵

Device Name:  PMGR_CON9_DCF ↵          Device Type: PMGR_ASYNC

PMGR Console Number (2-258):  9 ↵
Local Host address (21-15 decimal digits):  1111 ↵

Transmit timeout (5,2-180):  5 ↵
Max Packet Size (128,512):  512 ↵
DTE or DCE:  DCE ↵

# of PVC's :  0 ↵
# of SVC's :  25 ↵
```

Figure 6-7. Dialog for Adding a PMGR_ASYNC Link

The second PMGR asynchronous link connects HQ to a modem. This time use the name PMGR_CON2_LCF. Figure 6-8 shows how to enter the data into

this menu. As with the first PMGR_ASYNC link, the values you enter must be consistent with the XODIAC PREGEN values. The values are the same as for the first link, except for maximum packet size. Because this line will be switched, not dedicated, the maximum packet size must be 128.

```
Link Name is :  PMGR_CON2_LCF ↓

Device Name:  PMGR_CON2_DCF ↓          Device Type: PMGR_ASYNC

PMGR Console Number (2-258):  2 ↓
Local Host address (21-15 decimal digits):  1111 ↓

Transmit timeout (5,2-180):  5 ↓
Max Packet Size (128,512):  128 ↓
DTE or DCE:  DCE ↓

# of PVC's :  0 ↓
# of SVC's :  10 ↓
```

Figure 6-8. Dialog for Adding Another PMGR_ASYNC Link

Adding Remote Hosts

You now add the remote hosts. Return to the main NETGEN menu, and select option 4, Manage Remote Host Configuration. Then choose option 1, Add Remote Host Configuration.

NETGEN then asks you for the name of the remote host. When you enter the name, and press NEW LINE, AOS/VS NETGEN displays the following prompts (AOS does not have these prompts):

Use X25 transport (Y/N):
Use TCP/IP transport (Y/N):

Accept the default Y for the first question, because XODIAC uses the X.25 protocol. If your system uses the Internet protocol as well, answer Y to the second question. Otherwise, answer N. When you press NEW LINE again, NETGEN displays the second part of the Remote Host Configuration menu.

Note that the following sections omit the questions about X.25 and TCP/IP transport.

Adding Remote Hosts on the PMGR_ASYNC Links

The first remote host that you want to add is DESK0. Reply to the prompts as shown in Figure 6-9. Because you have only one link from HQ to DESK0, you accept the default of 1 for path number. The prompt, *Do you wish to configure path(1) for any PMGR switched line,* is for modem connections. You are not going to connect DESK0 to a modem, so you accept the default of N. You then enter the name of the link that connects your local host to this remote host. NETGEN then asks for the address of the remote host.

```
XODIAC Network Configuration Process -- Add Remote Host Configuration

Remote Host Filename is      : DESK0 ⤵
Remote Host Name is          : DESK0 ⤵
Host ID (None, 1-32767)      : 4 ⤵      Hostfile ACL (an AOS ACL) :  + RE ⤵

Path Number :  1 ⤵

Do you wish to configure path(1) for any PMGR switched line (Y or N)  : N ⤵
Link Name:  PMGR_CON9_LCF ⤵


Host Address (2-15 decimal digits):  4444 ⤵
```

Figure 6-9. Adding a Remote Host on a PMGR_ASYNC Link

Next, you want to configure DESK1 for use with a modem. Your field engineer has already set up the PMGR asynchronous device for modem support. When you return to the Remote Host Configuration menu, choose option 1, Add Remote Host Configuration.

DESK1 requires a modem, so you answer Y to the question about configuring this path for any PMGR switched line. NETGEN does not ask about the link name or host address as it did for DESK0. See Figure 6-10.

```
XODIAC Network Configuration Process -- Add Remote Host Configuration

Remote Host Filename is      : DESK1 ⤵
Remote Host Name is          : DESK1 ⤵
Host ID (None, 1-32767)      : 5 ⤵      Hostfile ACL (an AOS ACL) :  + RE ⤵

Path Number :  1 ⤵


Do you wish to configure path(1) for any PMGR switched line (Y or N) :  Y ⤵


Do you wish to configure another path?  N ⤵
```

Figure 6-10. Adding Another Remote Host on a PMGR_ASYNC Link

Adding a Remote Host on an ILC Link

The next thing you want to do is configure the hosts on the ILC link. Two hosts are connected to HQ through the ILC link: ADMIN and MFG. You must add both of these to complete your remote host configuration.

Return to the Remote Host Configuration menu and choose option 1, Add Remote Host. You use this screen twice, as shown in Figure 6-11 (for MFG) and Figure 6-12 (for ADMIN).

Your field engineer can provide the ILC station addresses for MFG and ADMIN.

```
XODIAC Network Configuration Process -- Add Remote Host Configuration

Remote Host Filename is      : MFG ↓
Remote Host Name is          : MFG ↓
Host ID (None, 1-32767)      : 3 ↓      Hostfile ACL (an AOS ACL) :  + RE ↓

Path Number :  1 ↓

Do you wish to configure path(1) for any PMGR switched line (Y or N)  : N ↓
Link Name:  ILC_LCF ↓
Link Type :ILC       ILC Station Address in
                     12 Hexadecimal Digits:  08001B1879CB ↓

Host Address (2-15 decimal digits):  3333 ↓

Do you wish to configure another path?  N ↓
```

Figure 6-11. Adding a Remote Host on an ILC Link

```
XODIAC Network Configuration Process -- Add Remote Host Configuration

Remote Host Filename is      : ADMIN ↓
Remote Host Name is          : ADMIN ↓
Host ID (None, 1-327670      : 2 ↓      Hostfile ACL (an AOS ACL) :  + RE ↓

Path Number :  1 ↓

Do you wish to configure path(1) for any PMGR switched line (Y or N) :  N ↓
Link Name:  ILC_LCF ↓
Link Type : ILC      ILC Station Address in
                     12 Hexadecimal Digits:  08001B76A54C ↓

Host Address (2-15 decimal digits):  2222 ↓

Do you wish to configure another path?  N ↓
```

Figure 6-12. Adding Another Remote Host on an ILC Link

Adding Network Process Names (NPNs)

Now you want to add the NPNs, if any are required, to the configuration. If you need to check the list of NPNs, return to the main NETGEN menu, and choose option 6, List Configurations. Figure 6-13 appears.

```
XODIAC Network Configuration Process -- Rev xx.xx

          P : Pop to Previous Level Screen

          1 : List Devices

          2 : List Links

          3 : List PVC's

          4 : List Remote Hosts

          5 : List NPN's

Choose one of the above functions: 5
```

Figure 6-13. The List Configuration Options Menu

If you choose option 5, List NPNs, the list shown in Figure 6-14 appears.

```
NPN'S CONFIGURED IN SPECFILE HQ__SPEC

                        * User Data Area or
NPN Entry Name            NPN Process Name      Access Control List

FTA                       FTA                    + RE
VTA                       VTA                    + RE
RMA                       RMA                    OP OWARE
RIA                       RIA                    + RE
RDA                       RDA                    + RE
CEO                       CEO                    + RE
CSA                       CSA                    + RE
```

Figure 6-14. The Default NPN Screen

As you look at the list of NPNs, you realize that all the NPNs you need are already preconfigured for you by default. Therefore, you configure no NPNs.

Generating the Network

You have now specified a network. You have not yet generated it. To do so, you return to the main NETGEN menu and select option 3, "Create Configuration Files." NETGEN asks for the name of the specification file. You enter HQ_SPEC. Based on the information you have just entered into the specification file, NETGEN creates the configuration files. You can then bring up the network.

Changing the Network Configuration

We now assume that you want to change your network configuration. Because traffic is heavy between HQ and ADMIN, you want to add an additional line between the two hosts. You install ISC devices on both hosts to configure an ISC link as the primary path between HQ and ADMIN. You must now change the specification file and generate new configuration files.

Execute NETGEN and choose option 2, "Access/Update Spec File," from the main NETGEN menu. NETGEN prompts for the name of the old specification file. Enter HQ_SPEC. It then asks for the name of the new file, giving HQ_SPEC as the default. Accept the default.

To install an ISC, you first configure the new device and then the new link. Finally, you change the existing specification for ADMIN to give the ISC link as the primary path.

To configure the device, choose option 2, Manage Device Configuration, from the main menu. Then choose option 1, Add Device Configuration. Enter the name and device type. NETGEN displays the appropriate questions. Since you want to run X25 on the controller, answer Y to the prompt, *Run X25 on this controller.* See Figure 6-15 for the complete screen.

```
XODIAC Network Configuration Process -- Add Device Configuration


Device Name: ISC_DCF ↵

Device Type
(DCU,MCA,NBS,ISC,PMGR_ASYNC,ILAN,ICB,ILC,IBC,SNA,LSC,LLC)
: ISC ↵
Device Code (octal)(1-76): 25 ↵
Run X25 on this controller(Y/N) : Y ↵
```

Figure 6-15. Adding an ISC Device

Adding a ISC Link

Next you add the ISC link. Choose the Manage Link Configuration menu and then option 1, "Add Link Configuration." Name your link ISC_LCF; enter the device name ISC_DCF. The ISC link screen appears, as shown in Figure 6-16.

Since the ISC link is not connected to a PDN, enter DATA GENERAL as the network type. Specify line #0 for the link. Accept the default values for most parameters but enter 25 for the number of switched virtual connections so that these values will be consistent throughout the network.

```
Link Name is : ISC_LCF ↓

Device Name: ISC_DCF ↓                    Device Type: ISC

Network types: TELENET, DATAPAC, DATA GENERAL, TRANSPAC, UK PSS,
               TYMNET, DDX, KDD, OTHER

Network Type: DATA GENERAL ↓              Line # (0-1) : 0 ↓
Protocol type (LAP, LAPB): LAPB ↓         DTE or DCE: DTE ↓
Local Host Address (2-15 decimal digits)  : 1111 ↓
Sequence Numbering Modulus (8, 128)       : 8 ↓
Connect retry count (0-99): 10 ↓          Transmit retry count (0-99): 10 ↓
Transmit timeout:(-1,0-3600): 3 ↓         Enable timeout: (-1, 0-3600): 3 ↓
Frame Window Size (1-7): 7 ↓              Packet Window Size (1-7): 2 ↓
                  Max Packet Size (32, 64, 128, 256, 512, 1024): 128 ↓

Framing Type (HDLC, BSC)      : HDLC ↓    HDCL Encloding (NRZ, NRZI) : NRZ ↓

Clocking (EXTERNAL, INTERNAL): EXTERNAL ↓

FULL or HALF duplex line      : FULL ↓
  ————————————— Virtual Call Numbering —————————————

# of PVC's : 0 ↓                  # of SVC's: 25 ↓              Start SVC # : 1 ↓
```

Figure 6-16. Adding an ISC Link

Adding an Additional Path to the Remote Host ADMIN

Now you want to configure ADMIN so that you can use the ISC line to communicate with it. Choose the Remote Host Configuration menu and then option 3, "Change Remote Host Configuration." NETGEN asks you for the name of the remote host. When you enter ADMIN and press NEW LINE, NETGEN displays the current values (see Figure 6-17) and asks if you want to change them. Press NEW LINE to accept each current value.

You want to make the ISC link the primary path to ADMIN. Therefore, when NETGEN reaches the field, *Path Number : 1*, press NEW LINE because you want to change the first path. NETGEN asks if you want to delete the path. Answer N. It then asks if you want to insert the path. Answer Y. It then asks whether this is a PMGR switched line. Answer N. Then enter the link name and the address of the remote host. When you have given this information, ISC_LCF becomes the primary path to ADMIN, and ILC_LCF becomes the first parallel path.

```
XODIAC Network Configuration Process -- Change Remote Host Configuration

Remote Host Filename is : ADMIN ↵
Remote Name is          : ADMIN ↵
Host ID (None, 1-32767) : 2 ↵       Hostfile ACL (an AOS ACL) : + RE ↵

Path Number : 1 ↵

    Paths Configured for Remote Host
    Link Name                Link Type     Station Address
        1 : ILC_LCF            ILC           08001B76A54C

Do you wish to delete this path? (Y or N): N ↵
Do you wish to insert this path? (Y or N): Y ↵
Do you with to configure path(1) for any PMGR switched line (Y or N) : N ↵
Link Name : ISC_LCF ↵

Link Type : ISC

Host Address (2-15 decimal digits) : 2222 ↵
Network Type : DATA GENERAL

Do you wish to configure another path? N

Are you sure that you want to make these changes (Y/N): Y ↵
```

Figure 6-17. Adding Another Link to a Remote Host Configuration

Printing the Specification File

To print the specification file, return to the main NETGEN menu and choose option 7, Print Configurations. NETGEN requests your print file name. Accept the default @LPT to queue the file directly to the line printer. If you want to create a disk file, overwrite @LPT with a pathname. For example, to call your file HQ_SPEC.LS, enter this name. To place the file in a directory other than the one in which you are running NETGEN, enter the whole pathname:

Enter Print File Name: :UDD:OP:LISTFILES:HQ_SPEC.LS ↵

Figure 6-18 shows the complete file that NETGEN generates.

```
                        NETWORK SPECIFICATION PRINT FILE



     Specfile: :NET:NETGEN:HQ_SPEC.LS

     Date: 31-Oct-85

     Time: 10:20:24 AM



                    LOCAL HOST CONFIGURATION



Local Host Name : HQ


ACL : + RE

Host ID : 1



                              DEVICE CONFIGURATION



Device Name : ILC_DCF


Device Type
(DCU,MCA,NBS,ISC,PMGR_ASYNC,ILAN,ICB,ILC,IBC,SNA,LSC,LLC)
: ILC

ILC Station Address in
12 Hexadecimal Digits : 08001B132435
Device code : 60
Run X25 on this controller(Y/N): Y
```

Figure 6-18. Specification Print File (continues)

```
                        DEVICE CONFIGURATION



Device Name : PMGR_CON9_DCF


Device Type
(DCU,MCA,NBS,ISC,PMGR_ASYNC,ILAN,ICB,ILC,IBC,SNA,LSC,LLC)
: PMGR_ASYNC

Maximum Number of Lines: 1




                        DEVICE CONFIGURATION



Device Name : PMGR_CON2_DCF


Device Type
(DCU,MCA,NBS,ISC,PMGR_ASYNC,ILAN,ICB,ILC,IBC,SNA,LSC,LLC)
: PMGR_ASYNC

Maximum Number of Lines: 1




                        DEVICE CONFIGURATION



Device Name : ISC_DCF


Device Type
(DCU,MCA,NBS,ISC,PMGR_ASYNC,ILAN,ICB,ILC,IBC,SNA,LSC,LLC)
: ISC
Device code : 25
Run X25 on this controller(Y/N): Y
```

Figure 6-18. Specification Print File (continued)

```
                              LINK CONFIGURATION


Link Name: ILC__LCF                       Device Name: ILC__DCF

                                          Device Type: ILC
Configure this link for X25(Y/N):Y

Local Host Address (2-14 decimal digits) : 1111

Transmit retry count (0-99)  :     4

Max packet size (512,1024)   :     512

# of PVC's :  0
# of SVC's : 25

Configure this link for TCP/IP(Y/N):N




                              LINK CONFIGURATION


Link Name: PMGR__CON9__LCF                Device Name: PMGR__CON9__DCF

                                          Device Type: PMGR__ASYNC

PMGR Console Number (2-258) : 9
Local Host Address (2-14 decimal digits) : 1111

Transmit timeout (5,2-180) :   5
Max. Packet Size (128,512) : 512
DTE or DCE :  DCE

# of PVC's :   0
# of SVC's :  10
```

Figure 6-18. Specification Print File (continued)

```
                              LINK CONFIGURATION

Link Name: PMGR__CON2__LCF                  Device Name: PMGR__CON2__DCF

                                            Device Type: PMGR__ASYNC

PMGR Console Number (2-258) : 2
Local Host Address (2-14 decimal digits) : 1111

Transmit timeout (5,2-180) :   5
Max. Packet Size (128,512) : 128
DTE or DCE :  DCE

# of PVC's :   0
# of SVC's :  10




                              LINK CONFIGURATION

Link Name: ISC__LCF                         Device Name: ISC__DCF


Network Type : DATA GENERAL                 Line # (0-1) : 0
Protocol Type(LAP,LAPB) : LAPB              DTE or DCE : DTE
Local Host Address (2-14 decimal digits) : 1111
Sequence Numbering Modulus (8,128) : 8
Transmit timeout (-1,0-3600) :    3     Enable timeout (-1,0-3600)   :    30
Frame Window Size (1-7)      :    7     Packet Window Size (1-7)     :     2
                          Max Packet Size (32,64,128,256,512,1024) :   128
Framing Type (HDLC,BSC)      : HDLC     HDLC Encoding (NRZ,NRZI)     :   NRZ
Clocking (EXTERNAL,INTERNAL) : EXTERNAL
FULL or HALF duplex line     : FULL

-------------------------- Virtual Call Numbering --------------------------
# PVC'S :   0                           # SVC'S :  25   Start SVC # :    1

------------------------------------------------------------------------------
```

Figure 6-18. Specification Print File (continued)

```
                        REMOTE HOST CONFIGURATION

Remote Host Filename : ADMIN

Link Name : ISC_LCF

Link Type : ISC

Network Type : DATA GENERAL

Host Address : 2222

Host ID : 2

Hostfile ACL: + RE


                        REMOTE HOST CONFIGURATION

Remote Host Filename : DESKO

Link Name : PMGR_CON9_LCF

Link Type : PMGR_ASYNC

Host Address : 4444

Host ID : 4

Hostfile ACL: + RE


                        REMOTE HOST CONFIGURATION

Remote Host Filename : DESK1

Remote Host will use any PMGR Switched line

Host ID : 5

Hostfile ACL: + RE
```

Figure 6-18. Specification Print File (continued)

```
                        REMOTE HOST CONFIGURATION

Remote Host Filename : MFG

Link Name : ILC__LCF

Link Type : ILC                    ILC Station Address in
                                    12 Hexadecimal Digits : 08001B1879CB


Host Address : 3333

Host ID : 3

Hostfile ACL: + RE




                            NPN CONFIGURATION


NPN-type entry name: FTA

Network Process Name: FTA

Access Control List: + RE




                            NPN CONFIGURATION


NPN-type entry name: VTA

Network Process Name: VTA

Access Control List: + RE
```

Figure 6-18. Specification Print File (continues)

```
                                NPN CONFIGURATION


NPN-type entry name: RMA

Network Process Name: RMA

Access Control List: OP OWARE




                                NPN CONFIGURATION


NPN-type entry name: RIA

Network Process Name: RIA

Access Control List: + RE




                                NPN CONFIGURATION


NPN-type entry name: RDA

Network Process Name: RDA

Access Control List: + RE
```

Figure 6-18. Specification Print File (continued)

```
                              NPN CONFIGURATION



NPN-type entry name: CEO

Network Process Name: CEO

Access Control List: + RE

                              NPN CONFIGURATION



NPN-type entry name: CSA

Network Process name: CSA

Access Control List: + RE
```

Figure 6-18. Specification Print File (concluded)

End of Chapter

Chapter 7
Using the XODIAC Routing Analyzer (XRA)

The XODIAC Routing Analyzer (XRA) is an administrative program that helps simplify the process of configuring a large network. If you are a network administrator responsible for a large number of hosts, you can let XRA determine the most efficient route between any two hosts in the network. The use of XRA is optional: it is possible to configure any XODIAC network using only NETGEN. Using XRA in addition to NETGEN, however, can simplify configuration.

You need to use XRA at only one site in the network. At that site, you input information about all the hosts in the network. XRA generates a routing table for the entire network. You then use XRA to extract an individualized table for each host. You ship the table to the host, where the system manager uses NETGEN to incorporate the routing table into the host's network specification file.

Your organization may require a more decentralized network administration. Within the total network, there may be discrete clusters of hosts, each with its own administrator, and each needing only limited access to the other clusters. XRA is flexible enough to support this decentralized organization. Each cluster can have its own XRA program to provide complete routing information among the hosts in the cluster. The administrator for each cluster can also use XRA to extract more limited routing information, which can then be made available to the other clusters in the network. In this way, hosts from one cluster can have access to hosts in other clusters.

This chapter documents XRA by covering these topics:

- XRA network terminology
- general directions for using XRA
- the steps in using XRA
- adding and changing XRA descriptions
- the XRA command dictionary
- a sample session

XRA Network Terminology

The XRA program introduces a few new terms to describe a complete XODIAC network. This section defines the new terminology.

Subnetworks

When defining your network to XRA, you create *subnetworks*. A subnetwork is a physical link that connects a set of hosts: for example, a point-to-point line between two hosts, or a local area network (LAN) or Multiprocessor Communications Adapter (MCA) that connects two or more hosts. Because they are directly connected, these hosts do not need routing to communicate with each other.

The hosts on one subnetwork can communicate with the hosts on another subnetwork if the two subnetworks share a *routing host*. A routing host must be an AOS/VS system running Routing XTS. A routing host can receive a communications packet from a host on one subnetwork and forward it to a host on a different subnetwork. Note that a routing host is part of both subnetworks.

The opposite of a routing host is an *end host*, which can send or receive a packet but cannot forward one. An end host can run AOS or AOS/VS. A routing host can also be an end host, that is, it can also send or receive a packet.

In deciding the most efficient path between any two hosts, XRA considers the number of *hops* between the hosts. A hop is an intermediate routing host and involves travel over that host's subnetwork. XRA tries to minimize the number of hops.

XRA also considers the *cost* of traveling over the hop's subnetwork. When you define the subnetwork to XRA, you assign it a cost, that is, an integer value that XRA uses in computing the cheapest route. Various factors contribute to the cost: for example, physical links have different line speeds, and different subnetworks bear varying levels of traffic. Because of these factors, one route may contain more hops than an alternate route, but may still be preferable because its hops may have far lower costs.

XRA requires you to assign each subnetwork a cost that is an integer between 1 and 10,000, where 1 is the lowest cost. You design your own formula for computing the cost. One simple formula is based on line speed. Let s be the speed of the physical link. The cost is 1/s, because cost varies inversely with line speed. Because the cost must be an integer, you need to derive a constant k such that (1/s) * k is an integer. You want the cost of the fastest line to be 1: (1/s) * k = 1, or k = s. Therefore, the constant multiplier k is the same as the speed of your fastest line.

Service Areas

A network with decentralized authority may have several clusters of hosts, each with its own administrator. In XRA terminology, each cluster is a *service area*. A service area is a set of one or more subnetworks that is controlled by a single XRA program. As the network administrator for this service area (or service area administrator), you provide information on the hosts, links, and subnetworks in your service area, and your XRA program generates the routing table for your area.

Your own service area is known as the *home service area*. From your point of view, every other service area in the network is a *foreign service area*.

XRA lets a host in one service area communicate with a host in a different service area, if the two administrators provide the necessary configuration. Each service area must have one routing host designated as a *gateway*. A gateway is a routing host that can direct packets into a foreign service area. There must be a link between the two gateways.

Each gateway contains a list of hosts in the foreign service area. When a host in the home service area wants to send a packet to a foreign host, the routing table directs the packet to the gateway, which forwards it to the peer gateway in the foreign service area. The foreign service gateway has detailed information for routing the packet to the destination host. In this way, a gateway does not need to know the configuration of the foreign service area. It needs only the list of hosts available through the peer gateway.

As a service area administrator, you use XRA to draw up the list of hosts in your area. You can choose to put only selected hosts on the list. You can also provide different lists to different foreign service areas. In this way, you determine which of your hosts can be reached from each foreign service area: if a host is not on the list you provide to a foreign service area's gateway, then the hosts in that area do not even know that the host exists.

How to Use XRA

This section describes various aspects of using XRA:

- XRA and INFOS II
- the XRA interface
- the files and reports XRA creates
- invoking XRA

XRA and INFOS II

XRA uses INFOS II to manage the information you provide about the network. XRA and INFOS II both run only under AOS/VS.

XRA generates files, described later in this chapter. Some of these files are in the format of INFOS II databases. Note that an INFOS II database is actually a pair of directories. For example, XRA produces a global specification file. You provide a filename, and XRA generates the two INFOS II directories, one named filename and the other named filename.DB. To refer to the specification file, you use the directory filename. You do not refer to the filename.DB directory nor to the INFOS II files contained in either directory.

For a large network, the INFOS II databases can grow to a large size. At certain points in the process of using XRA, you can dump a database to tape and delete the disk copy or simply delete the database without dumping it. This section describes the steps in using XRA. These descriptions clearly state when it is safe to dump a database and when you can delete it completely. For utilities that dump and load INFOS II databases, see the *AOS/VS INFOS II® System User's Manual.*

The XRA Interface

The XRA user interface is a series of menus. The first menu offers a selection of one-letter commands. For example, select A to add an item to the network specification file or G to generate the routing table. You type the command and press NEW LINE.

XRA then asks questions that prompt for further information. The question may display the valid values in parentheses: for example, a list of one-letter codes and their meanings, or the valid range for a numeric value. If the question has a default answer, it appears in square brackets. To accept the default, press NEW LINE. Otherwise, enter the value you want and then press NEW LINE.

If you enter an invalid value in response to an XRA question, XRA continues to redisplay the question until you enter a valid value. In most cases, XRA also displays a message indicating why the value is invalid.

While answering a set of questions about a single item, you can cancel your current responses by pressing CTRL-C CTRL-A. This control character sequence returns you to the XRA prompt that asks you to enter a command.

XRA offers on-line help messages. Use the XRA command H to get help. H without an argument displays a general description of XRA. H with a command as an argument displays the meaning of the command.

XRA Files and Reports

XRA takes as input the information that you provide about the network. As output, it generates a series of files. These files are for use by the XODIAC software in routing packets between hosts. The files are

- the global specification file
- the service area information files
- the routing table
- the local view specification files

This section describes these files.

The *global specification file* contains the information you provide to XRA about the network. When you first execute XRA, it asks for the name of the global specification file, and creates the file as an INFOS II database (that is, two directories, one named global-spec-filename and the other global-spec-filename.DB). As you use the A command to add the description of new items, XRA adds the items to the global specification file.

The *service area information files* contain the name of a service area and a list of hosts in the area. As a service area administrator, you use the E command to extract a service area information file from your global specification file. You can then exchange files with administrators from other service areas. When you add a gateway to your global specification file, you can include the file for the foreign service area to which the gateway is connected. The default name for a service area information file is global-spec-filename.SAIF.

Use of the service area information files is optional. You can use the A command to add information about each foreign host individually. The service area information files let you add this information in a single step: when you add a gateway, you can give a single filename, instead of adding each host one at a time.

The *routing table* is generated by XRA to provide routing information to the XODIAC software. Once you have a complete global specification file, use the G command to generate the routing table. The routing table is an INFOS II database, with one directory named global-spec-filename.RT and the other named global-spec-filename.RT.DB.

The routing table contains routing information for the entire service area. Each host needs an individualized version of this information. To provide this information, you use the E command to extract a separate *local view specification file* for each host in your service area. You supply the host name, and XRA extracts a file tailored to that host, with the filename hostname.LVS. You send the file to the host's system manager, who uses the Merge option of NETGEN to merge the information with a basic version of the host's network specification file. The basic file contains no information about remote hosts. The information comes from the local view specification file that XRA has generated. If all hosts use the centrally supplied files, all hosts are guaranteed to be using the same routing information.

The files that XRA produces are not printable. They are intended to be read only by the XODIAC software. To get printable reports, use the W command. This command can produce printable reports from the global specification file (named global-spec-filename.LS) and the routing table (named global-spec-filename.RT.LS).

Invoking XRA

To invoke XRA, use this format line:

XEQ XRA*[/G] [global-spec-filename]*

The global specification filename is the name of the file that you want to create or change. You must supply a filename, not a pathname. Therefore, if the file already exists, it must be in the directory in which you initially execute XRA. If you omit the filename, XRA prompts you for it.

If the file you specify does not exist, XRA asks for confirmation that you want to create it. If you enter Y, XRA then asks for the name of the home service area. You can supply any valid AOS or AOS/VS filename for the home service area.

The /G switch is equivalent to the G command, which generates the routing table from the global specification file. The switch lets you generate the table in batch mode, rather than in interactive. This option is especially useful if your network is very large, because generating a routing table for a large network can be time-consuming.

Steps for Using XRA

This section gives an overview of the steps involved in using XRA. The first list describes the simpler case of a network that consists of a single home service area, with no foreign service areas. The second list describes a network that includes foreign service areas.

If your network consists of a single home service area, follow these steps:

1. Create a global specification file that describes your network. Execute XRA and supply a name for the global specification file and for your home area. Then use the A command to add new descriptions to the file. A section later in this chapter discusses adding descriptions. You must add the descriptions in this order:

   a. A subnetwork
   b. The hosts on the subnetwork
   c. The link associated with the subnetwork and hosts

   Since there are no foreign service areas, you do not add gateways.

2. Generate the routing table from the global specification file. Use the G command or the /G switch.

3. At this point, you can dump the global specification file to tape. You must save the file, because any future changes to the network are made against this file.

4. Extract the local view specification files from the routing table. Use the E command once for each host in the network.

5. At this point, you can use the F command to delete the routing table. You do not need to dump it to tape, because any changes to the network invalidate the routing table. If you add changes to the global specification file, you must generate a new routing table.

6. Ship the local view specification files to the individual hosts. Each system manager then uses the Merge option of NETGEN to merge the file into the host's network specification file.

If your network contains foreign service areas, you are responsible for defining your home service area and for exchanging information with other service area administrators. Follow these steps:

1. Create a global specification file that describes your network. Execute XRA and supply a name for the global specification file and for your home area. Then use the A command to add new descriptions to the file. A section later in this chapter discusses adding descriptions. You must add the descriptions in this order:

   a. A subnetwork
   b. The hosts on the subnetwork
   c. The link associated with the subnetwork and hosts
   d. Gateways to foreign service areas

In this step, you can add information about each foreign host individually. If you add hosts individually, skip to step 5. If you plan instead to use service area information files, you can add the gateways later; or you can add gateways now, leaving the foreign service area information filenames blank. Follow the next several steps.

2. Extract a service area information file from the global specification file. Use the E command. You can include the names of all your hosts, include only specified hosts, or include all but some specified hosts.
3. Exchange service area information files with other service area administrators.
4. Add the foreign service area information files to your specification file. Use the A command to add a gateway, or use the C command to change an existing gateway description (that is, to add the service area information filename).
5. Generate the routing table from the global specification file. Use the G command or the /G switch.
6. At this point, you can dump the global specification file to tape. You must save the file, because any future changes to the network are made against this file.
7. Extract the local view specification files from the routing table. Use the E command once for each host in the network.
8. At this point, you can use the F command to delete the routing table. You do not need to dump it to tape, because any changes to the network invalidate the routing table. If you add changes to the global specification file, you must generate a new routing table.
9. Ship the local view specification files to the individual hosts. Each system manager then uses the Merge option of NETGEN to merge the file into the host's network specification file.

Adding and Changing XRA Descriptions

This section gives some detail on the questions XRA asks when you are adding or changing a description and offers suggestions on how to answer them. When you enter the A (Add) command, XRA asks whether you want to add a subnetwork, a host, a link, or a gateway. When you enter the C (Change) command, XRA offers the same options, plus the option of changing the home service area information (HSA_INFO). This extra option lets you change the name of your home service area.

XRA always asks you to name the item being added or changed. If a name already exists for the item — for example, if the item has already been named during a NETGEN session, or if a foreign service area manager has already assigned a name — use the existing name, rather than arbitrarily assigning a new name. Hosts, links, and foreign service areas have existing names. The subnetworks in your home service area do not. When you name a subnetwork, it is often useful to derive the name from the associated link. For example, a local area network associated with an ILC device could be LOCAL_ILC_SUB.

Adding or Changing a Subnetwork

When you add or change a subnetwork, XRA requests the following information:

Information	Reply Guidelines
Subnet name	Enter a name for the subnetwork. Each subnetwork name must be unique within the network.
Subnet type	Enter the type of physical device associated with the subnetwork from the list of types displayed: for example, MCA, NBS, or IEEE_802. If the type is not listed, enter O for Other.
Subnet cost	Enter the cost of traveling the subnetwork. The cost must be an integer in the range from 1 to 10000 (ten thousand). The default cost is 1. Cost is discussed earlier under "Subnetworks."
Comment	Enter a comment of up to 80 characters. Give any helpful information that you care to supply. XRA keeps this information as part of the global specification file and displays it when you enter the D command.

Adding or Changing a Host

When you add or change a host, XRA first asks if this is a home service area host. Answer Y if the host is in your home service area. If you answer Y, XRA requests the following information:

Information	Reply Guidelines
Host name	Enter the host's name. The name must be unique throughout the network. If two or more routing hosts could serve equally well as the next hop in a route, XRA chooses the host whose name comes last in alphabetical order. If you want a certain host chosen by default, give it a name beginning with one of the last letters of the alphabet.
Host attribute	Enter R if the host can perform routing. A routing host must run AOS/VS and Routing XTS. Enter E if the host is an end host that cannot perform routing.
Operating system	Enter A if the host runs AOS, and V if it runs AOS/VS.

You can add a foreign host by answering N when XRA asks if the host is in your own service area. Before you can add a foreign host, you must have defined one of your hosts as a gateway to the foreign service area. If you are adding a foreign host, XRA requests the following information:

Information	Reply Guidelines
Host name	Enter the name of the foreign host.
Foreign service area name	Enter the name of the foreign service area that contains the foreign host.

Instead of adding foreign hosts individually, you can use the service area information file supplied by the foreign service area manager. You specify this filename as input when you define the gateway to the foreign service area. See "Adding or Changing a Gateway."

Adding or Changing a Link

Adding a link means adding the information that a host contains a link configuration file (LCF) defining the host's view of the link. You therefore add a link for each LCF file on each host. When you add a link, you specify both a host name and a subnetwork name. In this way, you directly associate a link with a host and a subnetwork, and you indirectly assign a host to a subnetwork. When you add or change a link, XRA requests the following information:

Information	Reply Guidelines
Host name	Enter the name of the host that contains the LCF file defining the link.
Link name	Enter the link name. Use the name already assigned to the LCF file.
Subnetwork name	Enter the name of the subnetwork that you want to associate with this link. You have already associated the subnetwork with a specific kind of physical device. This step therefore associates the link with a physical device.
DTE address	Enter the X.25 address of the host you have specified for this link. Use the address that has been assigned to the host during the NETGEN session.
Station address	Enter the station address. XRA requests a station address only if for certain subnetwork types. If, in defining the subnetwork associated with the link, you assigned a subnetwork type of O (Other), XRA does not request a station address. Otherwise, it does. The station address format depends on the code you entered for the subnetwork type: Code Format M 1 to 15 digits N 1 to 32 digits I 12 hexadecimal digits Your field engineer can supply the station address.

Adding or Changing a Gateway

Adding a gateway means defining an existing host as a gateway to a foreign service area. Before adding a gateway, you must have defined the host and the link to the foreign service area.

If you are using a service area information file to define the remote hosts, the file must already exist when you specify the filename. You can leave the filename blank when initially defining a gateway and later use the C (Change) command to specify a file. At the point that you specify a service area information file, XRA actually adds the foreign host names to your global specification file.

When you add or change a gateway, XRA requests the following information:

Information	Reply Guidelines
Foreign service area name	Enter the name of the foreign service area to which this gateway is connected.
Host name of home service area gateway	Enter the name of the host in your home service area that is to be the gateway to the foreign service area. You must already have defined this host with the R (Routing) attribute.
Link name on the gateway host	Enter the link name that connects your gateway host to the foreign service area's gateway host. You must already have defined this link and associated it with the gateway host.
DTE address of the foreign service area gateway host	Enter the X.25 address of the foreign service area gateway host. The manager of the foreign service area or public data network can supply this address.
Station address	Enter the station address. See the guidelines for the station address under "Adding or Changing a Link." Those guidelines also apply here.
Filename of Foreign Service Area Information File	Enter the filename of the service area information file supplied by the foreign service area manager. You must supply a filename, not a pathname. The file must therefore be in the directory in which you executed XRA. The service area information file contains the name of the foreign service area, specified in response to a question from the E command that extracted the file. The name you have specified for the foreign service area must match the name in the file. Otherwise, XRA issues a warning.

The XRA Command Dictionary

The XRA commands are one letter long. If you type more than one letter, XRA repeats its prompt until you enter a single letter. Table 7-1 gives the XRA commands and their functions.

Table 7-1. The XRA Commands and Their Functions

Command	Function
A	Adds an entry to the global specification file.
B	Terminates the XRA program (stands for BYE).
C	Changes an entry in the global specification file.
D	Displays an entry in the global specification file.
E	Extracts a service area information file or a local view specification file.
F	Deletes the current routing table.
G	Generates the routing table.
H	Displays on-line help information.
L	Lists entries from the global specification file.
R	Removes an entry from the global specification file.
S	Saves updates made to the global specification file.
W	Writes a printable report file to disk.

The following pages present a detailed description of XRA commands in alphabetical order.

A

Adds an entry to your global specification file.

Description

The A command adds an entry to the global specification file. You can add a subnetwork, host, link, or gateway. When you enter A, XRA asks the type of entry to be added. Based on your reply, it asks for further information. See the earlier section on "Adding and Changing XRA Descriptions" for a list of the questions XRA asks and for suggestions on answering them. If a question has a default answer, XRA displays it in brackets. You accept the default by pressing NEW LINE.

When you have added the information for an entry, XRA asks if you want to add another entry of the same type. The default is N.

Note these points on the order of adding entries:

- Before adding a gateway, you must already have added the associated host and link.
- Before adding a link, you must already have added the associated host and subnetwork.

The standard order is to add a subnetwork, then the hosts, then the links associated with the subnetwork and the hosts, and finally the gateways.

Example

The following example adds a subnetwork entry to the global specification file:

Enter a command: A ↵
Type of entry to be added (S=subnet, H=host, L=link, G=gateway)[]: S ↵
Subnet name[]: SWITCHED_SUB ↵
Subnet type (M=MCA, N=NBS, I=IEEE_802, O=other)[]: O ↵
Subnet cost [1]: ↵
Comment about this subnet []: Modem between DESK1 and HQ. ↵

Do you want to add another subnet [N]: ↵

Because the device type is PMGR_ASYNC, you enter O for Other. You accept the default cost of 1 by pressing NEW LINE without entering a value.

B

Terminates the XRA program.

Description

The B command terminates the XRA program. When you enter B, any changes you have made during this session become a permanent part of the global specification file. You can use this command whenever the XRA command prompt appears.

Example

The following example terminates an XRA session and returns you to the CLI:

```
Enter a command: B ↵
The XODIAC Routing Analyzer is terminating
)
```

C
Changes an entry in the global specification file.

Description

The C command lets you change an entry in the global specification file. You can change an entry any time after you have added it to the global specification file. Changing an entry, however, invalidates any existing routing table. You must generate a new routing table from the updated global specification file.

You can change information about a subnetwork, host, link, or gateway. You can also change the name of the home service area.

Once you select the type of entry, XRA asks questions to identify the entry to be changed: for example, for a gateway, XRA asks for the name of the foreign service area; for a link, it asks for the name of the associated host and subnetwork. Once it has identified the entry, XRA displays each item in the entry. It displays the current value in brackets. To retain the current value, press NEW LINE. To change it, enter the new value and press NEW LINE.

On the questions that XRA asks, see the earlier section on "Adding and Changing XRA Descriptions."

Example

The following example changes a link entry in the global specification file:

```
Enter a command:  C ↵
Type of entry to be changed
(S=subnet,H=host,L=link,G=gateway,I=HSA_info)[]:  L ↵
Host name which contains this link []:  HQ ↵
Link name []:  PMGR_CON2_LCF ↵
Enter new host name [HQ]:  ↵
Enter new link name [PMGR_CON2_LCF]  ↵
Subnet name to which this link is attached [SWITCHED_SUB]  ↵
DTE Address [1111]:  1112 ↵
```

XRA prompts for the host name and link name to identify the link to be changed. It then displays the current values. You press NEW LINE to retain the current value. You change the DTE address from 1111 to 1112.

D

Displays an entry in the global specification file.

Description

The D command displays information from the global specification file about a subnetwork, host, link, or gateway. You can display information from the file any time after you have entered it.

The D command displays information about a single entry, which you identify in response to XRA's questions. Use the L command to display the names of all entries of a certain type.

Examples

The following example displays information about a link:

```
Enter a command:  D ↵
Type of entry to be displayed
(S=subnet,H=host,L=link,G=gateway,I=HSA_info)    []:  L ↵
Host name which contains this link []:  HQ ↵
Link name []:  ISC_LCF ↵

Subnet name, to which this link is attached  :  HQ_SUB
DTE address                                  :  1111

Do you want to display another link [N]:  ↵
```

Once you identify the link and the host that contains the LCF file for the link, XRA displays the rest of the information.

E

Extracts a local view specification file or a service area information file.

Description

The E command extracts either a local view specification file or a service area information file. For an explanation of these files, see "XRA Files and Reports" earlier in this chapter.

XRA extracts the local view specification file from the routing table. It extracts the service area information file from the global specification file.

When you enter the E command, XRA asks what kind of file you want to extract. You respond with either V (local view specification file) or I (service area information file). Depending on your response, XRA then prompts for further specifications about the information you want extracted.

If you enter V (extract a local view specification file), XRA asks for the following information:

1. *Enter a host name (+ for all hosts)*

   Enter the name of the host for which you want to extract a local view specification file. Enter a plus sign (+) if you want to extract files for all host in your home service area. If you enter +, XRA creates a file for each host, naming each file hostname.LVS.

2. *Do you want expanded routing information?*

   Expanded routing information concerns hosts in foreign services areas. By default, XRA includes information about all foreign service areas. If you answer Y, XRA lets you specify which foreign service areas you want to include in this local view specification file. The host receiving this file has access only to the foreign service areas that you have included.

   Type of expanded routing information desired (A=all, E=excluded, D=designated)

   If you want to include all foreign service areas, answer A. (Note that A is equivalent to answering N to the previous question.) If you want all except for certain ones that are to be excluded, answer E. If you want to designate the ones to include, answer D. If you answer E or D, XRA asks you to enter the name of a service area to be excluded (E) or included (D) and then asks if you want to specify another service area.

3. *Enter the name for the local view specification file*

   The default name is hostname.LVS. You can enter a different name here. If you answered the first question with + (extract files for all hosts), XRA does not ask this question but instead uses the default for each file.

E (continued)

If you enter I (extract a service area information file), XRA asks for the following information:

1. *Enter the name of this service area*

   Enter the name of your home service area. This name is stored in the extracted file. When the manager of the foreign service area adds a gateway to your service area, the name he or she assigns your area must match the name you enter here. Otherwise XRA returns a warning message.

2. *Type of information desired (A=all, E=excluded, D=designated)*

   If you want to include all your hosts in this file, answer A. If you want all except for certain ones that are to be excluded, , answer E. If you want to designate the ones to include, answer D. If you answer E or D, XRA asks you to enter the name of a host to be excluded (E) or included (D), and then asks if you want to specify another host.

   This option lets you control which of your hosts can be accessed from the foreign service area that receives this extracted file.

3. *Enter the name for this service area information file*

   The default name is spec-filename.SAIF, where spec-filename is the name of the global specification file from which you are extracting this information. You can enter a different name here.

Examples

The following example tells XRA to create local view specification files for all hosts in the home service area and to include expanded routing information for all but one specified foreign service area:

```
Enter a command:  E ↵
Type of file to be extracted
   (V=local view specification file, I=service area information file) [V]:  V ↵
Enter host name ('+' for all hosts) []:  + ↵
Do you want expanded routing information [N]:  Y ↵
Type of expanded routing information desired
(A=all, E=excluded, D=designated) [A]:  E ↵
Enter a service area name []:  TXS ↵
Do you want to specify another service area [N]:  ↵
```

The next example tells XRA to create a service area information file containing only the local hosts HQ and ADMIN:

Enter a command: **E** ⤸
Type of file to be extracted
(V=Local View Specfile, I=Service Area Information File) [V]: **I** ⤸
Type of information desired (A=all, E=excluded, D=designated) [A]: **D** ⤸
Enter a host name []: **HQ** ⤸

Do you want to specify another host name [N]: **Y** ⤸
Enter a host name []: **ADMIN** ⤸
Do you want to specify another host name [N]: ⤸
Enter the name for the service area information file [BOS.SAIF]: ⤸

The filename is the default, that is, the name of the global specification file (BOS) with the .SAIF extension.

F

Deletes the routing table.

Description

The F command deletes the routing table and frees the memory that it used.

Example

The following command deletes the routing table:

Enter a command: F ↵

G
Generates the routing table.

Description

The G command generates the routing table from information in the global specification file. After you have finished creating or changing the global specification file, you can generate the routing table.

XRA names the routing table spec-filename.RT, where spec-filename is the name of the global specification file. If a file with this name already exists, XRA deletes its contents and writes the new routing table information into it.

Example

The following example creates a new routing table:

Enter a command: G ↵
Creating a new Routing Table
The Routing Table is being generated -- please be patient
The Routing Table has been built

L

Lists entries from the global specification file.

Description

The L command lists all entries of the type that you specify from the current global specification file. In some cases, XRA prompts for additional information about the type of entry to be listed. You can list an entry any time after you have added it to the global specification file.

The L command lists all entries of the specified type. Use the D command to display complete information about a single entry.

Example

The following example lists all hosts currently in the global specification file:

```
Enter a command: L ↵
Type of entry to be listed (S=Subnet, H=host, L=link, G=gateway) []: H ↵
Type of hosts to be displayed (A=all, H=home service area
   hosts only, F=foreign service area hosts only) [H]: A ↵
     ---------- Home Service Area Hosts----------
     ADMIN      DESK0      DESK1      HQ
     MFG
     ---------- Foreign Service Area Hosts----------
     MNFT1      MNFT2      WEST
```

After you specify that you want to list the hosts, XRA asks for a further specification — local hosts, foreign hosts, or both — and then lists the names.

R

Removes an entry from the global specification file.

Description

The R command deletes a subnet, host, link, or gateway entry from the global specification file. You can remove an entry from the global specification file at any time after you enter it. Once you remove an entry, the routing table is no longer current. You must use the G command to generate a new routing table.

When you remove a subnetwork or host, XRA automatically removes all links associated with the subnetwork or host.

Examples

The following example removes the gateway to SFO from the global specification file:

Enter a command: R ↵
Type of entry to be removed (S=subnet,H=host,L=link,G=gateway) []: G ↵
Foreign service area name []: SFO ↵

Do you want to remove another gateway [N] ↵

S

Saves updates to the global specification file.

Description

The S command saves all the changes made to the global specification file since you began the current editing session or since you issued the last S command. When you issue an S command, the changes become a permanent part of the file. You can save updates at any point in an XRA session and then continue editing the file.

XRA automatically saves all changes when you terminate the program with the B command.

Example

The following example saves all changes made to this point in the session:

Enter a command: S ↵
The INFOS CHECKPOINT utility is currently executing

W

Writes a printable report file.

Description

The W command generates a printable report from the global specification file or the routing table. You can then use the CLI QPRINT command to print the report.

The printable global specification file is spec-filename.LS, and the printable routing table is spec-filename.RT.LS, where spec-filename is the name of the global specification file. If a file with this name already exists, XRA deletes the information in the existing file before it writes the new information.

Examples

The following example asks XRA to write printable versions of both the global specification file and the routing table:

Enter a command: W ↵
Write report for global specification file (G), Routing Table (R), or both (B) [G]: B ↵

Sample XRA Session

This section contains a sample network and the XRA session that describes the network. Figure 7-1 shows the sample network.

The network contains two service areas, BOS and SFO, which can communicate over a public data network. The following discussion takes the point-of-view of BOS, so BOS is the home service area and SFO the foreign service area. All configuration details of the home service area are shown. For the foreign service area, the only details shown are the host names and the DTE address of the gateway host. This is the only knowledge about a foreign service area that XRA requires.

The labels in the figure are the information that XRA requests during the session. The various kinds of information are distinguished as follows:

- The boxes are *hosts*. Each host contains a host name, the type of operating system, whether the host is a routing host (R) or an end host (E), the host's DTE address (4 decimal digits), and for hosts on a LAN the station address (12 hexadecimal digits).
- The lines between hosts are *subnetworks*. Each subnetwork also corresponds to a *link*. The subnetwork names end with _SUB, and the link names end with _LINK. The type of each subnetwork is also shown.

Table 7-2 describes the subnetworks in the home service area.

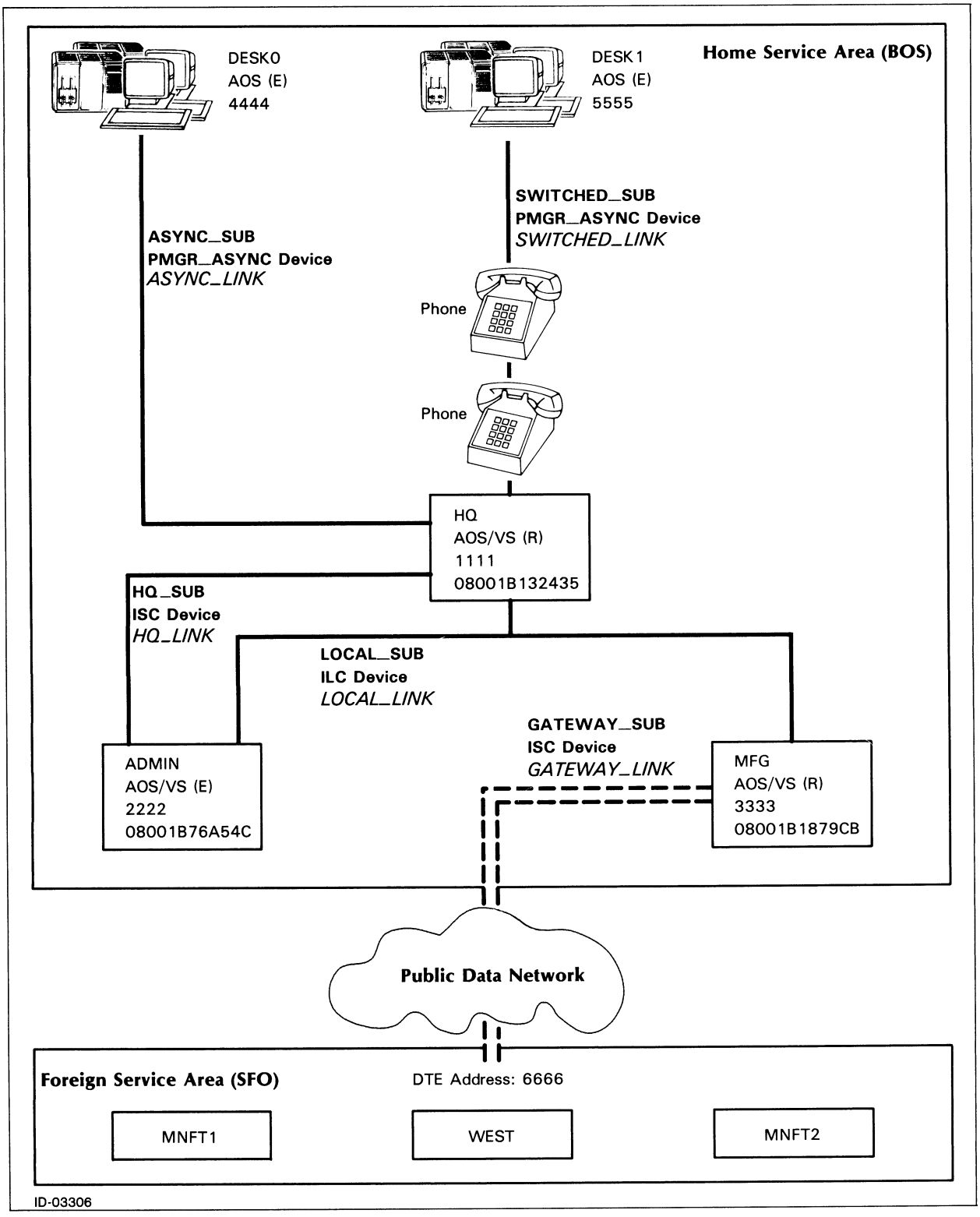


Figure 7-1. Sample Network with XRA Information

Table 7-2. Home Service Area Subnetworks

Subnetwork	Link	Hosts	Comment
ASYNC_SUB	ASYNC_LINK	DESK0 HQ	Two hosts connected by a PMGR asynchronous device.
SWITCHED_SUB	SWITCHED_LINK	DESK1 HQ	Two hosts connected by a phone link on PMGR asynchronous device.
LOCAL_SUB	LOCAL_LINK	HQ ADMIN MFG	Three hosts connected through an ILC device.
HQ_SUB	HQ_LINK	HQ ADMIN	Two hosts connected through an ISC device. Note that HQ and ADMIN are also directly connected on the LOCAL_SUB subnetwork.
GATEWAY_SUB	GATEWAY_LINK	MFG	MFG is the gateway to the SFO foreign service area, by way of an ISC device.

Beginning the XRA Session

Having this information, you can now invoke XRA and request it to create a global specification file:

```
) X XRA NET_SPEC ↵
```

The global spec file specified does not currently exist

Do you want to create a new global spec file[N]: Y ↵

Enter the name of the Home Service Area[]: BOS ↵

Creating a new global spec file.

The INFOS IFILE utility is currently executing.

The new global spec file has been initialized.

The associated Routing Table does not exist.

XODIAC Routing Analyzer - type H for help.

Enter a command:

Adding the XRA Definitions

First you add the subnetworks. The following is the dialog for adding the subnetworks:

Enter a command: A ↵
Type of entry to be added (S=Subnet, H=host, L=link, G=gateway) []: S ↵
Subnet name[]: ASYNC_SUB ↵
Subnet type (M=MCA, N=NBS, I=IEEE_802, O=other)[]: O ↵
Subnet cost [1]: ↵
Comment about this Subnet[]: DESK0 and HQ. ↵

Do you want to add another Subnet [N]: Y ↵
Subnet name[]: SWITCHED_SUB ↵
Subnet type (M=MCA, N=NBS, I=IEEE_802, O=other)[]: O ↵
Subnet cost [1]: ↵
Comment about this Subnet[]: Modem between DESK1 and HQ. ↵

Do you want to add another Subnet [N]: Y ↵
Subnet name[]: HQ_SUB ↵
Subnet type (M=MCA, N=NBS, I=IEEE_802, O=other)[]: O ↵
Subnet cost [1]: ↵
Comment about this Subnet[]: Primary path between HQ and ADMIN. ↵

Do you want to add another Subnet [N]: Y ↵
Subnet name[]: *LOCAL_SUB* ↵
Subnet type (M=MCA, N=NBS, I=IEEE_802, O=other)[]: I ↵
Subnet cost [1]: ↵
Comment about this Subnet[]: ILC between HQ, ADMIN, and MFG. ↵

Do you want to add another Subnet [N]: Y ↵
Subnet name[]: GATEWAY_SUB ↵
Subnet type (M=MCA, N=NBS, I=IEEE_802, O=other)[]: O ↵
Subnet cost [1]: ↵
Comment about this Subnet[]: Gateway between MFG and WEST. ↵

Do you want to add another Subnet [N]: N ↵

Next you add the hosts in your home service area. You do not add the foreign hosts at this point, because you will use a service area information file. The following is the dialog for adding the home service area hosts:

Enter a command: A ↵
Type of entry to be added (S=Subnet, H=host, L=link, G=gateway) []: H ↵
Is this a home service area host [Y]: Y ↵
Host name []: DESK0 ↵
Host attribute (R=Router E=End host) [E]: ↵
Operating System type (A=AOS V=AOS/VS) [V]: A ↵

Do you want to add another home service area host [N]: Y ↵

Host name []: DESK1 ↵
Host attribute (R=Router E=End_host) [E]: ↵
Operating System type (A=AOS V=AOS/VS) [V]: A ↵

Do you want to add another home service area host [N]: Y ↵

Host name []: HQ ↵
Host attribute (R=Router E=End host) [E]: R ↵
Operating System type (A=AOS V=AOS/VS) [V]: V ↵

Do you want to add another home service area host [N]: Y ↵

Host name []: ADMIN ↵
Host attribute (R=Router E=End_host) [E]: ↵
Operating System type (A=AOS V=AOS/VS) [V]: V ↵

Do you want to add another home service area host [N]: Y ↵

Host name []: MFG ↵
Host attribute (R=Router E=End host) [E]: R ↵
Operating System type (A=AOS V=AOS/VS) [V]: V ↵

Do you want to add another home service area host [N]: N ↵

You next add the links. You add a link for each link configuration file (LCF) on each host. For example, link ASYNC_LINK is defined on both DESK0 and HQ, because it connects these two hosts. You therefore add ASYNC_LINK once for DESK0 and again for HQ. The following is the dialog for adding the links:

Enter a command: A ↵
Type of entry to be added (S=Subnet, H=host, L=link, G=gateway) []: L ↵
Host name which contains this link []: DESK0 ↵
Link name []: ASYNC_LINK ↵
Subnet name, to which this link is attached []: ASYNC_SUB ↵
DTE address: 4444 ↵

Do you want to add another link [N] Y ↵
Host name which contains this link [DESK0]: DESK1 ↵
Link name []: SWITCHED_LINK ↵
Subnet name, to which this link is attached []: SWITCHED_SUB ↵
DTE address: 5555 ↵

Do you want to add another link [N] Y ↵
Host name which contains this link [DESK1]: HQ ↵
Link name []: SWITCHED_LINK ↵
Subnet name, to which this link is attached []: SWITCHED_SUB ↵
DTE address: 1111 ↵

Do you want to add another link [N] Y ↵
Host name which contains this link [HQ]: HQ ↵
Link name []: ASYNC_LINK ↵
Subnet name, to which this link is attached []: ASYNC_SUB ↵
DTE address: 1111 ↵

Do you want to add another link [N] Y ↵
Host name which contains this link [HQ]: HQ ↵
Link name []: LOCAL_LINK ↵
Subnet name, to which this link is attached []: LOCAL_SUB ↵
DTE address: 1111 ↵
Station address (12 hexadecimal digits) []: 08001B132435 ↵

Do you want to add another link [N] Y ↵
Host name which contains this link [HQ]: HQ ↵
Link name []: HQ_LINK ↵
Subnet name, to which this link is attached []: HQ_SUB ↵
DTE address: 1111 ↵

Do you want to add another link [N] Y ↵
Host name which contains this link [HQ]: ADMIN ↵
Link name []: HQ_LINK ↵
Subnet name, to which this link is attached []: HQ_SUB ↵
DTE address: 2222 ↵

Do you want to add another link [N] Y ↵
Host name which contains this link [ADMIN]: ↵
Link name []: LOCAL_LINK ↵
Subnet name, to which this link is attached []: LOCAL_SUB ↵
DTE address: 2222 ↵
Station address (12 hexadecimal digits) []: 08001B76A54C ↵

Do you want to add another link [N] Y ↵
Host name which contains this link [ADMIN]: MFG ↵
Link name []: LOCAL_LINK ↵
Subnet name, to which this link is attached []: LOCAL_SUB ↵
DTE address: 3333 ↵
Station address (12 hexadecimal digits) []: 08001B1879CB ↵

Do you want to add another link [N] Y ↵
Host name which contains this link [MFG]: ↵
Link name []: GATEWAY_LINK ↵
Subnet name, to which this link is attached []: GATEWAY_SUB ↵
DTE address: 3333 ↵

Do you want to add another link [N] N ↵

Finally, you add the gateway to the foreign service area. We assume that you have received a service area information file from the manager of the SFO service area. Before defining MFG as a gateway, load the file SFO.SAIF into your working directory. When you give the filename, XRA imports the information into your global specification file. The following is the dialog for adding a gateway:

Enter a command: A ↵
Type of entry to be added (S=Subnet, H=host, L=link, G=gateway) []: G ↵
Foreign service area name []: SFO ↵
Host name of home service area gateway []: MFG ↵
Link name on that host []: GATEWAY_LINK ↵
DTE address of foreign service area gateway []: 6666 ↵
Filename of Foreign service area information file []: SFO.SAIF ↵

Do you want to add another gateway? [N] ↵

Generating the Routing Table

When you have completed adding the information for the global specification file, you can generate the routing table. The dialog for doing so is as follows:

Enter a command: G ↵

Creating a new Routing Table

The Routing Table is being generated ---- please be patient

The Routing Table has been built

Extracting Files

You can now extract the service area information file and the local view specification files.

The following dialog extracts the service area information file from the global specification file. It includes all the hosts in the file except for DESK0 and DESK1. The foreign service areas receiving this file therefore cannot reach these hosts. The dialog is as follows:

Enter a command: E ↵
Type of file to be extracted
(V=local view spec file, I=service area information file) [V]: I ↵
Type of information desired
(A=all, E=excluded, D=designated) [A]: E ↵
Enter a host name []: DESK0 ↵
Do you want to specify another host name [N]: Y ↵
Enter a host name []: DESK1 ↵
Do you want to specify another host name [N]: ↵
Enter the name for the service area information file [BOS.SAIF]: ↵

The following dialog extracts local view specification files for all the hosts in the home service area. It requests expanded routing information. The dialog is as follows:

Enter a command: E ↵
Type of file to be extracted
(V=local view spec file, I=service area information file) [V]: V ↵
Enter host name ('+' for all hosts) []: + ↵
Do you want expanded routing information [N]: Y ↵
Type of expanded routing information desired
(A=all, E=excluded, D=designated) [A]: ↵

Creating Readable Reports

The global specification file and routing table are not readable. To get readable reports, use the W command. The following example creates readable versions of both the global specification file and the routing table:

Enter a command: W ⤸
Write report for global spec file (G), Routing Table (R), or both (B) [G]: B ⤸

Figure 7-2 shows the printable version of the global specification file.

```
The Home Service Area name is: BOS

    Subnet Name        Subnet Cost   Descriptive Comment
    -----------        -----------   -------------------

     ASYNC__SUB                 1    DESKO and HQ.
     GATEWAY__SUB               1    Gateway between MFG and WEST.
     HQ__SUB                    1    Primary path between HQ and ADMIN.
     LOCAL__SUB                 1    ILC between HQ, ADMIN, and MFG.
     SWTCHED__SUB               1    Modem between DESK1 and HQ.


    Host Name:  ADMIN                  This host is an end host
                                       This host is running AOS/VS

    The links on this host are:

    Link Name         attached to Subnet  DTE Address        Station Address
    ---------         ------------------  -----------        ---------------

    HQ__LINK            HQ__SUB           2222

    LOCAL__LINK         LOCAL__SUB        2222               08001B76A54C


*******************************************************************************

    Host Name:  DESKO                  This host is an end host
                                       This host is running AOS

    The links on this host are:

    Link Name         attached to Subnet  DTE Address        Station Address
    ---------         ------------------  -----------        ---------------

    ASYNC__LINK         ASYNC__SUB          4444
```

Figure 7-2. Printable Version of the Global Specification File (continues)

```
*****************************************************************

    Host Name:  DESK1                   This host is an end host
                                        This host is running AOS

    The links on this host are:

    Link Name         attached to Subnet  DTE Address       Station Address
    ---------         ------------------  -----------       ---------------

    SWITCHED__LINK        SWITCHED__SUB       5555


*****************************************************************

    Host Name:  HQ                      This host is a router host
                                        This host is running AOS/VS

    The links on this host are:

    Link Name         attached to Subnet  DTE Address       Station Address
    ---------         ------------------  -----------       ---------------

    ASYNC__LINK         ASYNC__SUB        1111

    HQ__LINK            HQ__SUB           1111

    LOCAL__LINK         LOCAL__SUB        1111              08001B132435

    SWITCHED__LINK      SWITCHED__SUB     1111


*****************************************************************

    Host Name:  MFG                     This host is a router host
                                        This host is running AOS/VS

    The links on this host are:

    Link Name         attached to Subnet  DTE Address       Station Address
    ---------         ------------------  -----------       ---------------

    GATEWAY__LINK     GATEWAY__SUB        3333
    LOCAL__LINK       LOCAL__SUB          3333              08001B1879CB
```

Figure 7-2. Printable Version of the Global Specification File (continued)

```
****************************************************************


    Foreign Service Area  -            Name:  SFO
                                  DTE Address:  3333
                              Station Address:

    Home Service Area     -     Gateway Host:  MFG
                                  using Link:  GATEWAY__SUB__LCF

    The hosts that can be reached in this Service Area are:

    MNFT1             MNFT2             WEST
```

Figure 7-2. Printable Version of the Global Specification File (concluded)

Figure 7-3 shows the printable version of the routing table. For each host, the table gives a path segment list, that is, the route to every other host. It tells the total cost of reaching the destination host (that is, the sum of the costs of each subnetwork between the hosts). It tells the outgoing link to be used to reach the destination host. It also tells the next hop (that is, the next intermediate routing host) in the route to the destination host. To get from the current source host to the destination host, the route goes to the next hop. There is a routing table at that hop as well, which tells what the next hop is. This continues until the next hop is the destination host.

Source Host Name: ADMIN

Path Segment List:

Destination Host Name	Total Cost	Outgoing Link Name	Next-hop: DTE Address Station Address	Next_hop Host Name
DESK0	2	HQ_LINK	1111	HQ
DESK1	2	HQ_LINK	1111	HQ
HQ	1	HQ_LINK	1111	
MFG	1	LOCAL_LINK	3333 08001B1879CB	

Source Host Name: DESK0

Path Segment List:

Destination Host Name	Total Cost	Outgoing Link Name	Next-hop: DTE Address Station Address	Next_hop Host Name
ADMIN	2	ASYNC_LINK	1111	HQ
DESK1	2	ASYNC_LINK	1111	HQ
HQ	1	ASYNC_LINK	1111	
MFG	2	ASYNC_LINK	1111	HQ

Figure 7-3. Printable Version of the Routing Table (continues)

```
Source Host Name:  DESK1

Path Segment List:

                                                Next-hop:
Destination                  Outgoing                DTE Address    Next_hop
 Host Name    Total Cost     Link Name             Station  Address   Host Name
----------    ----------    ---------             -----------------  ---------

ADMIN                 2     SWITCHED_LINK         1111                HQ

DESKO                 2     SWITCHED_LINK         1111                HQ

HQ                    1     SWITCHED_LINK         1111

MFG                   2     SWITCHED_LINK         1111                HQ

Source Host Name:  HQ

Path Segment List:

                                                Next-hop:
Destination                  Outgoing                DTE Address    Next_hop
 Host Name    Total Cost     Link Name             Station Address   Host Name
----------    ----------    ---------             ----------------  ---------

ADMIN                 1     HQ_LINK               2222

DESKO                 1     ASYNC_LINK            4444

DESK1                 1     SWITCHED_LINK         5555

MFG                   1     LOCAL_LINK            3333
                                                  08001B1879CB
```

Figure 7-3. Printable Version of the Routing Table (continued)

```
Source Host Name:  MFG


Path Segment List:

                                                Next-hop:
Destination                  Outgoing               DTE Address   Next__hop
 Host Name    Total Cost     Link Name             Station Address  Host Name
----------    ----------     ---------             ---------------  ---------

ADMIN                 1     LOCAL__LINK           2222
                                                  08001B76A54C

DESK0                 2     LOCAL__LINK           1111             HQ
                                                  08001B132435

DESK1                 2     LOCAL__LINK           1111             HQ
                                                  08001B132435

HQ                    1     LOCAL__LINK           1111
                                                  08001B132435
```

Figure 7-3. Printable Version of the Routing Table (concluded)

End of Chapter

Chapter 8
Controlling Network Processes

After you run NETGEN, you can use the Network Operator Process (NETOP) to create network processes on your local host, control what they do, and terminate them when necessary.

This chapter covers the following topics:

- an overview of the network processes: NETOP, and sons X25, XTS, SVTA, RMA, and FTA
- communicating with the network processes
- bringing up a network
- bringing down a network

Chapters 9 through 13 describe the NETOP commands for controlling the network processes, X25, XTS, RMA, FTA, and SVTA.

Appendix C describes how to respond to network process errors.

NETOP and Its Son Processes

The Network Operator process (NETOP) is your tool for controlling the network. NETOP interprets commands and generates reports for XODIAC system processes. When you bring up the network, you first bring up NETOP and then its son processes, X25 or XTS, SVTA, FTA, and RMA. SVTA, FTA, and RMA provide services to network users and are called NETOP's *agents*. You may also bring up other processes that provide network services, such as the Remote INFOS Agent (RIA) and the Remote Database Agent (RDA).

Each of NETOP's son processes has its own commands. When you send a command to a network process, NETOP receives, translates, and forwards it to the process. NETOP also sends you a message acknowledging receipt of your command, but only the process that executes the command can verify its successful completion. This process sends a confirmation message to NETOP, which translates and forwards the message to you.

NETOP and its son processes accept commands only from the username that started NETOP. You bring up the network from the system console, under username OP, so you must enter NETOP commands from the CLI process with the username OP.

Table 8-1 shows the processes with which you communicate through NETOP.

Table 8-1. NETOP's Son Processes

Process	What It Allows You to Do
RMA	Create, manage and access remote resources.
SVTA	Log on to a remote host.
FTA	Transfer files between hosts.
X25 (AOS) XTS (AOS/VS)	Control links and communication devices.

Communicating with NETOP Son Processes

You communicate with NETOP's son processes through the CLI. To send a command to one of these processes, you use the CLI CONTROL command as follows:

```
CONTROL  @process-name  command
```

For example, to enter FTA's TIMEOUT command, you enter

```
) CONTROL  @FTA  TIMEOUT ↓
```

The first argument to this command, @FTA, specifies that your command will go to NETOP's Interprocess Communication (IPC) port for FTA. The second argument, TIMEOUT, is your message to FTA.

An IPC port acts as an "inbox" for messages from other processes. In this case, the CLI is sending the message to NETOP. NETOP has a separate IPC port to receive messages meant for each son process. IPC ports are also represented by files located in :PER (the @ sign stands for :PER:). When the network is up, you can see IPC files for each of NETOP's son processes in :PER.

For example, when you enter the CONTROL @FTA TIMEOUT command, this is what happens:

- The CLI forwards the command to NETOP's IPC port for FTA, @FTA.
- NETOP receives your command from @FTA, translates the command, and forwards it to an IPC port called @FTA$.
- The FTA process receives the translated command from the IPC port, executes the command, and reports back to NETOP.
- Finally, NETOP translates FTA's message and displays it for you.

Using Macros to Enter NETOP Commands

The directory :NET:UTIL has macros that simplify the command line for controlling network processes. For example, instead of entering the FTA TIMEOUT command as the previous section showed, you can simply enter

```
) CFTA  TIMEOUT ↓
```

The macros for each process are as follows:

Macro	Substitutes for
CRMA	CONTROL @RMA
CSVTA	CONTROL @SVTA
CFTA	CONTROL @FTA
CXTS	CONTROL @XTS
CX25	CONTROL @X25

NETOP Messages

After issuing a CONTROL command, you receive two messages: one from NETOP and one from its son process. NETOP's response acknowledges your command; the process response returns the result of the command. For example, in response to a request that RMA turn on STATISTICS gathering, the following messages appear. The first message is from NETOP, and after a delay, the second comes from RMA (but again, through NETOP).

```
) CONTROL  @RMA  STATISTICS ↵
.
.
.
FROM PID 7 : (NETOP)                    NETOP acknowledges receipt of the
    TIME: 11:33:33                      command.
.
.
.
FROM PID 6 : (RMA)                      RMA returns the requested information.
    STATISTICS ON
```

By default, NETOP displays these responses at the terminal of its father process, but you can send the responses to another terminal. Each process has a SET command and /OUTPUT switch that directs responses to another terminal.

By using the process SET command with its /LOG switch, you can also send responses to a log file. The log file entries include the same messages that the output console displays. Enabling logging is a good practice, because a log can help you determine the cause of any errors that might occur. If you enter an incorrect command, NETOP informs you as follows:

```
) CONTROL  @RMA  STATASTICS ↵
.
.
.
FROM PID 7 : (NETOP)
    Unrecognized Command
    Command: STATASTICS
    TIME: 11:33:33
```

The following chapters, Chapters 9 through 13, have command descriptions and examples. The examples generally omit the NETOP response. Instead, they show just the response from the process to which you have sent the command.

Two of the main tasks you will have in controlling the network are bringing the network up and down. The next sections describe how to do that.

Bringing Up the Network

Bringing up the network comprises a series of steps that make network processes available on your system. While you bring up the network on only your own host, the network must also be up on each host to which you want to communicate. You can bring up the network only from PID 2 with the Superuser privilege turned on.

Bringing up the network is the same on AOS and AOS/VS systems except that AOS systems require X25, and AOS/VS systems require XTS. In general, the steps are as follows:

- Start the NETOP process (using the CLI PROCESS command).
- Enable logging to keep track of all events (using the SET command for each process).
- Start the NETOP son processes that provide transport service and manage links, X25 and XTS (using the START command for X25 or XTS).
- Enable links (using the ENABLE command).
- Start the agent processes, RMA, FTA, and SVTA (using each agent process START command).
- Enable virtual consoles (using the CONTROL @EXEC ENABLE command).

Bringing up your network may involve other steps specific to the needs of your system.

Before you bring up the network, you create the File Transfer Queue and open it to users. You usually do this when you bring up the operating system, but if you haven't, you can do it now:

```
) CONTROL  @EXEC  CREATE FTA FTQ ↓
) CONTROL  @EXEC  OPEN FTA FTQ ↓
```

For more information on creating and opening the File Transfer Queue, refer to *How to Generate and Run AOS* or *How to Generate and Run AOS/VS*.

The UP.NETWORK Macro

The directory :NET:UTIL contains a macro, UP.NETWORK.CLI, to help you bring up the network on your system. Instead of running the macro, you can enter the commands separately, using essentially the same steps. We point out any differences in a later section that explains each line in the macro.

The network UP.NETWORK macro is not executable until you edit it. The next section describes how to edit the macro.

The UP.NETWORK macro uses the WAIT_FOR_PORT macro. When the UP.NETWORK macro creates a process, the WAIT_FOR_PORT macro checks for the existence of the process's IPC port. When the IPC port appears, the process is ready to accept commands, and the UP.NETWORK macro continues.

Figure 8-1 shows the UP.NETWORK macro for an AOS/VS system. The macro for an AOS system is the same except that it starts X25 and not XTS. The next sections describe how to edit the macro and explain each line in it.

```
[!NEQUAL,,COMMENT]
    WRITE This is a non-executable sample of a network UP.NETWORK macro.
    WRITE In order to make it executable, first edit it to suit
    WRITE your system configuration.
    WRITE Then change "NEQUAL" in the first line of the macro
    WRITE to "EQUAL".
[!ELSE]

    [!EQUAL,2,[!PID]]
        PUSH
        SEARCHLIST [!SEARCHLIST] :NET :NET:UTIL
        SUPERUSER ON
        ACL :NET OP WARE + RE
        ACL :NET:LOGFILES OP WARE + RE
        PROCESS/DEFAULT/NAME=NETOP/DIRECTORY=@ NETOP
        WAIT_FOR_PORT @XTS
        CONTROL @(XTS RMA SVTA FTA) SET/LOG/DATE
        CONTROL @XTS START
        WAIT_FOR_PORT @XTS$
        [!EQUAL,,COMMENT]
            At this point you will want to activate each communications
            link. To do this, replace this comment with a series
            of commands to the XTS process such as:
              CONTROL @XTS ENABLE   link1
```

Figure 8-1. The UP.NETWORK.CLI Macro (continues)

```
            CONTROL @XTS ENABLE   link2
                .....
            where "link1" and "link2" were the names given to
            the various links during your NETGEN session.
        [!END]
        CONTROL @SVTA START/VCONS=8
        CONTROL @RMA START
        CONTROL @FTA START
        WAIT_FOR_PORT @FTA$
        CONTROL @FTA STREAMS 1
        CONTROL @FTA LIMIT/UFTA=10
        CONTROL @FTA LIMIT/SFTA=10
        CONTROL @FTA LIMIT/TOTAL=10
        CONTROL @EXEC START FTQ @FTA_EXEC
        CONTROL @EXEC CONTINUE @FTA_EXEC
        [!EQUAL,,COMMENT]
            To enable the virtual consoles now
            include the following commands:

            WAIT_FOR_PORT @VCON7
            CONTROL @EXEC ENABLE @VCON(0,1,2,3,4,5,6,7)
        [!END]
        POP
    [!ELSE]
        WRITE ERROR: %0\% is valid only when invoked by the master CLI
    [!END]
[!END]
```

Figure 8-1. The UP.NETWORK.CLI Macro (concluded)

Editing the UP.NETWORK Macro

To use the UP.NETWORK macro, you must edit it.

First, change `[!NEQUAL,,COMMENT]` in the first line of the macro to `[!EQUAL,, COMMENT]`.

Next, customize the macro to your network as follows.

Optional: Change the ACL command if you want to allow or prevent users from using network processes in :NET or :NET:UTIL.

Required: Activate each device and initiate each link, using the X25 or XTS ENABLE command.

On an AOS system, you can create a file that contains the names of all the hosts to which you want to enable links. Then you can use the filename as the ENABLE command argument instead of enabling each link separately. The step-by-step explanation explains how to do this.

Optional: Alter the command, `CONTROL @SVTA START/VCON=8`, if you want to specify a different number of virtual consoles.

Optional: Alter the command, `CONTROL @EXEC ENABLE @VCON(0,1,2,3,4,5,6,7)`, if you want to enable a different number of virtual consoles; change the `WAIT_FOR_PORT` macro above it accordingly.

Optional: Alter the `FTA LIMIT` commands if you want to allow more or fewer concurrent file transfers.

The UP.NETWORK Macro, Step by Step

This section explains each command line in the standard AOS/VS UP.NETWORK macro. The macro on an AOS system replaces XTS with X25. Also, if you look at a macro that is currently in use, you might see that the macro has been customized to include information specific to the network configuration.

To bring up the network interactively, use the same commands, but omit those lines marked *Macro Only*. Replace each `WAIT_FOR_PORT` macro with a CLI command that checks for the existence of the appropriate process. For example, instead of `WAIT_FOR_PORT @XTS`, use the CLI command, `WHO OP:XTS`. Wait until the system displays XTS's PID before proceeding.

For more information on the NETOP commands in the macro, refer to Chapters 9–13. For more information on the EXEC commands, refer to *How to Generate and Run AOS* or *How to Generate and Run AOS/VS*.

`[!EQUAL,2,[!PID]]` *Macro Only*

Checks to see that you are at PID 2. You can bring up the network only from the master CLI.

`PUSH`

Moves you to another level. This makes the search list change and

Superuser privilege in the next two lines valid during the macro's execution only.

```
SEARCHLIST [!SEARCHLIST] :NET :NET:UTIL
```

Changes your search list to include the directories :NET and :NET:UTIL. These directories have program files for network processes and macros that you will be using.

```
SUPERUSER ON
```

Invokes the Superuser privilege, which you need to gain access to the directories, :NET and :NET:UTIL.

```
ACL :NET OP WARE + RE
```

Gives OP Write, Append, Read, and Execute privileges to files in :NET. Gives all other users Read and Execute privileges to these files.

```
ACL :NET:LOGFILES OP WARE +RE
```

Sets the ACLS on :NET:LOGFILES to give OP Write, Append, Read, and Execute access to log files in :NET:LOGFILES. Gives all users Read and Execute access to the log files. These log files will be created only if you use NETOP's SET commands to enable logging, and accept the default log file destination. To send log files to another directory, change the directory in this command.

```
PROCESS/DEFAULT/NAME=NETOP/DIRECTORY=@NETOP
```

Creates a process whose name is NETOP. The /DEFAULT switch gives this process the same privileges as its creator process, OP. The /DIRECTORY switch specifies the initial directory for the NETOP process; @NETOP stands for :PER:NETOP.

When the NETOP process starts, it creates its IPC ports for the son processes @XTS, @FTA, @RMA, and @SVTA.

```
WAIT_FOR_PORT @XTS        Macro Only
```

Checks to see that @XTS exists and is ready to accept commands, since the UP.NETWORK macro will soon start XTS. NETOP's IPC port for XTS must exist so that NETOP can receive XTS commands.

```
CONTROL @(XTS RMA SVTA FTA) SET/LOG/DATE
```

Sets NETOP parameters to enable logging for each son process and includes the date in all logs. While logging is optional, you will find the log files useful for monitoring network operation, especially if errors occur. You submit these files as part of a Software Trouble Report.

By default, log files will be in :NET:LOGFILES. You can send log files to a different directory by appending an equal sign and the directory pathname to the /LOG switch and changing the pathname in the earlier ACL command.

The log file name has the format, processname_date.LOG.

```
CONTROL @XTS START
```

Starts the XTS process. Because the agent processes require the existence of XTS, you must start XTS first.

```
WAIT_FOR_PORT @XTS$
```
Macro Only

Checks for the XTS IPC port for receiving messages from NETOP, @XTS$. The last START command created this IPC port.

```
CONTROL @XTS ENABLE linkname
```

Enables one link for every ENABLE command line. Note that the format for enabling links is different on AOS and AOS/VS systems; check the command descriptions in the appropriate chapters for more information.

On AOS systems *only*, you can use a shortcut to enable links to multiple hosts with only one ENABLE command line. In the directory :NET:UTIL, create a file called NETWORK_HOSTS.CLI. In the file, enter the names of all the hosts to which you want to enable links, using the following format, and ending with an ampersand:

```
host1,host2,host3,host4&
```

Then you can use the file as an argument to the ENABLE command, as follows:

```
CONTROL @X25 ENABLE ([NETWORK_HOSTS])
```

```
CONTROL @SVTA START/VCONS=8
```

Starts the SVTA process and creates 8 virtual consoles. Edit this command if you want to create more or fewer virtual consoles. This command just sets up the virtual consoles in :PER; you enable them later by issuing the EXEC ENABLE command.

```
CONTROL @RMA START
```

Starts the RMA process.

```
CONTROL @FTA START
```

Starts the FTA process.

```
WAIT_FOR_PORT @FTA$
```
Macro Only

Checks to see if FTA's IPC port for receiving messages, @FTA$, exists yet before sending the next commands that set parameters for FTA. Pauses the UP.NETWORK macro and waits for the port to appear, if necessary.

```
CONTROL @FTA STREAMS 1
```

Sets the number of streams in the File Transfer Queue to 1.

```
CONTROL @FTA LIMIT/UFTA=10
CONTROL @FTA LIMIT/SFTA=10
CONTROL @FTA LIMIT/TOTAL=10
```

Limits concurrent file transfers to a total of 10. The total of 10 can be either a mixture of both UFTA and SFTA transfers, or up to 10 transfers

of either UFTA or SFTA. Edit this command if you want to allow more or fewer concurrent transfers.

The next two commands are optional; you may have issued them when you brought up your operating system.

```
CONTROL @EXEC START FTQ @FTA_EXEC
```

Starts the queue named FTQ and associates it with the IPC port for EXEC-to-FTA communication, @FTA_EXEC. When EXEC starts processing data in the File Transfer Queue, it notifies FTA through this port.

```
CONTROL @EXEC CONTINUE @FTA_EXEC
```

Continues queue processing. This command is needed whenever you start a queue.

For more information on the EXEC commands, refer to *How to Generate and Run AOS* or *How to Generate and Run AOS/VS*.

```
WAIT_FOR_PORT @VCON7
```
Macro Only

Checks to see if the IPC ports for the virtual consoles named in the SVTA START command actually exist, by checking for the IPC port of the last virtual console created. If you edited the number of consoles that the SVTA START command created, edit this command also.

```
CONTROL @EXEC ENABLE @VCON(0,1,2,3,4,5,6,7)
```

Enables the virtual consoles. You can edit this command to enable more or fewer virtual consoles.

```
POP
```

Returns you to the level from which you started executing the macro.

The network is now ready for use. You can, however, add commands that bring up applications specific to your system. Place the additional commands after the command that brings up XTS (or X25, on an AOS system). For example, to bring up RIA, the Remote INFOS Agent, add the following command:

```
CONTROL @RIA START
```

Bringing Down the Network

From time to time, it may be necessary to bring down the network. Bringing down the network consists of terminating the network processes. To bring down the network, you must be logged on at PID 2 and have Superuser privileges.

Before you bring down the network, you must disable all virtual consoles. Enter the following EXEC DISABLE command, including in the parentheses the number of each virtual console you previously enabled:

```
CONTROL @EXEC DISABLE @VCON(0...n)
```

The DISABLE command does not affect current users of virtual consoles; it simply disables those that are inactive and prevents new users from logging on. If you must bring the network down immediately, send a message to virtual console users and request that they log off. You can terminate the processes that do not log off, if necessary, by using the following EXEC TERMINATE command:

```
CONTROL @EXEC TERMINATE @VCONconsole-number
```

The DOWN.NETWORK Macro

The directory :NET:UTIL contains a macro, DOWN.NETWORK.CLI, to help you bring down the network on your system. You can bring down the network in an interactive session instead of running the macro, but the steps are essentially the same. We point out any differences in a later section that explains each line in the macro.

The DOWN.NETWORK macro is not executable until you edit it. The next section describes how to edit the macro.

After editing the macro, you can execute it. The macro starts by asking if you want to bring down the network. If you answer N, it stops. If you answer Y or YES, it begins to execute.

The WAIT_FOR_NO_PORT macro appears at several places in the DOWN.NETWORK macro. The WAIT_FOR_NO_PORT macro is analogous but opposite to WAIT_FOR_PORT in the UP.NETWORK macro. It causes the DOWN.NETWORK macro to wait until the IPC port for the process last terminated has disappeared. When the IPC port is gone, the DOWN.NETWORK macro continues. For more information on IPC ports, refer to the programmer's manual for your operating system.

Figure 8-2 is the DOWN.NETWORK macro for an AOS/VS system. The macro for bringing down the network on an AOS system is the same, except that it terminates X25 instead of XTS. In the next sections, we describe how to edit the macro and explain the macro line-by-line.

```
[!NEQUAL,,COMMENT]
    WRITE This is a non-executable sample of a network UP.NETWORK macro.
    WRITE In order to make it executable, first edit it to suit
    WRITE your system configuration.
    WRITE Then change "NEQUAL" in the first line of the macro
    WRITE to "EQUAL".
[!ELSE]
    [!EQUAL,2,[!PID]]
        WRITE [!ASCII 212]
        WRITE ****** Make sure all virtual consoles are disabled and all
        WRITE ****** users of virtual consoles are logged off!!!!
        STRING [!READ [!ASCII 212 212]Do you want to bring down the network?,]
        [!EQUAL,([!STRING]),(Y)]
            STRING YES
        [!END]
        [!EQUAL,([!STRING]),(YES)]
            PUSH
            SEARCHLIST [!SEARCHLIST] :NET:UTIL
            CONTROL/2=IGNORE @(XTS RMA SVTA FTA) SET/NOOUTPUT
            CONTROL/2=IGNORE @XTS HALT
            TERMINATE/2=IGNORE OP:(SVTA FTA RMA)
            WAIT_FOR_NO_PORT @(SVTA FTA RMA)$
            WAIT_FOR_NO_PORT @XTS$
            TERMINATE/2=IGNORE OP:NETOP
            WAIT_FOR_NO_PORT @XTS
            POP
        [!END]
    [!ELSE]
        WRITE ERROR: %0\% is valid only when invoked by the master CLI
    [!END]
[!END]
```

Figure 8-2. The AOS/VS DOWN.NETWORK.CLI Macro

Editing the DOWN.NETWORK Macro

Editing the DOWN.NETWORK macro involves two steps:

- Change `[!NEQUAL,,COMMENT]` in the first line to `[!EQUAL,,COMMENT]`.
- Add termination commands for any applications specific to your system.

The DOWN.NETWORK Macro, Step by Step

This section explains each command line in the macro DOWN.NETWORK.CLI.

`[!EQUAL,2,[!PID]]`

Checks to see that you are logged on at PID 2. Only the master CLI can bring down the network.

```
PUSH
```

Moves you to another level; this makes the search list change in the next line valid during the macro's execution only.

```
SEARCHLIST [!SEARCHLIST] :NET:UTIL
```

Changes your search list to include the directory :NET:UTIL. This directory contains macros that this UP.NETWORK macro will invoke.

```
CONTROL/2=IGNORE @(XTS RMA SVTA FTA) SET/NOOUTPUT
```

Uses the SET command to disable the display of messages from each process named in the parentheses. This prevents each termination message from appearing on your screen. If you have previously enabled logging, termination messages will continue to appear in log files. The /2=IGNORE switch causes any error (for example, if one of the processes doesn't currently exist) to be ignored, so the macro can continue.

```
CONTROL/2=IGNORE @XTS HALT
```

Disables all links and terminates the XTS process.

```
TERMINATE/2=IGNORE OP:(SVTA FTA RMA)
```

Terminates the SVTA, FTA, and RMA processes.

```
WAIT_FOR_NO_PORT @(SVTA FTA RMA)$
```

Checks to see that SVTA, FTA, and RMA have terminated by ensuring that their ports for receiving IPC messages have been deleted.

```
WAIT_FOR_NO_PORT @(XTS)$
```

Checks to see that XTS has terminated by ensuring that its IPC port for receiving IPC messges has been deleted.

```
TERMINATE/2=IGNORE OP:NETOP
```

Terminates the NETOP process, now that all of NETOP's son processes are gone and NETOP has reported and logged their termination.

```
WAIT_FOR_NO_PORT @XTS
```

Checks to see that NETOP has terminated by checking to see that its IPC port for receiving XTS commands has been deleted.

```
POP
```

Returns you to the level from which you started executing this macro.

The network on your host is now down.

End of Chapter

Chapter 9
Using NETOP with X25

X25 is the process that implements the X.25 protocol on AOS systems. X25 maintains a connection between remote hosts by managing communication between Data General hosts, connecting Data General hosts to public or private networks, breaking messages into packets, sending the packets along the route to their destination, and performing error checks on packets. The agents RMA, FTA, and SVTA depend on X25 for communications functions. Users can also write programs that use X25.

For a general discussion of Data General's implementation of the X.25 protocol, refer to the manual, *Programming with the XODIAC Network Management System (AOS and AOS/VS).*

As a network operator, you control certain aspects of the X25 process. Table 9-1 lists the X25 commands and tells what you use each command to do.

Table 9-1. X25 Commands

Command	Operator Function
ACCOUNT	Start the logging of accounting and exception information in the system log file.
CLEAR	Clear a virtual connection.
CUSTOMERS	Display a list of PIDs that are X25 customers.
DISABLE	Discontinue the use of a link.
ENABLE	Open a link for use.
HALT	Terminate the X25 process, clearing virtual connections.
LINKS	List the active links.
LRESET	Reinitialize a link's statistics accumulators.
LSTATUS	Display a report on a link's status.
NOACCOUNT	Stop the logging of accounting and exception information in the system log file.
NOTRACE	Stop a trace of packets on the network.
RESET	Reset a virtual connection.
RESOURCES	Display a report of X25 resources for a process.

(continues)

Table 9-1. X25 Commands

Command	Operator Function
RESTART	Restart a link, clearing all of its active switched virtual connections.
SET	Set parameters that determine how NETOP manages communication from X25 to you.
START	Start the X25 process.
STATUS	Display a report on a virtual connection.
SVCMAX	Set or display the maximum number of switched virtual connections.
TIMEOUT	Set or display the X25 time-out period.
TRACE	Start a trace of packets on the network.

(concluded)

NETOP X25 Command Dictionary

This section describes the NETOP X25 commands and related switches. The command descriptions are in alphabetical order and include examples. You can use unique abbreviations for commands, switches, and keywords. For example, you can use STAR for START and STAT for STATUS.

Examples show the X25 response to commands, but not the NETOP response. The examples assume that you enter the commands from the console that receives system output. You can reset the destination console for output by using the SET command.

To use the commands in this section, enter them in the following format at the CLI prompt:

```
CONTROL  @X25  command-name
```

You can also use the CX25 macro, as follows:

```
CX25  command-name
```

Link Names and Host Names

Some commands take link names or host names as arguments. The link name is the filename of the link configuration file (LCF). The host name is the name of the host for which this link has been designated the primary path. Both are assigned during a NETGEN session.

ACCOUNT

Starts X25 accounting.

Format

ACCOUNT

Description

This command directs the X25 process to place accounting and exception information in the system log file. When accounting is on, information for a virtual connection is logged when the connection clears, and exception information is logged when error conditions occur.

The REPORT program lets you display the contents of the system log file. For more information on the REPORT program, refer to *How to Generate and Run AOS*. Appendix A shows the file's X.25 parameters.

Command Switches

None.

Example

The following command turns accounting on:

```
) CONTROL @X25 ACCOUNT ↓
) .
  .
  .
FROM PID  8 : (X25)
  ACCOUNTING ON
  TIME: 09:46:00
```

CLEAR
Clears a virtual connection.

Format

CLEAR vc-number

where

vc-number is an octal number that represents a virtual connection.

Description

This command directs X25 to clear the virtual connection (VC) that you specify. If you specify a permanent VC (PVC), NETOP resets the virtual connection instead of clearing it. You'll find this command useful for debugging X.25 application programs.

Command Switches

None.

Example

In this example, the CUSTOMERS command first displays the local processes currently using X25, and the RESOURCES command displays their virtual connections. The CLEAR command then closes virtual connection 11.

```
) CONTROL @X25 CUSTOMERS ↓
) .
  .
  .
FROM PID  8 : (X25)
  CUSTOMER LIST
  9,12,14,17,19,24,31
TIME: 04:26:53

) CONTROL @X25 RESOURCES 012 ↓
  .
  .
  .
FROM PID  8 : (X25)
  RESOURCE REPORT
  FOR PID: 012
  A RECV. INT. REQ. IS ACTIVE
  NO. OF VC'S OWNED: 009
  VC NUMBERS:
    2,4,6,10,11
    13,20,21,22
  TIME:  4:27:49

) CONTROL @X25 CLEAR 11 ↓
.
.
.
FROM PID  8 : (X25)
  VC CLEARED:  11
  TIME: 4:27:58
```

CUSTOMERS

Reports X25 customer processes.

Format

CUSTOMERS

Description

This command reports the PID numbers of the processes that are X25 customers: processes that have issued a request for X25 services and are still connected to X25.

Command Switches

None.

Example

The following command lists X25 customer PIDs:

```
) CONTROL @X25 CUSTOMERS ↓
) .
  .
  .
FROM PID  8 : (X25)
  CUSTOMER LIST
  9,12,14,17,19,24,31
  TIME:  04:26:53
```

DISABLE

Discontinues use of an X25 link.

Format

DISABLE { linkname | hostname }

where

linkname is the name of a link.

hostname is the name of the host for which this link is the primary path.

Description

This command discontinues the use of a link that the ENABLE command has previously enabled. X25 will notify all affected user processes. The command report displays the name of the disabled link.

Command Switches

None.

Example

The following command disables link LINK1:

```
) CONTROL @X25 DISABLE LINK1 ↓
) .
  .
  .
FROM PID  8 : (X25)
  LINK DISABLE REPORT
  LINK NAME: LINK1
  TIME:  10:16:12
```

ENABLE
Enables an X25 link.

Format

ENABLE { linkname | hostname }

where

linkname is the name of a link.

hostname is the name of the host for which this link is the primary path.

Description

This command makes a link available for communications. The system report displays the name of the enabled link.

When it starts, X25 automatically enables loopback links 0 and 1. You cannot disable or enable these links yourself.

Command Switches

None.

Example

The following command enables link LINK3:

```
) CONTROL @X25 ENABLE LINK3 ↓
) .
  .
  .
FROM PID  8 : (X25)
  LINK ENABLE REPORT
  LINK NAME:  LINK3
  TIME:  14:02:15
```

HALT
Terminates the X25 process.

Format

HALT

Description

The HALT command terminates the X25 process, immediately closing all connections without informing remote X25.

Command Switches

None.

Example

The following command immediately terminates X25:

```
) CONTROL @X25 HALT ⤸
) .
  .
  .
FROM PID  8 : (X25)
  HALT REPORT
  TIME:  15:04:42
```

LINKS
Lists active links.

Format

LINKS

Description

This command generates a list of active links.

Command Switches

None.

Example

The following command lists the active links:

```
) CONTROL @X25 LINKS ↓
  .
  .
  .
FROM PID  8 : (X25)
  ACTIVE LINK LIST

  LOOPBACK1              LOOPBACK0        NBS_LCF
  TIME:  16:25:34
```

LRESET

Reinitializes the statistics accumulators for a link.

Format

LRESET { linkname | hostname }

where

linkname is the name of a link.

hostname is the name of the host for which this link is the primary path.

Description

This command reinitializes the statistics accumulators for the link you specify. The command requires a link name or host name.

Command Switches

None.

Example

The following command resets the statistics accumulators for LINK0:

```
) CONTROL @X25 LRESET LINK0 ↓
  .
  .
  .
FROM PID  8: (X25)
  RESET LINK STATUS REPORT
  FOR LINK0
  TIME:  10:35:31
```

LSTATUS

Reports the status of a link.

Format

LSTATUS*[/RESET]* { linkname | hostname }

where

linkname — is the name of a link.

hostname — is the name of the host for which this link is the primary path.

Description

The LSTATUS command generates a status report for a link. The command requires a host name or link name as an argument.

The command report includes the link's device type and state, and the number of bytes the link has transmitted and received since you last reset the accumulators, by using LSTATUS/RESET or LRESET or bringing the system up. The report varies, depending on the type of link you specify. For example, an NBS link returns a different status message from an ISC link.

Command Switches

/RESET — Reinitializes statistics for the specified link. This switch has the same effect as the LRESET command.

Examples

The following LSTATUS command reports on the synchronous link, SYNCH_LINK:

```
) CONTROL @X25 LSTATUS SYNCH_LINK )
) .
  .
  .
FROM PID  8 : (X25)
  LINK STATUS        ;LINK: SYNCH_LINK
  DATE: 20-JUL-85        TIME: 13:24:46
  STATUS INTV:  15:07:22
  DEVICE: SLN - LINE NUMBER: 0
  TIME: 13:24:47 ; 20-JUL-1985
```

```
FROM PID  8 : (X25)
  LINK STATUS        ;LINK: SYNCH_LINK
  FRAMES: RCV.:0       XMT.:0
  BYTES: RCV:0  XMT.:0
  STATE: DCE/LINK TASK ACTIVE/ENABLE IN PROGRESS
  NUMBER OF ACTIVE VC'S: 0
  TIME:  13:24:47 ; 20-JUL-1985

FROM PID  8 : (X25)
  LINK STATUS        ;LINK: SYNCH_LINK
  FRAMES RESENT; 0; I-FRAMES TIMED OUT: 0
  RNR'S:  RCV.:0  XMT.:0
  REJ'S:  RCV.:0  XMT.:0
  LINK RESETS:  RCV.: 0  XMT.: 0
  FRAMES WITH CRC ERRORS: 0; DATA OVERRUNS SEEN: 0
  TIME:  13:24:47 ; 20-JUL-1985
```

We know from the report that SYNCH_LINK has neither received nor transmitted any frames although the link is active and enabled, no virtual connections are active, no frames have been sent or timed out, no frames have been sent or transmitted when the receiver has not been ready (RNR) to accept them, nor have any frames been rejected (for arriving out of sequence). We also know that no frames arrived with Cyclic Redundancy Check (CRC) errors; that is, all of the parity bits were as they should have been when the frames arrived. Finally, we know that data did not overrun the input buffers.

The next command displays a status report on an NBS link:

```
) CONTROL @X25 LSTATUS NBS_LINK ↓
) .
  .
  .
FROM PID  8 : (X25)
  LINK STATUS        ;LINK: NBS_LCF
  DATE:  20-JUL-85       TIME:  13:24:46
  STATUS INTV:  15:07:18
  DEVICE:  NBS
  TIME:  13:24:47 ; 20-JUL-1985

FROM PID  8 : (X25)
  LINK STATUS        ;LINK: NBS_LCF
  FRAMES:  RCV.:3984  XMT.:3985
  BYTES:  RCV:130804  XMT.:752407
  STATE:  MOD 8
  # OF ACTIVE VC'S: 2
  TIME:  13:24:47 ; 20-JUL-1985

FROM PID  8 : (X25)
  LINK STATUS        ;LINK:  NBS_LCF
  FRAMES RETRANSMITTED:  110
  RECEIVE BUFFER BUSY ERRORS:  0
  BUFFER OVERFLOW ERRORS:  0
  TIME:  13:24:47 ; 20-JUL-1985
```

LSTATUS (continued)

```
FROM PID  8 : (X25)
  LINK STATUS       ;LINK:  NBS_LCF
  REACKNOWLEDGEMENT WARNINGS:  0
  TRANSMISSION ERRORS:  11
  NEGATIVE ACKNOWLEDGEMENT ERRORS:  0
  TIME:  13:24:47 ; 20-JUL-1985

FROM PID  8 : (X25)
  LINK STATUS       ;LINK: NBS_LCF
  INVALID RESPONSE ERRORS:  0
  NO RESPONSE ERRORS:  121
  NO ACK AFTER 7 RETRIES ERRORS:  0
  RECEIVE DISABLED ERRORS:  0
  TIME:  13:24:47 ; 20-JUL-1985

FROM PID  8 : (X25)
  LINK STATUS       ;LINK: NBS_LCF
  NBS UNIT : 15
  STATE:  DTE/READY
  # OF ACTIVE VC'S : 0
  TIME:  13:24:47 ; 20-JUL-1985
```

From the report, we know that the interval between the last status command and this one was 15 hours, 7 minutes, and 18 seconds. NBS_LCF has received 3984 frames and transmitted 3985. It has received 130804 bytes and transmitted 752407. The link is active, with two active virtual connections.

X25 also reports on the types and numbers of errors that have occurred. One hundred ten frames had to be retransmitted. No errors occurred because the receiving buffer already held data from a previous transmission; the buffer was able to accommodate all of the incoming data. No reacknowledgement warnings were necessary. There were 11 transmission errors.

Because an acknowledgement was received within 7 retries, no error occurred. None of the systems received an error because another system was disabled.

Last, NBS unit 15 is a DTE ready to accept data. There are no active virtual connections on this device.

NOACCOUNT
Turns off X25 accounting.

Format

NOACCOUNT

Description

This command directs X25 to turn off accounting.

Command Switches

None.

Example

The following command disables accounting:

```
) CONTROL @X25 NOACCOUNT ↓
) .
  .
  .
FROM PID  10 : (X25)
  ACCOUNTING OFF
  TIME:  08:56:00
```

NOTRACE
Terminates a trace.

Format

NOTRACE

Description

This command turns off tracing, terminating the trace begun by the previous TRACE command and closing the trace file. The trace file is the file to which X25 dumped packet images.

The NTRACE program lets you examine the contents of a trace file. It is described in Appendix B.

Command Switches

None.

Example

In the following example, the first command sets up a global trace in which X25 dumps packet images into the file PACKETS. The second command begins a new trace on virtual connection 12, using a trace file called VC12PACK. Finally, the NOTRACE command turns off tracing.

```
) CONTROL @X25 TRACE/GLOBAL :UDD:BARBARA:PACKETS ↵
) .
  .
  .
FROM PID  12 : (X25)
  TRACE ON
  TIME:  12:13:38

) CONTROL @X25 TRACE/VC=12 VC12PACK ↵
) .
  .
  .
FROM PID  12 : (X25)
  TRACE ON
  TIME:  12:14:11

) CONTROL @X25 NOTRACE ↵
) .
  .
  .
FROM PID  12 : (X25)
  TRACE OFF
  TIME:  12:15:37
```

RESET

Resets a virtual connection (VC).

Format

RESET vc-number

where

vc-number is an octal number that represents a virtual connection.

Description

This command directs X25 to reset a virtual connection. X25 notifies the local VC owner that the connection has been reset. You will find this command useful when debugging an X.25 application program.

Command Switches

None.

Example

The following command resets virtual connection 201:

```
) CONTROL @X25 RESET 201 ↓
) .
  .
  .
FROM PID   12 : (X25)
  RESET VC:   201
```

RESOURCES

Reports X25 resources for a process.

Format

RESOURCES pid

where

pid is the process identifier.

Description

The RESOURCE command displays a resource report for a particular process.

The report displays the number of virtual connections (VCs) owned by the process, and lists their VC numbers in octal values. The report also indicates whether the process has issued a Receive Interrupt request (?NRVI), and whether it currently has one active.

The message format for resource reports is as follows:

FROM PID x : (X25)
RESOURCE REPORT
FOR PID: x
[A RECV. INT. REQ. WAS ISSUED
[A RECV. INT. REQ. IS ACTIVE]
NO. OF VC'S OWNED: yyy
VC NUMBERS:
zzz,zzz,zzz,zzz,zzz
zzz, . . .

(The display may include only one of these messages.)

where

x represents the identifier number for this process.

yyy represents a decimal value.

zzz represents an octal value.

The STATUS command displays more information about the virtual connections for the process.

Command Switches

None.

Example

The following command directs X25 to display a resource report for PID 12:

```
) CONTROL @X25 RESOURCES 12 ↓
  .
  .
  .
FROM PID  8 : (X25)
  RESOURCE REPORT
  FOR PID: 012
  A RECV. INT. REQ. IS ACTIVE
  NO. OF VC'S OWNED: 009
  VC NUMBERS:
  2,4,6,10,11
  13,20,21,22
  TIME:  11:24:49
```

We know from the report that PID 12 has an active Receive Interrupt request and that it owns nine virtual connections with the numbers 2, 4, 6, 10, 11, 13, 20, 21, 22.

RESTART
Restarts a link.

Format

RESTART { linkname | hostname }

where

linkname — is the name of a link.

hostname — is the name of the host for which this link is the primary path.

Description

This command restarts a link and clears all of its active switched virtual connections (SVCs). You will find this command helpful in debugging X.25 application programs.

Command Switches

None.

Example

The following command restarts LINK0:

```
) CONTROL @X25 RESTART LINK0 ↓
) .
  .
  .
FROM PID  12 : (X25)
  LINK RESTART REPORT
  LINK: LINK0
```

SET

Sets conditions for logging and message reporting.

Format

SET*[/switches]*

Description

This command sets internal NETOP parameters that determine the nature and destination of system response messages. You can use the SET command before starting X25 or at any subsequent time.

Normally, the console of NETOP's father process displays X25 reports. You can change the destination for reports by using the /OUTPUT switch. If it is unable to send a message to the terminal you specify, NETOP resets the output destination to the console of its father process. If NETOP encounters an error while sending a message to that console, however, the message will be lost.

You can also send reports to a log file by using the /LOG switch.

Command Switches

/DATE	Includes the date with all reports.
/LOG*[=logfile]*	Enables logging and creates a new log file. Without an argument, the log file has a default filename and is in the directory :NET:LOGFILES. With an argument, the log file name and directory are those that you specify in an absolute pathname.
/NODATE	Suppresses the date in reports. This is the default setting.
/NOLOG	Disables logging.
/NOOUTPUT	Disables reporting to the console.
/NOPROMPT	Suppresses the following in NETOP messages: *FROM PID n : (NETOP)* *TIME: nn:nn:nn*
/NOTIME	Suppresses the time in NETOP messages.

SET (continued)

/OUTPUT[=*@console-name* | =*pid* | =*process-name*]

Specifies the destination console for X25 reports. Without an argument, messages go to the console of NETOP's father process. With an argument, messages go to the console *@console-name* or to the console owned by the *pid* or *process-name* that you specify.

/PROMPT

Displays the NETOP prompt. This is the default setting.

/TIME

Displays the time in NETOP messages. This is the default setting.

Examples

The following SET command causes the ENABLE command report to include the time. Note that there is no report for the SET command.

```
) CONTROL @X25 SET/TIME ↵
) CONTROL @X25 ENABLE 5 ↵
) .
  .
  .
FROM PID  10 : (X25)
  LINK ENABLE REPORT
  LINK NO. : 005
  TIME:  13:27:34
```

The next SET command causes X25 to send its reports to PID 5:

```
) CONTROL @X25 SET/OUTPUT=5 ↵
```

This final command causes X25 to write responses to the file :COMLOG:NOV24:

```
) CONTROL @X25 SET/LOG=:COMLOG:NOV24 ↵
```

START

Starts the X25 process.

Format

START*[/switches]*

Description

The START command initiates the X25 process, making it available for remote communications. By default, X25 is a resident process, and must be resident unless your system includes only MCA and/or asynchronous devices.

If NETOP encounters a problem in starting X25, you receive a termination message that includes the PID number assigned to X25 and the reason for termination. Depending on the type of error, NETOP may also display the contents of the accumulators and the program counter.

To optimize performance, include the switches that specify devices you do not have. Each switch releases the X25 code for the specified device, freeing memory for use by data buffers. To reverse the effect of the switch, you simply issue another START command, omitting the switch.

Before issuing another START command, you must terminate X25, using the HALT command.

Command Switches

/NOASYNC	Releases memory reserved for X25's ASYNC code. Use this switch if you do not have a device of type PMGR_ASYNC.
/NO802	Releases memory reserved for X25's 802 code. Use this switch if you do not have an 802 device.
/NOMCA	Releases memory reserved for X25's MCA code. Use this switch if you do not have an MCA device.
/NONBS	Releases memory reserved for X25's NBS code. Use this switch if you do not have an NBS device.
/NOSYNC	Releases memory reserved for X25's code for synchronous controllers. Use this switch if you do not have a DCU, ISC, or ISMC device.
/PREEMPTIBLE	Starts X25 as a pre-emptible process. You can use this switch if your system includes only MCA and/or asynchronous devices.
/PRIORITY=n	Sets the initial priority for the X25 process to n. The default priority is 2.

START (continued)

/RESIDENT	Initiates X25 as a resident process. This is the default.
/SWAPPABLE	Initiates X25 as a swappable process. You can use this switch if your system includes only MCA and/or asynchronous devices.

These switches relate to operating system concepts explained in the *Advanced Operating System (AOS) Programmer's Manual.*

Examples

The following command starts X25 as a resident process:

```
) CONTROL @X25 START/RESIDENT ↵
) .
  .
  .
FROM PID  7 : (X25)
  STARTED
  PID =  12
  TIME:  16:05:17
```

This next command starts X25, using only synchronous lines:

```
) CONTROL @X25 START/SWAPPABLE/NOASYNC/NO802/NOMCA/NONBS ↵
) .
  .
  .
FROM PID  7 : (X25)
  STARTED
  PID =  12
  TIME:  17:21:32
```

STATUS

Reports the state of a virtual connection.

Format

STATUS vc-number

where

vc-number is an octal number that represents a virtual connection.

Description

The STATUS command displays information about a specific virtual connection.

Each of the report's two sections begin with the following information: the virtual connection, the link, and the PID numbers. The first section gives the date and time that the connection began, and the number of packets received and transmitted. The second section gives the process name, the remote DTE's address, the way in which the call was established, and the state of the connection.

Figure 9-1 illustrates the format of the STATUS report. Table 9-2 describes the connection states reported by the command.

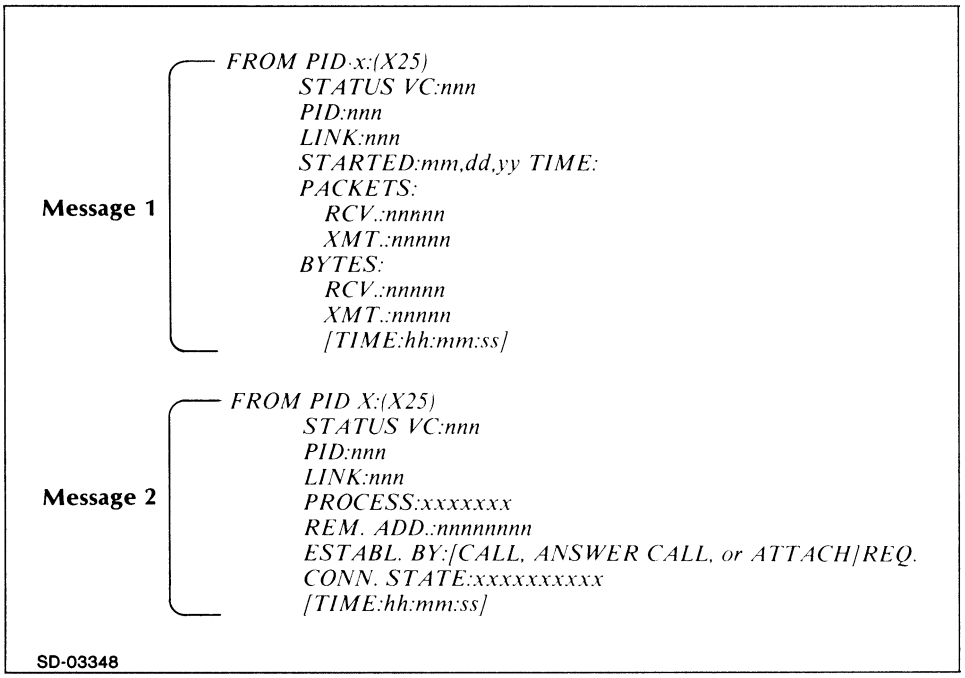


Figure 9-1. STATUS Message Formats

STATUS (continued)

Table 9-2. Connection States

Connection State	Meaning
ACCEPT CALL IN PROGRESS	The other side has put in a call, but X25 does not accept it until it receives the first read or write command from its customer.
ASSIGNED	Connected.
CLEAR WHEN POSSIBLE	Waiting to clear the connection.
OUTGOING CALL IN PROGRESS	X25 has sent out a call request on behalf of its customer, but has not received a confirmation from X25 on the remote host.
READY	The connection is established and is able to send and receive data.
WAITING FOR CLEAR CONFIRM.	X25 has sent out a clear request to close the connection. It is now waiting for an acknowledgement message from X25 on the remote host. X25's customer has acknowledged the close of the connection.
WAITING FOR CLEAR CONFIRM. AND ?NCLOSE	X25 has sent out a clear request to close the connection. It is now waiting for an acknowledgement message from X25 on the remote host. It is also waiting for its customer to acknowledge the close of the connection.

(continues)

Table 9-2. Connection States

Connection State	Meaning
WAITING FOR INCOMING CALL	X25 is currently available to accept an incoming call.
WAITING FOR ?NCLOSE	X25 is waiting to receive an acknowledgement for a request to close the connection from a customer.

(concluded)

STATUS (continued)

Command Switches

None.

Examples

The following STATUS command obtains statistics for virtual connection 12:

```
) CONTROL @X25 STATUS 12 ↓
) .
  .
  .
FROM PID  6 : (X25)
  STATUS VC:12 ;PID: 7  LINK: NBS_LCF
  ESTBL.: 6-JUN-85  TIME: 13:45:27
  PACKETS:  RCV.: 0  XMT.: 0
  BYTES:  RCV.: 0  XMT.: 0
  TIME:  12:08:15

) .
  .
  .
FROM PID  6 : (X25)
  STATUS VC:  12 ;PID: 7  ; LINK: NBS_LCF
  PROCESS: OP:RMA
  REM. ADD.: 18
  ESTBL. BY: ANSWER CALL REQ.
  CONN. STATE: WAITING FOR INCOMING CALL
  TIME:  12:08:15
```

The system responses show that virtual connection 12 was established on June 6, 1985 at 13:45:27. It has neither received nor transmitted any packets or bytes. It is being used by the RMA process, which established the connection by answering a call request. The address of the remote host is 18. The virtual connection is currently waiting for an incoming call.

The following command requests statistics about a virtual connection not in use:

```
) CONTROL @X25 STATUS 8 ↓
) .
  .
  .
FROM PID  6 : (X25)
  STATUS VC:  8
  VIRTUAL CALL INACTIVE
  TIME:  08:08:49
```

SVCMAX

Sets or displays the maximum number of concurrent switched virtual connections (SVCs).

Format

SVCMAX *[n]*

where

n is a decimal that represents the maximum number of concurrent SVCs.

Description

The SVCMAX command resets or displays the maximum number of concurrent SVCs.

To set the SVC maximum, enter the command with an argument. To display the SVC maximum, enter it without an argument.

Command Switches

None.

Examples

The following command displays the maximum number of concurrent SVC's:

```
) CONTROL @X25 SVCMAX ↓
) .
  .
  .
FROM PID  12: (X25)
  SVCMAX REPORT
  MAX NO. OF CONCURRENT SVC'S:  12
  TIME:  12:13:47
```

The following command sets the maximum number of concurrent SVCs to 14:

```
) CONTROL @X25 SVCMAX 14 ↓
) .
  .
  .
FROM PID  12: (X25)
  SVCMAX REPORT
  MAX NO. OF CONCURRENT SVC'S RESET TO:  14
  PREVIOUS VALUE:  12
  TIME:  12:14:00
```

TIMEOUT

Sets or displays the X25 time-out period.

Format

TIMEOUT *[n]*

where

n is, in seconds, the default time period X25 will allow in processing a customer's request.

Description

The TIMEOUT command sets or displays the default for the X25 time-out period. The time-out period specifies how long X25 will keep a customer's request. A process that uses X25 can accept the default or sets its own time-out period.

To set the time-out period, enter the command with an argument. To display the current time-out period, enter the command without an argument.

Command Switches

None.

Examples

The following command displays the current time-out value:

```
) CONTROL @X25 TIMEOUT ⤸
) .
  .
  .
FROM PID  12: (X25)
  TIMEOUT REPORT
  REQUEST TIMEOUT VALUE:  8 SECONDS
  TIME:  12:17:24
```

This next command resets the current time-out value to 3 seconds:

```
) CONTROL @X25 TIMEOUT 3 ⤸
) .
  .
  .
FROM PID  12: (X25)
  TIMEOUT REPORT
  REQUEST TIMEOUT VALUE RESET TO: 3 SECONDS
  PREVIOUS VALUE:  8 SECONDS
  TIME:  12:17:44
```

TRACE

Starts a trace.

Format

TRACE*[/switches]* pathname

where

pathname identifies the file to which you want packet images copied.

Description

This command directs X25 to dump images of the packets received and transmitted on the network to a file that you specify. Examining these packet images gives you information about network activity.

The trace file whose pathname you specify must not yet exist. Only one trace file can be open at a time, since only one trace can be in operation at a time. If you issue a second TRACE command, it terminates the current trace and begins a new one. To turn a trace off, you use the NOTRACE command.

The NTRACE program allows you to examine the contents of a trace file. Appendix B describes that program.

Command Switches

/GLOBAL	Traces all packets on the network. This is the default setting.
/LINK=linkname	Traces all packets on the link specified by linkname.
/PID=pid-no	Traces connections owned by the process that pid-no specifies.
/VC=vc-no	Traces the virtual connection specified by vc-no.

Examples

The following command dumps images of all packets on the network to the file, UDD:SAL:PACKETS:

```
) CONTROL @X25 TRACE :UDD:SAL:PACKETS ↵
) .
  .
  .
FROM PID 10  : (X25)
  TRACE ON
  TIME:  17:41:32
```

TRACE (continued)

The next command dumps packet images of all of PID 5's virtual connections to a file called PID5PACK:

```
) CONTROL @X25 TRACE/PID=5 PID5PACK ↓
) .
  .
  .
  FROM PID  10 : (X25)
    TRACE ON
    TIME:  17:41:03
```

This command dumps packet images of virtual connection 12 to a file called VC12PACK:

```
) CONTROL @X25 TRACE/VC=12 VC12PACK ↓
) .
  .
  .
  FROM PID  10 : (X25)
    TRACE ON
    TIME:  17:42:52
```

End of Chapter

Chapter 10
Using NETOP with XTS

The XODIAC Transport Service (XTS) is a process that implements the X.25 protocol on AOS/VS systems. XTS manages communication between Data General hosts, connects Data General hosts to public or private networks, breaks data into packets, sends packets on their network routes, and performs error checking. The agent processes, RMA, FTA, and SVTA, depend on XTS for communications functions.

Running X.25 on an Intelligent Controller

XTS gives you the option of running the X.25 portion of its program on an intelligent controller, such as an ISC or ILC, rather than on the main CPU. In this way, you can decrease the processing load on the CPU by offloading the work of connection management onto the controller.

You can run X.25 on a controller only if you have configured it to do so. When you configure an intelligent controller, NETGEN's Device Configuration screen asks, *Run X25 on this controller?* If you want to run X.25 on the controller, answer Y. Note that this answer simply permits you to run X.25 on the controller. It does not actually cause it to run there.

The XTS ENABLE command opens a link for use. It also specifies the device whose X.25 program owns (that is, does the processing for) the link. The device can be the host CPU or an intelligent controller that has been configured to run X.25. If you include the /X25=devicename switch, you designate the specified controller as the owner of the link. XTS checks whether X.25 is currently running on the controller. If it is not, XTS loads X.25 onto the controller.

Note that any X.25, whether running on the host or on an intelligent controller, can own any link. This means that an intelligent controller's X.25 can own a link that has been configured on a different controller, either intelligent or nonintelligent. This flexibility has an effect on disabling the links. When you disable the last XTS link on a controller, XTS relinquishes the controller, so that other protocol implementations (such as TCP/IP) can use it. If you have X.25 running on a controller, XTS relinquishes the controller only after you have

- disabled all XTS links on the controller, and
- disabled all XTS links on other controllers that this controller's X.25 owns.

Nonintelligent controllers, such as NBAs and MCAs, are controlled by the host, and cannot run X.25.

Using XTS Commands

As a network operator, you control certain aspects of the XTS process. Table 10-1 lists the XTS commands and tells what you use each command to do.

Table 10-1. XTS Commands

Command	Operator Function
DISABLE	Discontinue use of a link.
DUMP	Dump the memory of an intelligent controller or XTS on a host.
ENABLE	Make a link available for use.
HALT	Terminate the XTS process.
LIST	Display a list of the resources that XTS currently controls.
PARAMETERS	Set or display the maximum number of connections, the default time-out period for user programs, and the state of accounting.
RESTART	Restart a link, clearing all of its active virtual connections.
SET	Set parameters that determine how NETOP reports communication from XTS to you.
START	Start the XTS process.
STATISTICS	Display statistics about XTS usage on a link.
STATUS	Display information on XTS resources on a device or link.
TRACE	Start, stop, or display the state of tracing.

XODIAC Transport Service (XTS) Command Dictionary

The following section describes the NETOP commands for XTS. The commands are in alphabetical order and include examples. You can use unique abbreviations for the commands and their switches.

Examples show the XTS response to commands, but not the NETOP response. The examples assume that you are entering the commands from the console that receives system output. You can reset the destination console for output by using the SET command.

To use one of the commands in this section, enter it as an argument to the CLI CONTROL command, using the following format:

```
CONTROL @XTS command-name
```

You can also use the CXTS macro, as follows:

```
) CXTS command-name ↓
```

Link Names and Device Names

The name of a link is the filename of the link configuration file (LCF). The name of a device is the filename of the device configuration file (DCF). These names are assigned during a NETGEN session.

DISABLE

Discontinues use of a link.

Format

DISABLE *[linkname]*

where

linkname is the name of a link.

Description

This command discontinues use of a link that the ENABLE command has previously opened for use. XTS disables the link by closing all connections on the link and notifying user processes.

With a link name, the command disables that link only. Without a link name, the command disables all links. You can use the LIST command to get information on the links before you disable them.

If you disable the last XTS link on a nonintelligent controller, XTS relinquishes ownership of the controller. If you are running X.25 on an intelligent controller, XTS relinquishes ownership of the controller when you have

- disabled all XTS links on the controller, and
- disabled all XTS links on other controllers that this controller's X.25 owns.

To re-establish XTS ownership of the controller, you must re-enable the link.

Command Switches

None.

Examples

The following command disables link NBS_LCF:

```
) CONTROL @XTS DISABLE NBS_LCF ↓
) .
  .
  .
FROM PID  8 : (XTS)
  DISABLE REPORT
  NBS_LCF
  WAS DISABLED

  TIME: 10:16:12  ;24-OCT-1985
```

In the next example, the LIST command displays information about the active links. Next, the DISABLE command uses the default to disable all active links.

```
) CONTROL @XTS LIST/LINK ↓
) .
  .
  .
FROM PID  8 : (XTS)
  LIST LINKS
  X25 ON HOST
  NBS_LCF
  X25 ON ILC_DCF
  ILC_DCF

  TIME: 10:16:12  ;24-OCT-1985

) CONTROL @XTS DISABLE ↓
) .
  .
  .
FROM PID  8 : (XTS)
  LINK DISABLE REPORT
  ALL LINKS WERE DISABLED

  TIME: 10:17:43  ;24-OCT-1985
```

DUMP

Dumps the memory of the host or controllers.

Format

DUMP/FILE=filename [*devicename* | *HOST*]

where

devicename is the name of a intelligent controller.

HOST refers to XTS running on the host.

Description

This command copies to a file an XTS memory dump from either an intelligent controller or the host. The mandatory /FILE switch specifies the pathname of the dump file. When you dump an intelligent controller, XTS appends to the filename an underscore and the device code assigned to the controller through NETGEN.

To dump the memory of an intelligent controller, specify its device name as an argument. If you do not specify a device name, XTS dumps all active controllers. A controller dump disassociates the controller from XTS. To dump the memory of XTS on the host, use the argument, HOST.

Include a copy of the dump file when you submit a Software Trouble Report to Data General.

Command Switches

/FILE=filename Writes the dump to the filename you specify.

Examples

The following command dumps the contents of the memory of an ISC controller to the file, DUMPFILE:

```
) CONTROL @XTS DUMP/FILE=DUMPFILE ISC_DCF )
) .
  .
  .
FROM PID  8 : (XTS)
  DUMP CONTROLLER REPORT
  ISC_DCF
  WAS DUMPED

  TIME: 12:15:03  ;10-OCT-85
```

The dump file will have the name, DUMPFILE_devicecode.

The following command copies memory of XTS running on the host to the file, INFO:

```
) CONTROL @XTS DUMP/FILE=INFO HOST ↵
) .
  .
  .
FROM PID  8 : (XTS)
  DUMP CONTROLLER REPORT
  HOST
  WAS DUMPED

  TIME: 12:17:23  ;10-OCT-85
```

The dump file will have the name, INFO.

ENABLE
Allows the use of a link.

Format

ENABLE*[/X25=devicename]* linkname

where

linkname is the name of a link.

Description

This command directs XTS to open a link, making it available for XTS communications. The command also gives control of the link to the X.25 program on the host or an intelligent controller.

The /X25 switch specifies the device that will own (control) the link. You can specify an intelligent controller whose NETGEN device configuration file allows it to run X.25, or the literal, HOST. One controller can be the owner of a link on another controller.

If you enter the ENABLE command without the /X25 switch, the owner of a link on a nonintelligent controller is always the host. The owner of a link on an intelligent controller is determined by that controller's device configuration file, as follows:

- If the device configuration file allows the controller to run X.25, the controller will own the link.
- If the device configuration file does not allow the controller to run X.25, the host will own the link.

Command Switches

/X25=devicename — Specifies the device whose X.25 program will own the link. The device name is the name of an intelligent controller or the literal, HOST.

Examples

The following command enables ISC_LCF for use with X.25 on the ISC device, ISC_DCF:

```
) CONTROL @XTS ENABLE ISC_LCF ↓
) .
  .
  .
FROM PID  8 : (XTS)
  ENABLE REPORT
  isc_lcf
  TRANSPORT:       X25
  CONTROLLER: ISC_DCF
  TIME: 14:02:15  ;15-OCT-1985
```

The following command enables ISC_LCF for use with X.25 on the host computer:

```
) CONTROL @XTS ENABLE/X25=HOST ISC_LCF ↓
) .
  .
  .
FROM PID  8 : (XTS)
  ENABLE REPORT
  isc_lcf
  TRANSPORT:       X25
  CONTROLLER:      HOST

  TIME: 14:04:25  ;15-OCT-1985
```

HALT

Terminates the XTS process.

Format

HALT*[/WAIT]*

Description

The HALT command sends a message to users, disables all links, and terminates the XTS process.

If you omit the /WAIT switch, the command takes effect immediately. If you use the /WAIT switch, XTS denies new requests for connections, but it allows existing connections to clear normally. It terminates only when all connections are clear.

Command Switches

/WAIT Delays termination until all connections have cleared normally.

Examples

The following command halts the XTS process but allows existing connections to clear:

```
) CONTROL @XTS HALT/WAIT ↓
) .
  .
  .
FROM PID  8 : (XTS)
  HALT REPORT

  TIME: 16:21:22;  02-OCT-85
```

This command immediately halts the XTS process:

```
) CONTROL @XTS HALT ↓
) .
  .
  .
FROM PID  8 : (XTS)
  HALT REPORT

  TIME: 16:22:23;  02-OCT-85
```

LIST
Lists XTS resources.

Format

```
LIST { /CONNECTIONS  }
     { /CONTROLLERS  }
     { /CUSTOMERS    }
     { /LINKS        }
```

Description

The LIST command displays a list of the resources that XTS currently controls. The command requires a single switch.

Command Switches

/CONNECTIONS	Lists the active connections, and tells what X.25 program is managing the connection.
/CONTROLLERS	Lists active controllers. The list returned distinguishes between *controllers* (that is, intelligent controllers) and *devices*, (that is, both intelligent and nonintelligent controllers).
/CUSTOMERS	Lists XTS users by PID number.
/LINKS	Lists active links, and the device that owns each link.

Examples

The following LIST command with the /CONTROLLERS switch displays a list of active intelligent controllers and a list of all active devices:

LIST (continued)

```
) CONTROL @XTS LIST/CONTROLLERS ↓
) .
  .
  .
FROM PID  8 : (XTS)
  LIST CONTROLLERS
  ACTIVE CONTROLLERS:
  ILC_DCF
  ISC_DCF

  TIME: 08:14:35  ;10-OCT-85

FROM PID  8 : (XTS)
  LIST CONTROLLERS
  ACTIVE DEVICES:
  NBS_DCF
  ILC_DCF
  ISC_DCF

  TIME: 08:12:37  ;10-OCT-85
```

The next command displays a list of active links running under XTS. The command report shows two links: nbs_lcf running X.25 on the host, and ilc_lcf running X.25 on ILC_DCF.

```
) CONTROL @XTS LIST/LINKS ↓
) .
  .
  .
FROM PID  8 : (XTS)
  LIST LINKS
  X25  ON  HOST
  nbs_lcf
  X25  ON  ILC_DCF
  ilc_lcf

  TIME: 08:12:45  ;10-OCT-85
```

The last command displays a list of currently open connections:

```
) CONTROL @XTS LIST/CONNECTIONS ↓
) .
  .
  .
FROM PID  8 : (XTS)
  LIST CONNECTIONS
  X25  ON  ILC_DCF
  2
  3
  4

  TIME: 08:12:85  ;05-OCT-85
```

PARAMETERS
Sets or displays parameters for the XTS program.

Format

PARAMETERS { /RCONNECTIONS[=n] | /LCONNECTIONS[=n] | /GCONNECTIONS[=n] } devicename

or

PARAMETERS { /TIMEOUTS[=n] | /ACCOUNTING [=ON | =OFF] }

where

devicename is the name of a device.

Description

This command sets or displays parameters for the XTS program. The parameters are the maximum number of connections for a given XTS, the default time-out period for user programs, and XTS accounting.

You can set only one parameter at a time with this command. This means that a PARAMETERS command line must have exactly one switch.

Using this command, you can set or display the maximum number of concurrent virtual connections permitted for the specified device. The /RCONNECTIONS switch applies to routed connections, the /LCONNECTIONS switch applies to local connections, and the /GCONNECTIONS switch applies to global connections. If you use one of these switches with an n value, you set the maximum number of connections. If you omit the n value, you display the current maximum. The system response looks the same whether you set or display the value.

The /TIMEOUTS=n switch sets, in seconds, the default time-out period for X.25 customer processes defined in the X.25 user interface. Such processes can accept the default value or they can set their own time-out period. When sending data long distances through a public data network, you may want to increase this time-out period. Using /TIMEOUTS without an n value displays the current default.

The /ACCOUNTING switch turns accounting ON or OFF. If accounting is ON, XTS places all accounting and exception information in the system log file. To display the contents of the system log file, you use the REPORT program, which is explained in *How to Generate and Run AOS/VS*. Appendix A shows the log file parameters for X.25 information. Accounting logs exception

PARAMETERS (continued)

information as errors occur. It also logs accounting information for a virtual connection when the connection is cleared. If you use /ACCOUNTING without ON or OFF, you display whether accounting is currently on or off.

Command Switches

/ACCOUNTING[=ON / =OFF] — Sets or displays the current state of accounting. /ACCOUNTING=ON turns accounting on. /ACCOUNTING=OFF turns accounting off. /ACCOUNTING displays whether accounting is on or off.

/GCONNECTIONS*[=n]* — With an *n* value, sets the number of global (that is, routed plus local) connections for an X.25 program. Without an *n* value, displays the number of global connections.

/LCONNECTIONS*[=n]* — With an *n* value, sets the number of local connections for an X.25 program. Without an *n* value, displays the number of local connections.

/RCONNECTIONS*[=n]* — With an *n* value, sets the number of routed connections for an X.25 program. Without an *n* value, displays the number of routed connections. Note that this parameter applies only if the host is the routing host, not the end host.

/TIMEOUTS*[=n]* — With an *n* value, sets the default timeout period for X.25 customer processes. Without an *n* value, displays the current default.

Examples

The following PARAMETERS command uses the /RCONNECTIONS switch to display the number of routed connections for the controller ILAN_DCF.

```
) CONTROL @XTS PARAMETERS/RCONNECTIONS ILAN_DCF ↵
) .
  .
  .
FROM PID  12 : (XTS)
  PARAMETER REPORT

  FOR DEVICE:  ILAN_DCF
  ROUTED CONNECTIONS:  64
  TIME: 05:45:34;  08-23-85
```

This next command sets the timeout period to 15 seconds.

```
) CONTROL @XTS PARAMETERS/TIMEOUT=15 ↵
) .
  .
  .
FROM PID  12 : (XTS)
  PARAMETER REPORT

  TIMEOUT VALUE:  15
  TIME: 05:45:34;  08-23-85
```

RESTART

Restarts a link.

Format

RESTART { hostname | linkname/NODE=node-id }

where

hostname is the name of a host.

linkname is the name of a link.

node-id is a physical address of the controller on a remote host. The **node-id** notation depends on the device it represents and can be octal or hexadecimal. A hexadecimal **node-id** must have 12 digits. An octal **node-id** must have fewer than 12 digits. A **node-id** of −1 will clear all connections on the link.

Description

The RESTART command restarts a link and clears all of its active virtual connections. The RESTART command is useful for debugging purposes.

With a host name as an argument, the RESTART command affects the active link that has first priority for that host, according to your NETGEN specification file. For more information, refer to the section on configuring remote hosts in Chapter 4.

With a link name and its (mandatory) /NODE switch as an argument, the RESTART command affects the particular link to the particular node that you specify.

Note that if your connection to the remote host is through a routing host, the RESTART command passes to the routing host. In this case, the command clears all connections between the routing host and the hosts to which it connects.

Command Switches

None.

Example

The following command restarts the active link with first priority on the host ADMIN. The command report gives the link name, ILC_LCF.

```
) CONTROL @XTS RESTART ADMIN ↓
) .
  .
  .
FROM PID  12 : (XTS)
  RESTART REPORT
  LINK: ilc_lcf
  REMOTE STATION ADDRESS:  2

  TIME: 05:45:34;  08-23-85
```

SET

Sets conditions for logging and message reporting.

Format

SET*[/switches]*

Description

This command sets internal NETOP parameters that determine the nature and destination of system response messages. You can use the SET command before starting XTS or at any subsequent time.

Normally, the console of NETOP's father process displays XTS reports. You can change the destination console for reports by using the /OUTPUT switch. If NETOP is unable to send a message to the terminal that you specify, it resets the destination to the console of its father process . If NETOP encounters an error while sending a message to that console, however, the message will be lost.

You can also send reports to a log file by using the /LOG switch.

Command Switches

/DATE	Includes the date with all reports.
/LOG*[=logfile]*	Enables logging and creates a new log file. Without an argument, the log file has a default pathname, and is in the directory :NET:LOGFILES. With an argument, the log file name and directory are those that you specify in a fully qualified pathname.
/NODATE	Suppresses the date in reports. This is the default.
/NOLOG	Disables logging.
/NOOUTPUT	Disables console display of reports.
/NOPROMPT	Suppresses the following NETOP prompt: *FROM PID n : (NETOP)* *TIME: nn:nn:nn*
/NOTIME	Suppresses the time in reports.

/OUTPUT [=*console-name* | =*pid-no* | *process-name*] — Specifies the destination console for reports. Without an argument, reports go to the console of NETOP's father process. With an argument, reports go to the console specified by *console-name*, or the console owned by the process specified by *pid-no* or *process-name*.

/PROMPT — Includes the NETOP prompt. This is the default setting.

/TIME — Includes the time in NETOP messages. This is the default setting.

Examples

The following SET command causes messages to include the time. While the SET command gives no report, the ENABLE command report includes the time.

```
) CONTROL @XTS SET/TIME ↵
) CONTROL @XTS ENABLE NBS_LCF ↵
) .
  .
  .
FROM PID  10 : (XTS)
  LINK ENABLE REPORT
  nbs_lcf
  TRANSPORT:  X25
  TIME: 13:27:34
```

The following command causes XTS messages to go to PID 5:

```
) CONTROL @XTS SET/OUTPUT=5 ↵
```

The last command sends responses to the file :COMLOG:OCT29:

```
) CONTROL @XTS SET/LOG=:COMLOG:OCT29 ↵
```

START
Starts XTS.

Format

START*//switches]*

Description

This command starts the XTS process. You can run only one XTS process at a time. By default, XTS is a resident process, and must be resident unless your system includes only MCA and/or asynchronous devices. You cannot issue another START command until after you have terminated XTS by using the HALT command.

If an error occurs when NETOP attempts to start XTS, NETOP sends a termination message that includes XTS's PID number and the reason for termination.

Command Switches

/NODUMP	Suppresses the dump option. By default, AOS/VS creates a memory dump of XTS in :NET if the process terminates abnormally.
/PREEMPTIBLE	Initiates XTS as a pre-emptible process. You can use this switch if your system includes only MCA and/or asynchronous devices.
/PRIORITY=n	Sets the initial priority for the XTS process to n. The default priority is 2.
/RESIDENT	Starts XTS as a resident process. This is the default setting, and XTS must be resident unless you are running only MCA and/or asynchronous devices.
/SWAPPABLE	Starts XTS as a swappable process. You can use this switch if your system includes only MCA and/or asynchronous devices.
/WSMAX=x	Sets the maximum working set size to x.
/WSMIN=y	Sets the minimum working set size to y.

These switches relate to operating system concepts explained in the *Advanced Operating System/Virtual Storage (AOS/VS) Programmer's Manual*, Volumes I and II.

Examples

The following command starts XTS as a resident process:

```
) CONTROL @XTS START ↓
) .
  .
  .
FROM PID  7 : (XTS)
  STARTED
  PID =  12
  TIME: 16:05:17  ;06-OCT-1985
```

STATISTICS

Reports XTS usage statistics.

Format

STATISTICS { /LINK[/*RESET*] / /X25[/*RESET*] } linkname

where

linkname is the name of a link.

Description

The STATISTICS command displays information about XTS usage on a link that you specify. The statistics that the command displays vary according to the type of link you specify. You must use a switch. The /LINK switch displays link-layer statistics; the /X25 switch displays network-layer statistics. The command report includes the name of the device that owns the link.

Command Switches

/LINK Reports link-layer statistics.

/RESET Resets the statistics accumulators to zero; affects link-layer or network-layer statistics, depending on the other switch you use. You must use this switch in conjunction with one of the other switches.

/X25 Reports network-layer statistics.

Examples

The following STATISTICS command displays link statistics for the link, ilc_lcf:

```
) CONTROL @XTS STATISTICS/LINK ilc_lcf ↓
) .
  .
  .
FROM PID  7 : (XTS)
  LINK STATISTICS
  ilc_lcf
  FRAMES TRANSMITTED:        4202
  FRAMES RECEIVED:           4162
  BYTES TRANSMITTED:         873924
  BYTES RECEIVED:            35564
  FRAMES RETRANSMITTED:      32
  TRANSMIT ERRORS:           0
  RECEIVE ERRORS:            0
  TIME SINCE LAST RESET:     20960
  TIME: 18:21:32  ;12-OCT-85
```

The next STATISTICS command has the /X25 switch. The command displays the network-layer statistics for X.25.

```
) CONTROL @XTS STATISTICS/X25 ilc_lcf ↓
) .
  .
  .
FROM PID  7 : (XTS)
  X25 STATISTICS
  ILC_DCF
  LINK: ilc_lcf

  PACKETS SENT:              2413
  PACKETS RECEIVED:          1639
  BYTES SENT:                848589
  BYTES RECEIVED:            14329
  ACTIVE CONNECTIONS:        1
  ACTIVE NODE PAIRS:         3
  CONNECTION NUMBERS:
  2,
  TIME: 18:21:32;  29-OCT-1985
```

STATUS

Reports information on XTS resources.

Format

STATUS { /CONTROLLER *[devicename]* | /X25 *[devicename]* | /LINK *[linkname]* }

where

devicename is the name of an intelligent controller configured by NETGEN, or the literal, HOST.

linkname is the name of a link configured by NETGEN.

Description

The STATUS command returns information about the XTS resources that you specify.

You must enter a switch with the command. Each switch specifies a resource type. Without an argument, the command displays information on all devices or links associated with the resource type. Enter the command with an argument to obtain information on a specific device or link. The argument, *devicename*, can be an intelligent or nonintelligent controller, or the literal, HOST.

Command Switches

/CONTROLLER Reports on the intelligent controller(s).

/X25 Reports on X.25 programs.

/LINK Reports on the link(s).

Examples

The following command obtains a report on the X.25 program on the controller, ILC_DCF:

```
) CONTROL @XTS STATUS/X25 ILC_DCF ↵
) .
  .
  .
FROM PID 7 : (XTS)
  X25 STATUS
  ILC_DCF
  CONTROLLER TYPE:              ILC CONTROLLER
  CONTROLLER STATE:             READY
  ENTITY TYPES:
    LINK
    X25
  TIME: 13:15:31   ;05-OCT-l985
```

The response shows the controller type, and tells that the controller is in the ready state. It also lists the active entity types on the controller. An entity is a functional unit of code. The X25 entity implements the X.25 protocol, and the link entity manages the link.

The next command displays a report on the link, ilc_lcf:

```
) CONTROL @XTS STATUS/LINK ilc_lcf ↵
) .
  .
  .
FROM PID  7 : (XTS)
  LINK STATUS
  ilc_lcf
  TRACE: ON
  ASSOCIATED DEVICE:
  ILC_DCF
  NETWORK TYPES CONTROLLING THIS LINK:
  ILC_DCF X25

  TIME: 13:15:31   ;12-OCT_l985
```

TRACE

Sets or displays the current status of tracing.

Formats

The first formats turn X25 tracing ON and OFF:

TRACE/X25/ON/LINK=linkname filename

TRACE/X25/OFF [*/ID=tracenumber* | */LINK=linkname*]

The second pair of formats turn link-level tracing ON and OFF:

TRACE/ON/LINK=linkname [*/MATCH=* { *x/MASK=y* | *DISK* | *DM* | *FRMR* | *SABM* | *SARM* } *[/DELAY=n]* [*/RECEIVED* | */SEND*]] filename

TRACE/OFF [*/ID=tracenumber* | */LINK=linkname*]

The last format displays the status of tracing:

TRACE { /LINK=linkname | /X25/LINK=linkname }

All TRACE formats use these values, where

filename	is the name of the trace file.
linkname, *linkname*	is the name of a link.
n	is the number of frames to trace after a match is made.
DM, DISC, FRMR, SABM, and *SARM*	are HDLC frame types.
tracenumber	is the identifier for a trace. XTS displays this number when you start a trace.
x	is a four-digit hexadecimal number that represents the address and control bytes of a frame that you want to match.
y	is a four-digit hexadecimal number whose binary equivalent is the pattern for matching a frame.

Description

The TRACE command starts and stops tracing, or displays whether tracing is ON or OFF. When tracing is ON, XTS puts images of data received and transmitted over the network in the specified file. Examining the contents of this file gives you information about network activity. Two types of traces are available: network-layer (or X.25) tracing, and link-layer tracing. A network-layer trace is for packets; a link-layer trace is for frames.

To start a network-layer trace, use TRACE/X25/ON, with the /LINK switch to specify the link whose packets you want to trace. The trace filename is the argument to the command.

To stop a network-layer trace, use TRACE/X25/OFF if only one X25 trace is on. If more than one is on, include the /ID switch or the /LINK switch. The argument for /ID is the trace number that XTS displayed when you started the trace. The argument for /LINK is the link name.

To start a link-layer trace, use TRACE/ON with the /LINK switch to specify the link whose frames you want to trace. You can, optionally, use the /MATCH switch to trace a particular frame. When XTS comes across the frame, the trace stops. The frame that you specify as an argument to the /MATCH switch can be a standard HDLC frame (DM, DISC, FRMR, SABM, or SARM), or a frame that you specify (x). If you specify a frame, use the /MASK=y switch to specify the pattern for the match. A zero (0) bit in the y value's binary equivalent can be ignored, while a 1 bit must be matched. The /DELAY switch allows the trace to continue for n frames after the match occurs. Finally, the filename for the trace file is a mandatory argument. The file must not yet exist.

To stop a link-layer trace, you can simply enter TRACE/OFF if only one link-layer trace is on. If more than one is on, use the /ID or /LINK switch. The argument for /ID is the trace number displayed when you started the trace. The argument for /LINK is the link name.

To display the current status of link-layer tracing, enter TRACE/LINK=linkname. To display the current status of network-layer tracing, enter TRACE/X25/LINK=linkname.

To display the contents of a network-layer trace file, you use the NTRACE facility that Appendix B describes. To display the contents of a link-layer trace file, consult your Data General representative.

TRACE (continued)

Command Switches

/ID=tracenumber	Identifies a trace; XTS displays this identifier when it starts the trace.
/LINK=linkname	Specifies a link on which XTS traces data.
/MATCH={ x/MASK=y | DM | DISC | FRMR | SABMC | SARM }	Stops a link-layer trace when the specified frame is found. DM, DISC, FRMR, SABM, and SARM are standard HDLC frames; x is a frame to which you apply a bit mask specified by the /MASK=y switch. Both x and y are four-digit hexadecimal numbers. The x value represents the address byte and control byte of the frame; the y value's binary equivalent is the pattern for the matching operation.
/ON	Starts a trace.
/OFF	Stops a trace. When only one trace exists, this can be the only switch. When multiple traces exist, you must use the /ID or /LINK switch.
/RECEIVE	Limits a link-layer trace to incoming frames.
/SEND	Limits a link-layer trace to outgoing frames.
/X25	Specifies a network-level trace.

Examples

The following command starts a packet-level trace on the link, ISC_LCF, and creates the trace file, :UDD:MARG:PKTS:

```
) CONTROL @XTS TRACE/ON/X25/LINK=ISC_LCF   :UDD:MARG:PKTS ↓
) .
  .
  .
FROM PID  10 : (XTS)
  X25 TRACE
  TRACE STATE:  ON
  TRACE ID:     1
  TIME: 17:41:32  ;20-OCT-1985
```

The command report includes the trace ID number, 1.

The following command starts a link-level trace on the link, ISC_LCF, and creates the trace file, :UDD:TIM:FRAMES.

```
) CONTROL @XTS TRACE/ON/LINK=ISC_LCF   :UDD:TIM:FRAMES ↓
) .
  .
  .
FROM PID  10 : (XTS)
  LINK TRACE
  TRACE STATE:  ON
  TRACE ID:     2

  TIME: 17:41:32  ;15-OCT-1985
```

End of Chapter

Chapter 11
Using NETOP with RMA

The Resource Management Agent (RMA) provides authorized users and programs with direct access to resources on remote hosts in the network. URMA handles local users' outgoing requests for remote resources. SRMA handles incoming requests from remote users for local resources. A single RMA process implements both URMA and SRMA on a host.

As a network operator, you control certain aspects of RMA. Table 11-1 lists the RMA commands and tells what you use each command to do.

Table 11-1. RMA Commands

Command	Operator Function
ACCOUNT	Start XTS accounting in the system log file.
CONNECTIONS	Set or display a limit on URMA connections.
DISABLE	Stop RMA servicing of user requests.
ENABLE	Start RMA servicing of user requests.
MAXBUFFER	Set or display the maximum size of incoming data buffers (AOS only).
NOACCOUNT	End RMA accounting in the system log file.
RESET	Reinitialize statistics accumulators.
SET	Set parameters that determine how NETOP manages communication from RMA to you.
START	Start the RMA process. (This command includes an implicit ENABLE.)
STATUS	Display RMA usage statistics.
SURROGATES	Set or display a limit on surrogate processes.
TERMINATE	Stop RMA from serving a specified process. (This command does not terminate the RMA process.)
TIMEOUT	Set or display the length of time that a surrogate process exists.

For a discussion of the user interfaces to RMA and definitions of RMA terms, refer to the manual, *Using the XODIAC Network Management System.*

Resource Management Agent (RMA) Command Dictionary

The following pages include descriptions of all the operator commands for RMA. The command descriptions are in alphabetical order and include examples. You can use unique abbreviations for all commands and keywords.

In examples, we show both the command you give and the system response, assuming that you are entering the commands from the console that receives system output. You can reset the destination console for output by using the SET command.

To use one of the commands in this section, enter it as an argument to the CLI CONTROL command, using the following format:

```
CONTROL @RMA command-name
```

You can also use the CRMA macro, as follows:

```
CRMA command-name
```

Link Names and Device Names

The name of a link is the filename of the link configuration file (LCF). The name of a device is the filename of the device configuration file (DCF). These names are assigned during a NETGEN session.

ACCOUNT

Turns on accounting.

Format

ACCOUNT

Description

This command directs RMA to start accounting. When accounting is on, information on RMA's services to each user is entered in the system log file. You can use the accounting information for billing purposes or system load analysis.

Accounting is normally off when an RMA process starts running; you must explicitly turn it on with the ACCOUNT command or by adding the /ACCOUNT switch to the ENABLE command. If accounting is already on when you issue one of these commands, you simply receive a confirmation. To turn accounting off, you can issue the NOACCOUNT command.

The REPORT program lets you display the contents of the system log file. Refer to *How to Generate and Run AOS/VS* or *How to Generate and Run AOS* for information on the REPORT program. Appendix B shows the X.25 parameters for the log file.

Command Switches

None.

Example

The following command starts accounting:

```
) CONTROL @RMA ACCOUNT ↓
) .
  .
  .
FROM PID  6 : (RMA)
  ACCOUNTING ON
```

CONNECTIONS

Sets or displays the maximum number of virtual connections for URMA.

Format

CONNECTIONS [/CUSTOMER | /GLOBAL] [n]

where

n is a decimal number in the range 1–50. An argument of –1 is equivalent to the default setting, 20.

Description

The CONNECTIONS command sets or displays the number of virtual connections that URMA can establish. This command, therefore, limits the local resources available to support user access to remote resources.

To set the connections limit, enter the command with a value as an argument. To display the current limit, enter the command without an argument.

The /CUSTOMER switch sets or displays the limit for any one customer process. The /GLOBAL switch sets or displays the limit for all customer processes.

Command Switches

/CUSTOMER	Sets or displays the number of virtual connections that any one URMA customer process can establish. This is the default.
/GLOBAL	Sets or displays the total number of virtual connections that all URMA customer processes can establish.

Example

The following command sets the customer connection limit to 10:

```
) CONTROL @RMA CONNECTIONS 10 ↓
) .
  .
  .
FROM PID  6 : (RMA)
  CUSTOMER CONNECTION LIMIT
  SET TO: 10
```

The command response shows the connection limit, and looks the same whether you set or display the limit.

DISABLE

Discontinues RMA servicing.

Format

DISABLE*[/switches]*

Description

This command allows you to stop URMA and/or SRMA from servicing user requests. It does not terminate RMA.

The DISABLE command disables both URMA and SRMA agents, unless you include either the /URMA or /SRMA switch. Each switch disables only that agent.

Command Switches

/SRMA Disables SRMA.

/URMA Disables URMA.

Example

The following command disables both SRMA and URMA:

```
) CONTROL @RMA DISABLE ↓
) .
  .
  .
FROM PID  6 : (RMA)
  DISABLE REPORT
  SRMA DISABLED
  URMA DISABLED
```

ENABLE

Makes URMA and/or SRMA servicing available.

Format

ENABLE*[/switches]*

Description

This command lets you make URMA and/or SRMA available. It can also turn on accounting functions. By default, the ENABLE command starts both URMA and SRMA; alternatively, you can enable only one of the agents by using the appropriate switch.

To start accounting, enter the /ACCOUNT switch, which is equivalent to the ACCOUNT command. Unless you use this switch, the ENABLE command disables accounting. If you try to start accounting when it is already on, you simply get a confirmation message.

Command Switches

/URMA	Enables URMA to service local user requests.
/SRMA	Enables SRMA to service remote user requests.
/ACCOUNT	Turns on accounting.

Example

The following command enables URMA and SRMA but disables accounting:

```
) CONTROL @RMA ENABLE ↓
) .
  .
  .
FROM PID  6 : (RMA)
  ENABLE REPORT
  URMA ENABLED
  SRMA ENABLED
```

MAXBUFFER

Sets or displays the maximum size of RMA incoming data buffers on AOS systems.

Format

MAXBUFFER *[n]*

where

n is a decimal number in the range 1024–4096 bytes. The argument, –1, is equivalent to the default value, 1024.

Description

The MAXBUFFER command, which applies only to AOS systems, sets or displays the size of RMA buffers for incoming data. While RMA has a fixed amount of buffer space, it can divide the space into partitions of varying size. By using this command to specify the size of each buffer, you also determine the number of buffers RMA can create.

RMA also has one large buffer which handles data that is too large for the incoming data buffers. Since there is only one such large buffer, requests may wait in line to use it, which slows their completion.

Large incoming buffers speed the completion of each request, but, since fewer buffers exist, they also limit the number of concurrent requests. Small incoming buffers allow more concurrent requests, but can result in slower processing of large requests that must wait for the single large buffer.

To set the maximum buffer size, enter the command with an argument. To display the maximum buffer size, enter the command without an argument.

Command Switches

None.

Example

The following command displays the maximum RMA buffer size:

```
) CONTROL @RMA MAXBUFFER ↓
) .
  .
  .
FROM PID  6 : (RMA)
  MAXIMUM I/O BUFFERSIZE
  SET TO: 1024
```

The command response shows the current value, and is the same whether you set or display the buffer size.

NOACCOUNT
Turns off accounting.

Format

NOACCOUNT

Description

This command directs the RMA process to turn the accounting function off.

Command Switches

None.

Example

The following command turns accounting off:

```
) CONTROL @RMA NOACCOUNT ↓
) .
  .
  .
FROM PID  6 : (RMA)
  ACCOUNTING OFF
```

RESET
Reinitializes global statistics accumulators.

Format

RESET

Description

The RESET command directs the RMA process to reinitialize the global statistics accumulators. The accumulators are normally reset to zero each time you bring up RMA.

You can also reinitialize these accumulators at the time you display the statistics, by adding the /RESET switch to the STATUS command.

Command Switches

None.

Example

The following command reinitializes the statistics accumulators:

```
) CONTROL @RMA RESET ↓
.
.
.
FROM PID  6 : (RMA)
  GLOBAL STATISTICS RESET
```

SET

Sets conditions for logging and message reporting.

Format

SET*[/switches]*

Description

This command sets internal NETOP parameters that determine the nature and destination of system response reports. You can use this command before starting RMA, or at any other time.

Normally, the console of NETOP's father process displays RMA reports. You can change the destination console for reports by using the /OUTPUT switch. If NETOP encounters an error while sending a report to the console you specify, it resets the destination to the console of its father process. If NETOP encounters an error in sending a report to that console, however, the report will be lost.

You can also send reports to a log file by using the /LOG switch.

Command Switches

/DATE	Includes the date in each report.
/LOG*[=pathname]*	Enables logging and creates a new log file. Without an argument, the file has a default pathname and is in the directory :NET:LOGFILES. If you include the pathname argument, you specify the filename and directory of the log file.
/NODATE	Suppresses the date in reports. This is the default.
/NOLOG	Disables logging.
/NOOUTPUT	Disables output of reports to a console.
/NOPROMPT	Suppresses the following NETOP prompt: *FROM PID n : (NETOP)* *TIME: nn:nn:nn*
/NOTIME	Suppresses the time in reports.

/OUTPUT [=*@console-name* | =*pid* | =*process-name*]	Specifies the destination console for reports. Without an argument, sets the destination for reports to the console of NETOP's father process. With an argument, sets the destination to *@console-name* or to the console owned by the *pid* or *process-name* that you specify.
/PROMPT	Restores the NETOP prompt.
/TIME	Includes the time in reports. This is the default.
/PARAMETERS	Displays the current RMA log file name and output destination.

Example

The following command displays the current parameters:

```
) CONTROL @RMA SET/PARAMETERS ↵
) .
  .
  .
FROM PID  6 : (RMA)

  PARAMETERS:

  LOGFILE =:NET:LOGFILES:RMA_12_15_80.LOG
  OUTPUT  = FATHER'S CONSOLE
```

START
Starts an RMA process.

Format

START*[/switches]*

Description

The START command tells NETOP to create the RMA process.

If an error occurs while NETOP is starting RMA, the error message goes to the console of NETOP's father process, unless you have previously used the SET command to specify a different output console.

This command enables both URMA and SRMA unless you use the /URMA or /SRMA switch to enable only that agent.

Command Switches

/ACCOUNT	Turns accounting on.
/NOACCOUNT	Disables accounting. This is the default.
/PREEMPTIBLE	Initiates RMA as a pre-emptible process.
/PRIORITY=n	Sets the initial priority for the RMA process to n. The default priority is 2.
/PROCESSORS=x	Creates a number (x) of message tasks for RMA, where x is in the range, 1–9. The default is 3. This switch applies to AOS systems only.
/RESIDENT	Initiates RMA as a resident process. This is the default setting.
/SRMA	Enables SRMA support for remote users.
/SWAPPABLE	Initiates RMA as a swappable process. This is the default switch.
/URMA	Enables URMA support for local users.
/WSMAX=y	Sets the maximum working set size for RMA. This switch applies to AOS/VS systems only.
/WSMIN=z	Sets the minimum working set size for RMA. This switch applies to AOS/VS only.

These switches relate to operating systems concepts explained in the programmer's manual for your operating system.

Example

The following command creates the RMA process, enabling both SRMA and URMA by default:

```
) CONTROL @RMA START ↓
) .
  .
  .
FROM PID  6 : (RMA)
  STARTED
  PID=6
  DATE: 27-FEB-1981
```

STATUS

Reports RMA usage statistics.

Format

STATUS*//RESET] [pid]*

where

pid is the process identifier number for a local or surrogate process.

Description

This command displays statistics about RMA activity. Without an argument, the STATUS command displays a global status report on the usage of local RMA. With a process identifier (PID) number as an argument, the command displays a report on the use of RMA by that process. You can specify the PID of a local or surrogate process.

The status report includes both current and total information. The totals represent activity since you last reinitialized the statistics accumulators by using the RESET command or the STATUS command with the /RESET switch.

Note that the time-out period affects these statistics, by varying the duration of surrogates, and thus, the duration of connections. Also, note that a customer-server relationship exists between RMA and its customer process, even after the customer process has stopped actively using RMA. The number of customers, therefore, can exceed the number of active RMA user processes.

The global status report is in three sections: global (total RMA use), URMA and SRMA. The first section contains the following global information:

STATUS INTERVAL	The time that has elapsed since you last issued the STATUS command.
CUSTOMERS	The current and total number of local processes that have requested RMA services.
SURROGATES	The current and total number of surrogate processes on this host.
VIRTUAL CIRCUITS	The numbers of the virtual connections currently serving RMA customer processes.

The second section of the global report contains the following information on URMA use:

CONNECTIONS	The current and total number of connections serving local customer processes.
DURATION	The cumulative time that URMA has been serving customer processes.

SYSTEM CALLS	The number of system calls deflected by URMA and sent to other hosts for processing.
BYTES TRANSMITTED and RECEIVED	The total bytes transmitted and received by URMA since the last statistics reset.
CUSTOMER LIST	The PIDs of active local URMA customers.

The third section of the global report contains the following information on SRMA use:

DURATION - SURROGATES	The total time that surrogate processes have existed.
SYSTEM CALLS	The total number of system calls that SRMA received and assigned to local surrogates.
BYTES TRANSMITTED and RECEIVED	The total bytes transmitted and received by SRMA since the last statistics reset.
SURROGATE LIST	The PIDs of active local surrogate processes.

If you give the STATUS command a PID argument, and the PID identifies a local customer of URMA, the status display includes the following information about that process:

PID	Its process identifier.
INITIAL ACCESS	The time when it first used RMA services.
CONNECTIONS - TOT.	The total connections it has made (one process can be using resources on a number of remote hosts through RMA).
SYSTEM CALLS	The number of system calls that URMA has passed to a remote process on its behalf.
BYTES TRANSMITTED and RECEIVED	The total bytes transmitted and received by URMA on its behalf.
VIRTUAL CIRCUITS	The numbers of the virtual connections it currently has open.

STATUS (continued)

If you give the STATUS command a PID argument, and the PID identifies a surrogate process (customer of SRMA), the status display includes the following information about the surrogate:

CUST. PID	The PID of the remote customer whose RMA request resulted in its creation. The customer PID has the format, host-identifier:process-identifier.
INITIAL ACCESS	The time when SRMA first created it. Initial access also represents the remote customer's first access of local SRMA.
SURROGATE PID	Its local PID, specified in your STATUS command.
VIRTUAL CIRCUIT	The virtual connection number for its connection.

Command Switches

/RESET Reinitializes the statistics accumulators. This switch is equivalent to the RESET command.

Examples

The following example shows the STATUS command and its global status report. Each section of the three-part report has a header that reports the PID for the RMA process (PID 6 in this example), the command name (STATUS), and the scope of the section (global, URMA, or SRMA).

```
) CONTROL @RMA STATUS ↓
) .
  .
  .
FROM PID  6 : (RMA)
  STATUS (GLOBAL) ;TIME: 16:06:48 17-DEC-1985
  STATUS INTERVAL.: 0:20:15
  CUSTOMERS- CUR.: 5  TOT.: 6
  SURROGATES- CUR.: 1  TOT.: 4
  VIRTUAL CIRCUITS - 10 ; 17-DEC-1985

FROM PID  6 : (RMA)
  STATUS ( URMA )
  CONNECTIONS - CUR: 1  TOT: 5
  DURATION - CUSTOMERS  : 1:12:38
             CONNECTIONS: 0:00:38
  SYSTEM CALLS: 172
  BYTES - TRANSMITTED: 14214
          RECEIVED: 35796
  CUSTOMER LIST-
  56,62,28,43,20          ;17-DEC-1985

FROM PID  6 : (RMA)
  STATUS ( SRMA )
  DURATION - SURROGATES:  0:02:44
  SYSTEM CALLS: 152
  BYTES - TRANSMITTED: 35390
          RECEIVED: 64522
  SURROGATE LIST -
  22                      ;17-DEC-1985
```

STATUS (continued)

The next STATUS command displays a report for PID 12, a local customer process. Note that this process has used RMA to gain access to resources on two other hosts, and therefore, has two connections.

```
) CONTROL @RMA STATUS 12 ↓
) .
  .
  .
FROM PID  6 : (RMA)
  STATUS (CUSTOMER)
  PID: 12
  INITIAL ACCESS: 10:59:06 15-DEC-1985
  CONNECTIONS - TOT.:2
  SYSTEM CALLS: 595
  BYTES - TRANSMITTED: 15554
          RECEIVED: 30750
  VIRTUAL CIRCUITS -
  4,5
```

This last STATUS command displays a status report for PID 30, a surrogate process. This surrogate was created by SRMA in response to an RMA request by remote customer PID 12 on host 32500.

```
) CONTROL @RMA STATUS 30 ↓
) .
  .
  .
FROM PID  6 : (RMA)
  STATUS (SURROGATE)
  CUST. PID: 32500:12
  INITIAL ACCESS; 15:43:06 16-DEC-1985
  SURROGATE PID: 30
  VIRTUAL CIRCUIT: 1
```

SURROGATES

Sets or displays the surrogate process limit.

Format

SURROGATES *[n]*

where

n is a decimal number in the range 1–50. An argument of –1 is equivalent to the default limit 20.

Description

The SURROGATES command lets you set or display the number of surrogate processes allowed on your host. The command, therefore, limits remote users' access to your local resources.

To set the limit for surrogate processes, enter the command with an argument. To display the current limit, enter the command without an argument.

Command Switches

None.

Example

The following command sets the surrogate limit to 50:

```
) CONTROL @RMA SURROGATES 50 ⤸
) .
  .
  .
FROM PID  6 : (RMA)
  SURROGATE LIMIT
  SET TO: 50
```

The command response shows the surrogate limit and looks the same whether you set or display the limit.

TERMINATE
Denies RMA services to a process.

Format

TERMINATE pid

where

pid is the process identifier (PID) of a local customer.

Description

This command stops RMA from serving a PID you specify. Current RMA services stop immediately when you enter the command.

When the process you specify is a local process (a customer of URMA), all RMA use by that process stops. The PID itself remains, but cannot use RMA. If the PID attempts to use RMA, it gets an error messge. RMA keeps track of each process you terminate, listing it as a customer, but continuing to deny RMA services to it. When the process terminates in a system logoff, the effect of the TERMINATE command stops. A new process can log on and use RMA, even if it has the same PID number.

When the process you specify is a surrogate process (a customer of SRMA), RMA terminates the process itself, thereby discontinuing service to the remote URMA customer. The surrogate PID will disappear.

Command Switches

None.

Example

The following command terminates all RMA service to the customer on PID 13:

```
) CONTROL @RMA TERMINATE 13 ↵
) .
  .
  .
FROM PID  2 : (RMA)
  TERMINATION OF SERVICE
  FOR PID: 13
```

TIMEOUT

Sets or displays the surrogate time-out duration.

Format

TIMEOUT *[n]*

where

n is, in minutes, the time-out duration, and can be an integer in the range 2 to 546. The argument, zero (0) or –1, represents the default time-out value.

Description

This command allows you to specify the surrogate process time-out period.

Each surrogate process remains active as long as it has an open file or active son process. In addition, the surrogate remains active for a certain time after satisfying its remote user's initial request. The TIMEOUT command specifies the length of this time period. During this time, the surrogate waits for additional RMA requests from its remote user. If it receives another request, RMA restarts the time-out countdown after the surrogate satisfies it.

The argument, zero (0) or –1, specifies the default time-out value, eight minutes.

Command Switches

None.

Examples

The following command displays the current time-out period:

```
) CONTROL @RMA TIMEOUT ↓
) .
  .
  .
FROM PID  6 : (RMA)
  SURROGATE TIMEOUT SET
  TO: 8 MIN (MINUTES)
```

TIMEOUT (continued)

The following command sets the surrogate time-out period at two minutes:

```
) CONTROL @RMA TIMEOUT 2 ↵
) .
  .
  .
FROM PID  6 : (RMA)
  SURROGATE TIMEOUT SET
  TO: 2 MIN (MINUTES)
```

End of Chapter

Chapter 12
Using NETOP with FTA

The File Transfer Agent (FTA) lets users transfer files across a network. Using FTA (UFTA) handles local requests, whereas Serving FTA (SFTA) handles requests made by users on remote hosts.

Users can request FTA services by the following methods:

- adding the /FTA switch to the CLI MOVE and COPY commands
- placing an entry on the FTA queue by using the CLI QFTA command
- executing the interactive UFTA program by entering EXECUTE UFTA from the CLI

For more information on the user interface to FTA, refer to *Using the XODIAC Network Management System.*

As a network operator, you control certain aspects of the FTA process. Table 12-1 lists the FTA commands and tells what you use each command to do.

Table 12-1. FTA Commands

Command	Operator Function
ACCOUNT	Start FTA accounting to the system log file.
CHECKPOINT	Set or display the amount of data that FTA transmits between checkpoints.
CONNECTION	Set or display the length of time FTA waits on an inactive line before disconnecting.
DELAY	Set or display the period that FTA waits before attempting to complete an interrupted transfer.
DISABLE	Stop UFTA and/or SFTA servicing of user requests.
ENABLE	Start UFTA and/or SFTA servicing of user requests.
HALT	Disable UFTA and SFTA; then halt and terminate the FTA process.
LIMIT	Set or display the limit for concurrent file transfers.
NOACCOUNT	Stop FTA accounting.
NOSTATISTICS	Turn statistics gathering off.

(continues)

Table 12-1. FTA Commands

Command	Operator Function
RECOVERY	Display or delete the contents of the file that contains recovery information.
REPLY	Set or display the period incoming data buffers wait without receiving a response.
RETRY	Set or display how many times FTA attempts to finish an incomplete file transfer.
SEND	Send messages to a remote UFTA user.
SET	Set parameters that determine how NETOP manages communication from FTA to you.
START	Start the FTA process. (This command includes an SFTA and UFTA ENABLE.)
STATISTICS	Turn statistics gathering on.
STATUS	Display FTA usage statistics.
STREAMS	Set or display a limit for EXEC/FTA transfer requests.
TERMINATE	Terminate a file transfer.

(concluded)

Using FTA Commands to Tune Performance

The commands, CHECKPOINT, CONNECTION, LIMIT, and REPLY, can help tune FTA performance and allocate system resources among the network agent processes.

Before you adjust the checkpoint frame size, connection time-out period, file transfer limit, or reply time-out period, consider these questions with respect to your site's needs:

- Do you prefer to limit the number of concurrent file transfers to maintain a fast transfer rate, or to cycle FTA resources among a large number of transfers, which might slow the transfer rate?
- How important is FTA in relation to the other agent processes? How many connections do you want FTA to have at any one time? How quickly do you want to time out inactive FTA connections?

For information on each command, refer to the Command Dictionary that follows.

File Transfer Agent (FTA) Command Dictionary

The rest of this chapter describes the NETOP commands for FTA. The command descriptions are in alphabetical order and include examples. You can use unique abbreviations for the commands and their switches.

In examples, we show both the command you give and the system response, assuming that you are entering the commands from the console that receives system output. You can reset the destination console for output by using the SET command.

To execute one of the commands, enter it as an argument to the CLI CONTROL command, using the following format:

```
CONTROL @FTA command-name
```

You can also use the CFTA macro, as follows:

```
CFTA command-name
```

Link Names and Device Names

The name of a link is the filename of the link configuration file (LCF). The name of a device is the filename of the device configuration file (DCF). These names are assigned during a NETGEN session.

ACCOUNT

Turns on accounting.

Format

ACCOUNT

Description

This command directs the FTA process to turn on accounting. When accounting is on, FTA records its services to each user in the system log file. This information can be useful for billing purposes or system load analysis.

By default, accounting is off when an FTA process starts running. If accounting is already on when you issue the ACCOUNT command, you simply receive a confirmation message, and accounting stays on. To turn accounting off, use the NOACCOUNT command.

Appendix A shows the system log parameters for X.25 information. To display the contents of the system log file, use the REPORT program, specifying that you want a report of the FTA process resources. For more information on the REPORT program, see *How to Generate and Run AOS/VS* for AOS/VS systems or *How to Generate and Run AOS* for AOS systems.

Command Switches

None.

Example

The following command turns on accounting:

```
) CONTROL @FTA ACCOUNT ↓
) .
  .
  .
FROM PID 6: (FTA)
  ACCOUNTING ON
```

CHECKPOINT

Sets or displays the checkpoint frame size.

Format

CHECKPOINT *[frame size]*

where

frame size is the amount of data (in kilobytes) that you want FTA to transmit between checkpoints.

Description

The CHECKPOINT command sets or displays the checkpoint frame size. A checkpoint is a place in a file before which all previous records are valid. If a transmission error occurs and you must recover a file, you can begin from the last checkpoint. Checkpoint frame size is measured in kilobytes.

To set the checkpoint frame size, enter the command with an argument. To display the current frame size, enter just the command.

Small checkpoint sizes, such as 8 or 10 kilobytes, are useful if your medium is slow (such as a phone line), if the line is noisy, or if data must travel great distances. On a fast, quiet line (such as a local area network), you can use large checkpoint sizes (such as 40 kilobytes and above), since there is less chance of an error occurring.

Command Switches

None.

Example

The following command sets the checkpoint frame size at 10 kilobytes:

```
) CONTROL @FTA CHECKPOINT 10 ↵
) .
  .
  .
FROM PID 6: (FTA)
  FTP CHECKPOINT FRAME SIZE SET TO 10 KILOBYTES
```

CONNECTION

Sets or displays the FTA connection time-out duration.

Format

CONNECTION *[n]*

where

n is an integer between 0 and 65535 that specifies how many seconds FTA will wait before disconnecting.

Description

This command sets or displays a global time-out period for an inactive FTA connection. The global time-out period specifies how long FTA will wait before disconnecting.

Command Switches

None.

Example

The following command displays the current time-out setting:

```
) CONTROL @FTA CONNECTION ↓
  .
  .
  .
FROM PID 6: (FTA)
  FTP CONNECTION TIMEOUT SET TO 900 SECONDS
```

DELAY

Sets or displays the period that FTA will wait before attempting to complete a previously interrupted file transfer.

Format

DELAY*[/AFTER=hh:mm]* *[ALL / n]*

where

ALL are all streams on the File Transfer Queue (FTQ). This is the default setting.

n is a number from 1 to 7 that specifies an FTQ stream.

Description

The DELAY command allows you to set or display the time that FTA waits before trying to complete an incomplete file transfer. By default, FTA waits for 5 minutes on stream 1, 10 minutes on stream 2, 15 minutes on stream 3, and so forth.

To set the FTA delay time, use the /AFTER switch. The argument, ALL, sets the delay time for all FTQ streams. A stream number as an argument sets the delay time for that stream only.

To display the FTA delay time, enter just the command with no switch. The argument, ALL, displays the delay time for all FTQ streams. A stream number as an argument displays the delay time for that stream only.

If you omit an argument, the DELAY command sets or displays the delay time for all streams.

Use this command in conjunction with the RETRY command: the RETRY command specifies how many times FTA tries to complete a file transfer, while the DELAY command specifies how long it waits between tries.

Command Switch

/AFTER=hh:mm Specifies how long FTA waits before trying to finish an interrupted file transfer: hh are hours and mm are minutes. The longest time you can enter is 23:59.

DELAY (continued)

Examples

The following example displays the delay time setting for the seven FTQ streams:

```
) CONTROL @FTA DELAY ↓
.
.
.
```

FROM PID 6: (FTA)
DELAY REPORT

STREAM NO.	*DELAY TIME (HRS:MIN)*
1	*0:5*
2	*0:10*
3	*0:15*
4	*0:20*
5	*0:25*
6	*0:30*
7	*0:35*

TIME: 11:23:41 ; 29-AUG-1985

The following command resets the delay time for stream one to two hours and fifty-five minutes:

```
) CONTROL @FTA DELAY/AFTER=02:55 1 ↓
.
.
.
```

FROM PID 6: (FTA)
DELAY REPORT

STREAM NO.	*DELAY TIME (HRS:MIN)*
1	*2:55*

TIME: 11:24:39 ; 29-AUG-1985

DISABLE
Discontinues FTA servicing.

Format

DISABLE*[/switches]*

Description

This command allows you to prevent the local UFTA and/or SFTA from servicing user requests. It does not terminate FTA, in contrast to the TERMINATE command. By default, the DISABLE command disables both agents; use the /SFTA or /UFTA switch to disable only that one agent.

The DISABLE command allows all active requests to complete. However, UFTA and SFTA stop accepting requests, and queued requests in the File Transfer Queue pend, until you enter the ENABLE command.

Command Switches

/SFTA Disables SFTA.

/UFTA Disables UFTA.

Example

The following command disables both SFTA and UFTA:

```
) CONTROL @FTA DISABLE ↓
) .
  .
  .
```

FROM PID 6: (FTA)
DISABLE REPORT
SFTA DISABLED UFTA DISABLED

ENABLE

Makes UFTA and/or SFTA services available.

Format

ENABLE*[/switches]*

Description

This command makes UFTA and/or SFTA services available. It can also turn on accounting and statistics functions. By default, the ENABLE command starts both UFTA and SFTA, but you can use the /UFTA or /SFTA switch to enable only that one agent.

To start accounting and/or statistics gathering, enter the /ACCOUNT and/or /STATISTICS switch, which are equivalent to the ACCOUNT and STATISTICS commands. Unless you use these switches, the ENABLE command disables accounting and statistics gathering. If you attempt to start accounting or statistics when it is already on, you simply get a confirmation message.

Command Switches

/UFTA	Enables UFTA to service local user requests.
/SFTA	Enables SFTA to service remote user requests.
/ACCOUNT	Turns on accounting.
/STATISTICS	Turns on statistics gathering.

Examples

This command enables UFTA and SFTA and turns on accounting and statistics:

```
) CONTROL @FTA ENABLE/UFTA/SFTA/ACCOUNT/STATISTICS ↓
) .
  .
  .
FROM PID 6: (FTA)
  ENABLE REPORT
  U-FTA ENABLED
  S-FTA ENABLED
  ACCOUNTING ON
  STATISTICS ON
```

This command enables UFTA and SFTA, but disables accounting and statistics:

```
) CONTROL @FTA ENABLE ↓
) .
  .
  .
```

FROM PID 6: (FTA)
ENABLE REPORT
U-FTA ENABLED
S-FTA ENABLED
ACCOUNTING OFF
STATISTICS OFF

HALT

Terminates the FTA process.

Format

HALT

Description

This command disables UFTA and SFTA, then halts and terminates FTA. HALT has the same effect as the DISABLE command, but in addition, it terminates the FTA process.

This command allows all active transfers to complete but prevents FTA from accepting new transfer requests. Transfers in the File Transfer Queue will get an error message.

Command Switches

None.

Example

The following command halts the FTA process:

```
) CONTROL @FTA HALT ↓
) .
  .
  .
FROM PID 6: (FTA)
  HALT
```

LIMIT

Sets or displays the maximum number of concurrent FTA file transfer requests.

Format

LIMIT*//switch] [n]*

where

n is a decimal number between 0 and 20 that specifies how many file transfer requests can be active at one time. The default is 20.

Description

This command sets or displays the maximum number of concurrent file transfer requests. To set the limit, enter the command with an argument; to display the limit, enter the command without an argument.

By default, the LIMIT command sets or displays the total limit for both agents, but switches let you specify that you want to limit total transfers, UFTA transfers, or SFTA transfers. The command takes only one switch at a time.

If you receive an *Insufficient Memory* error message, lower the limit. This error occurs because the buffer space cannot handle the amount of incoming data. By lowering the limit, you lessen the need for buffer space.

Command Switches

/TOTAL Limits the total number of UFTA and SFTA transfers. This is the default setting.

/SFTA Limits the number of SFTA transfers.

/UFTA Limits the number of UFTA transfers.

Example

The following command limits the number of concurrent FTA transfers to 10:

```
) CONTROL @FTA LIMIT 10 ↓
) .
  .
  .
FROM PID 6: (FTA)
  LIMIT REPORT
  FTA TOTAL TRANSFER REQUESTS LIMIT SET TO 10 REQ.
```

NOACCOUNT
Turns off accounting.

Format

NOACCOUNT

Description

This command directs the FTA process to turn off accounting.

To turn accounting back on, use the ACCOUNT command or the ENABLE command with the /ACCOUNT switch.

Command Switches

None.

Example

The following command disables accounting:

```
) CONTROL @FTA NOACCOUNT ↵
) .
  .
  .
FROM PID 6: (FTA)
  ACCOUNTING OFF
```

NOSTATISTICS
Turns off statistics gathering.

Format

NOSTATISTICS

Description

This command directs the FTA process to stop gathering statistics. To restart statistics gathering, use the STATISTICS command.

Alternatively, you can use the /STATISTICS and /NOSTATISTICS switches on the ENABLE and START commands to start and stop statistics gathering.

Command Switches

None.

Example

The following command turns off statistics gathering:

```
) CONTROL @FTA NOSTATISTICS ↓
) .
  .
  .
FROM PID 6: (FTA)
  STATISTICS OFF
```

RECOVERY

Displays or deletes the contents of the FTA recovery file.

Format

RECOVERY*[/switches]*

Description

The FTA recovery file records information that you may need if your system fails during a file transfer. The RECOVERY command displays or deletes the contents of the recovery file.

Used without a switch or with the /REPORT switch, the RECOVERY command provides information on current file transfers, generating a separate report for each active transfer.

The RECOVERY command can also delete some or all of the recovery file's contents, depending on the switches you enter. Combine only the switches, /COMPACT and /BEFORE or /COMPACT and /REPORT.

Command Switches

/BEFORE=date:time	Deletes information on all transfers started before the specified date and/or time.
/COMPACT	Deletes such outdated information as details about successfully completed file transfers. Combining the /COMPACT and /REPORT switches first applies the /REPORT switch, and then compacts the recovery file. Combining the /COMPACT and /BEFORE switches uses the time frame you specify with /BEFORE to compact the file.
/PURGE	Deletes the entire contents of the recovery file.
/REPORT	Reports current file transfer information. This is the default setting.

Example

The following command deletes from the FTA recovery file entries dated before March 13, 1985:

```
) CONTROL @FTA RECOVERY/COMPACT/BEFORE=13-MAR-85 ↓
.
.
.
FROM PID 6 : (FTA)
  RECOVERY REPORT
  RECOVERY DATABASE COMPACTED
  RECOVERY DATA DELETED FOR TRANSFERS
  STARTED BEFORE 13-MAR-1985:12:00:00

UNIQUE TRANSFER ID: 12345
RECOVERY STARTED 31-JUL-1985:12:31:02
HOST:MADISON;  USER:MARGARET
TIME:  16:01:50  ;22-AUG

UNIQUE TRANSFER ID: 24355
RECOVERY STARTED 31-JUL-1985:01:16:03
HOST:BRONX  ;  USER:NINA
TIME:  16:01:55  ;22-AUG
```

REPLY

Sets or displays the reply time-out period.

Format

REPLY *[n]*

where

n is an integer between 0 and 65535 that specifies in seconds how long the system will wait before reassigning an incoming data buffer.

Description

When FTA is waiting for a data transfer from FTA on a remote system, it reserves a buffer to receive incoming data. The REPLY time-out command specifies how many seconds the buffer will wait for remote data before the system reassigns it to another active transfer. The time-out period cycles buffer resources among the waiting transfers when remote FTA is slow or heavily loaded.

The default REPLY time-out interval is 300 seconds (5 minutes). To allow each transfer to hold its buffer until it completes, set the time-out period to zero. To cycle buffer resources among many active transfers, use a short time-out period, such as 5 or 10 seconds.

Buffer availability circulates among transfers, so a transfer's loss of a buffer due to a time-out is only temporary. REPLY time-out, in contrast with the CONNECTION command time-out, does not break the transfer's FTA connection.

Command Switches

None.

Example

The following command sets the reply time-out period to 360 seconds:

```
) CONTROL @FTA REPLY 360 ↓
) .
  .
  .
FROM PID 6: (FTA)
  FTP REPLY TIMEOUT SET TO 360 SECONDS
```

RETRY

Sets or displays the maximum number of FTA attempts to finish an incomplete transfer.

Format

RETRY*[/MAX=x]* $\left[\begin{matrix} ALL \\ n \end{matrix}\right]$

where

ALL are all streams on the File Transfer Queue (FTQ). This is the default argument.

n is a number from 1 to 7 that specifies an FTQ stream.

Description

The RETRY command allows you to set or display the maximum number of times that FTA will attempt to recover a file whose transfer was interrupted. By default, FTA tries seven times.

To set the retry count, use the /MAX=n switch. To display the current retry count, enter the command without a switch.

Use the argument, ALL, to set or display the retry count for all streams on the File Transfer Queue (this is the default setting); specify a number from 1 to 7 to set or display the retry count for a specific FTQ stream.

Command Switches

/MAX=x Sets the retry count to the number you specify. x is an integer from 1 to 32,767.

Examples

The following example displays the retry count for all FTQ streams:

```
) CONTROL @FTA RETRY ↓
.
.
.

FROM PID 6: (FTA)
    RETRY REPORT
    STREAM NO.          NUMBER OF RETRIES
            1                   7
            2                   7
            3                   7
            4                   7
            5                   7
            6                   7
            7                   7

    TIME:   12:24:41    ;   29-AUG-1985
```

The following command sets the retry count to 10 for FTQ stream 2:

```
) CONTROL @FTA RETRY/MAX=10 2 ↓
.
.
.
FROM PID 6: (FTA)
    RETRY REPORT
    STREAM NO.          NUMBER OF RETRIES
            2                   10
    TIME:   12:27:29    ; 29-AUG-1985
```

SEND
Sends a message to a remote UFTA user.

Format

SEND transfer-request-number message

where

transfer-request-number	is the number of the transfer request with which you wish to communicate.
message	is the message you send to the user.

Description

The SEND command lets you send a message to a remote UFTA process. You identify the remote process by supplying its **transfer-request-number** (TRNO) as a command argument.

Your **message** is the command's second argument. The message will appear on the remote UFTA user's console. You can use the STATUS command to get a list of the current TRNOs.

Command Switches

None.

Example

The following command sends a message to the user of transfer request number 15:

```
) CONTROL @FTA SEND 15 FTA is coming down at 1:00. ↵
) .
  .
  .
```

FROM PID 6: (FTA)
SEND REPORT
MESSAGE SENT TO USER OF TRANSFER REQUEST NO. 15:
FTA is coming down at 1:00.

SET

Sets conditions for logging and report display.

Format

SET*[/switches]*

Description

The SET command sets internal NETOP parameters that determine the nature and destination of system reports. You can use the SET command before starting FTA or at any subsequent time.

Normally, the console of NETOP's father process displays UFTA and SFTA reports. You can, however, change the destination console for reports by using the /OUTPUT switch. If NETOP encounters an error while sending a report to the console you specify, it resets the destination to the console of its father process. If an error occurs when it sends a report to that console, however, the report will be lost.

You can also send reports to a log file by using the /LOG switch.

Command Switches

/DATE	Includes the date in each NETOP system response report.
/LOG[=pathname]	Enables logging and creates a new log file. Without an argument, the log file has a default filename and is in the directory :NET:LOGFILES. If you include the pathname argument, the filename and directory are those you specify.
/NODATE	Suppresses the date in reports. This is the default setting.
/NOLOG	Disables logging.
/NOOUTPUT	Disables display of reports at a console.
/NOPROMPT	Suppresses the following NETOP prompt: *FROM PID n : (NETOP)* *TIME: nn:nn:nn*
/NOTIME	Suppresses the time in NETOP response reports.

/OUTPUT [=*@console-name* | =*pid* | =*process-name*]	Specifies the destination console for reports. Without an argument, reports go to the console of NETOP's father process. With an argument, reports go to the console that you specify with *@console-name*, or to the console owned by the process that you specify with *pid* or *process-name*.
/PROMPT	Includes the NETOP prompt. This is the default setting.
/TIME	Includes the time in reports. This is the default setting.
/PARAMETERS	Displays the current FTA log file name and output destination.

Example

The following command displays the current log file name and output destination:

```
) CONTROL @FTA SET/PARAMETERS ↓
) .
  .
  .
FROM PID 6 : (FTA)
  PARAMETERS:

  LOGFILE =:NET:LOGFILES:FTA_12_15_80.LOG
  OUTPUT = FATHER'S CONSOLE
```

START
Starts an FTA process.

Format

START*//switches]*

Description

The START command starts the FTA process.

If an error occurs while NETOP is starting FTA, the error message goes to the console of NETOP's father process, unless you have previously used the SET command to specify a different output console.

This command enables both UFTA and SFTA unless you use the /UFTA or /SFTA switch to enable only that agent.

Command Switches

/ACCOUNT	Turns on accounting.
/NODUMP	Suppresses the dump option. If you omit this switch, AOS/VS creates a memory dump of FTA when the process terminates abnormally. This switch applies only to AOS/VS systems.
/PREEMPTIBLE	Initiates FTA as a pre-emptible process.
/PRIORITY=n	Sets the initial priority of the FTA process to n. The default priority is 2.
/RESIDENT	Initiates FTA as a resident process.
/SFTA	Enables SFTA to serve remote users.
/STATISTICS	Starts the statistics gathering facility.
/SWAPPABLE	Initiates FTA as a swappable process. This is the default setting.
/UFTA	Enables UFTA to serve local users.
/WSMAX=x	Sets the FTA maximum working set size to x. This switch applies to AOS/VS systems only.
/WSMIN=y	Sets the FTA minimum working set size to y. This switch applies to AOS/VS systems only.

These switches relate to operating system concepts explained in the programmer's manual for your operating system.

Example

The following command starts the FTA process:

```
) CONTROL @FTA START ↓
) .
  .
  .
FROM PID  6 : (FTA)
  STARTED
  PID=6
  DATE: 27-FEB-1985
```

STATISTICS

Turns on statistics gathering.

Format

STATISTICS

Description

This command directs the FTA process to begin gathering statistics.

The STATUS command displays the statistics; the NOSTATISTICS command turns off statistics gathering.

Command Switches

None.

Example

The following command turns on the FTA statistics facility:

```
) CONTROL @FTA STATISTICS ↓
) .
  .
  .
FROM PID 6: (FTA)
  STATISTICS ON
```

STATUS

Reports FTA usage statistics.

Format

STATUS*[/switch]*

Description

The STATUS command displays statistics about the FTA process. With no switch, the command displays a global status report with information about the entire FTA process. With a switch, the command displays information on the user transfer request or user process that you specify. You can use only one switch.

These statistics began accumulating when you issued the STATISTICS, START/STATISTICS or ENABLE/STATISTICS commands.

The global status report displays the following information about the FTA process:

REMOTE USERS	Number of remote FTA users.
REMOTE USERS' TRNO's	Transfer request numbers (TRNOs) of remote users' transfers. The TRNO is a number that FTA assigns to each user request.
LOCAL USERS	Number of local FTA users.
LOCAL USERS'S TRNO'S	Transfer request numbers of remote users' transfers.
CURRENT CONNECTIONS	Number of current connections.
CONNECTION ERRORS	Number of connection errors. If many connection errors occur, you may have a noisy connection. FTA will automatically recover from many connection errors, but you can facilitate recovery by using the CHECKPOINT command to make the checkpoint frame size smaller.
FUNCTIONAL ERRORS	Number of functional errors. Functional errors occasionally occur due to remote system problems.
TOTAL TRANSFER REQ'S	Number of remote and local transfer requests.

STATUS (continued)

DATA MESSAGES: RECV: XMT:	Number of data messages received and transmitted. Data messages are the units into which FTA breaks down a file for transfer. As an indication of activity, they let you compare the amount of data your system is receiving with the amount it is sending out.
LOCAL FILE I/O BLOCKS	Number of read and write operations FTA has performed. You can use this figure to see how much computer activity FTA is generating.
FSB LAST INITIALIZED: TIME:	Last time FTA reset the FTA Statistics Block. FTA keeps statistics in this block; it is reinitialized each time you start statistics gathering by using the STATISTICS command or the ENABLE or START command with the /STATISTICS switch.

With the /REQUEST switch, the STATUS command first reports whether a local or remote customer made the transfer request, and whether the request is currently active (transferring data). Then it gives the following information for the transfer request you specified:

LOCAL or REMOTE USER PID	The PID of the user who initiated the request.
CONNECT TIME: h:mm:ss	The duration of the connection in hours, minutes, and seconds.
TRANSFER REQUESTS	The total number of currently active transfer requests.
CUSTOMER NAME	The username of the person who made the request.
EXEC STREAM NO.: n	The transfer's FTQ stream.
VC	The transfer's virtual connection.

With the /PID switch, the command displays the transfer request numbers for the PID you specify.

Command Switches

/GLOBAL	Reports the global status. This is the default setting.
/PID=pid-number	Reports the status of the PID you specify.
/REQUEST=transfer-request-number	Reports the status of the transfer you specify.

Examples

The following STATUS command displays a global status report:

```
) CONTROL @FTA STATUS ↓
  .
  .
  .
FROM PID 6 :(FTA)
  GLOBAL STATUS REPORT
  REMOTE USERS: 0
  REMOTE USERS' TRNO'S:
  NONE
  LOCAL USERS: 0
  LOCAL USERS' TRNO'S:
  NONE

FROM PID 6 :(FTA)
  GLOBAL STATUS REPORT
  CURRENT CONNECTIONS: 0
  CONNECTION ERRORS: RECOVERED : 0 FATAL : 0
  FUNCTIONAL ERRORS: RECOVERED : 0 FATAL : 0

FROM PID 6 : (FTA)
  GLOBAL STATUS REPORT
  TOTAL TRANSFER REQ'S: REMOTE: 21 LOCAL: 15
  DATA MESSAGES: RCV.:286 XMT.:24
  LOCAL FILE I/O BLOCKS: 2730
  FSB LAST INITIALIZED: 19-MAY-1985 TIME: 15:39:16
```

STATUS (continued)

The next command displays statistics on a transfer request that you specify, using the /REQUEST switch:

```
) CONTROL @FTA STATUS/REQUEST=0 ↓
  .
  .
  .
FROM PID 6 :(FTA)
STATUS REPORT FOR TRANSFER REQUEST NO. 0
LOCAL USER PID: 30 ;CONNECT TIME:      1:29:22
TRANSFER REQUESTS: 65542 ;CUSTOMER NAME: DAVI
EXEC STREAM NO.: 0   ;VC: 0
TIME: 15:29:22 ;16-OCT-1985
```

This last command uses the /PID switch to display statistics on PID 30:

```
) CONTROL @FTA STATUS/PID=30 ↓
  .
  .
  .
FROM PID 6 :(FTA)
STATUS REPORT FOR PID 30
TRANSFER REQUEST NUMBERS:
0
TIME: 15:29:43 ;16-OCT-1985
```

STREAMS
Limits or displays EXEC/FTA transfer requests.

Format

STREAMS *[n]*

where

n is a decimal number between 0 and 7 that specifies how many EXEC/FTA requests can be concurrently active in the File Transfer Queue.

Description

This command limits or displays the number of concurrent EXEC/FTA transfer requests. The command does not affect any active transfer, but does prevent EXEC from submitting any additional requests for transfers beyond the limit you specify.

Enter the command with an argument to set the limit; enter the command without an argument to display the limit.

Command Switches

None.

Example

The following command limits the number of concurrent EXEC/FTA transfer requests to 5:

```
) CONTROL @FTA STREAMS 5 ⤸
) .
  .
  .
FROM PID 6: (FTA)
  STREAMS REPORT
  EXEC --> FTA TRANSFER REQUESTS LIMIT SET TO 5 REQ.
```

TERMINATE
Terminates a file transfer.

Format

TERMINATE transfer-request-number

where

transfer-request-number is the number of the file transfer that you want to terminate.

Description

This command terminates a file transfer. You must supply a transfer-request-number (TRNO) as an argument; for a list of the current TRNOs, use the STATUS command. When you terminate a file transfer, FTA sends a termination message to the user's terminal or output file.

The file can be recovered in the following cases:

- if the user specified the /RECOVER switch on a CLI MOVE/FTA or COPY/FTA command
- if the user specified the /RECOVER switch on a UFTA STORE or RETRIEVE command
- if the user specified the /CHECKPOINT switch on a QFTA command

Example

The following command terminates file transfer request 13:

```
) CONTROL @FTA TERMINATE 13 ↓
) .
  .
  .
FROM PID 6: (FTA)
  TERMINATION FOR TRANSFER OPERATION
  FOR TRANSFER REQUEST 13
```

End of Chapter

Chapter 13
Using NETOP with SVTA

The Virtual Terminal Agent (VTA) allows a user on one host to log on to another host as if the user's terminal were directly connected to the other system. Serving VTA (SVTA) handles the incoming requests of remote users; Using VTA (UVTA) handles local requests to call remote hosts.

The relationship between UVTA and SVTA differs from the relationship between URMA and SRMA or UFTA and SFTA. While each host has a single RMA process and a single FTA process, each containing both the Using and Serving functions, VTA's Using and Serving functions are separate. SVTA, a son process of NETOP, waits on a host for incoming requests from remote users who want to log on. UVTA, in contrast, becomes active only when a user issues the CLI command, EXECUTE UVTA. UVTA is then a son process of that user's CLI process. You can therefore use NETOP commands to control SVTA, but not UVTA.

The PAD Facility

The SVTA process includes the X.29/Host Packet Assembler/Disassembler (PAD) facility. PAD allows a remote user at an asynchronous terminal to log on to a Data General host through a public data network (PDN), such as Datapac (Canada), PSS (British Post Office), Telenet (USA), Transpac (France). A somewhat different user interface exists for SVTA users who log on to the host through the PAD facility: the PAD user's virtual console supports different features than other virtual consoles.

Because the SVTA process includes services to both VTA and PAD, some of the commands in this chapter affect VTA and/or PAD connections or virtual consoles.

For a discussion of the user interface to VTA, and an introduction to X.29/Host PAD, refer to the manual, *Using the XODIAC Network Management System.*

Operator Commands for SVTA

As a network operator, you control certain aspects of the SVTA process. Table 13-1 lists the SVTA commands and tells what you use each command to do.

Table 13-1. SVTA Commands

Command	Operator Function
DISABLE	Prevent new calls for virtual consoles.
ENABLE	Establish a connection with X25 or XTS and enable virtual consoles.
OWNER	Set or display the default owner process for virtual consoles.
PARAMETERS	Display the parameters of a PAD connection.
REVERSE	Allow or prevent PAD users from reversing the charges.
SET	Set parameters that determine how NETOP manages SVTA communication to you.
START	Start the SVTA process. (This command includes an implicit ENABLE.)
STATUS	Display the current connection status of virtual consoles.

Virtual Terminal Agent (VTA) and X.29/Host PAD Command Dictionary

The rest of this chapter describes the NETOP commands that control SVTA's services to VTA and PAD. The descriptions are in alphabetical order and include examples. You can use unique abbreviations for commands and their switches.

Some of the commands apply exclusively to VTA or X.29/Host PAD processes, while some apply to both.

Examples assume that you are entering the commands from the console that receives system output. You can reset the destination for output by using the SET command.

To use one of the commands in this section, enter it as an argument to the CLI CONTROL command, using the following format:

```
CONTROL @SVTA command-name
```

You can also use the CSVTA macro, as follows:

```
CSVTA command-name
```

Link Names and Device Names

The name of a link is the filename of the link configuration file (LCF). The name of a device is the filename of the device configuration file (DCF). These names are assigned during a NETGEN session.

DISABLE
Disables VTA or PAD.

Format

DISABLE*[/switch]*

Description

The DISABLE command prevents new calls from being established by making virtual consoles unavailable to VTA or PAD. DISABLE does not terminate current virtual consoles.

You must use a single switch to specify whether you want to disable VTA or PAD calls. If you omit or use both switches, DISABLE does not affect either PAD or VTA calls.

Command Switches

/PAD Disables new calls for PAD.

/VTA Disables new calls for VTA.

Example

The following command prevents users from making new connections to PAD:

```
) CONTROL @SVTA DISABLE/PAD ↓
) .
  .
  .
FROM PID 5: (SVTA)
  DISABLE REPORT
    PAD IS DISABLED
  TIME:  13:41:28
```

ENABLE
Enables VTA and/or PAD.

Format

ENABLE*[/switch]*

Description

The ENABLE command directs the SVTA process to establish a connection with X25 or XTS and enable virtual consoles for use by VTA and/or PAD. Since starting SVTA enables virtual consoles for VTA, but not PAD, you must use this command to enable virtual consoles for PAD. You also use ENABLE when X25 or XTS has terminated and come back up.

Normally, without a switch, the command enables only VTA. However, if X25 or XTS terminates and comes back up, the command's default switch reflects conditions prior to the termination. If you previously enabled PAD and not VTA, ENABLE without a switch will affect PAD and not VTA.

Command Switches

/PAD Allows PAD to use virtual consoles.

/VTA Allows VTA to use virtual consoles.

Examples

The following command establishes an SVTA connection with the transport service and enables VTA:

```
) CONTROL @SVTA ENABLE/VTA ↵
) .
  .
  .
FROM PID 5: (SVTA)
  ENABLE REPORT
    VTA IS ENABLED
  TIME:  13:44:28
```

The next command enables PAD operations:

```
) CONTROL @SVTA ENABLE/PAD ↵
) .
  .
  .
FROM PID 5: (SVTA)
  ENABLE REPORT
    PAD IS ENABLED
  TIME:  13:44:28
```

OWNER

Sets or displays the default username and process name for VTA and/or PAD.

Format

OWNER*[/switches] [processname]*

where

processname is the name of the process that will be the default.

Description

The OWNER command lets you set or display the default owner process for virtual consoles under the control of VTA and/or PAD. The initial default process for consoles under VTA and PAD is OP:EXEC.

To set the default owner process, enter the OWNER command with its argument, a process name. With a switch, the command sets the default owner of either VTA or PAD virtual consoles. Without a switch, the command sets the default owner for both PAD and VTA.

To display the default owner process of VTA and/or PAD, enter the command without an argument. With a switch, the command displays the default owner of either VTA or PAD. Without a switch, the command displays the default owner of both.

Command Switches

/PAD Sets or displays the default owner process for virtual consoles under PAD control.

/VTA Sets or displays the default owner process for virtual consoles under VTA control.

Examples

The following command displays the default owner process for PAD virtual consoles:

```
) CONTROL @SVTA OWNER/PAD ↓
) .
  .
  .
FROM PID 5: (SVTA)
OWNER REPORT FOR
  PAD CONSOLES
  DEFAULT PROCESS NAME : OP:EXEC
  TIME:  13:44:55
```

OWNER (continued)

The next command sets OP:TPMS as the default owner process for VTA virtual consoles:

```
) CONTROL @SVTA OWNER/VTA OP:TPMS ↓
) .
  .
  .
FROM PID 5: (SVTA)
OWNER REPORT FOR
  VTA CONSOLES
  DEFAULT PROCESS NAME : OP:TPMS
```

PARAMETERS

Reports the current parameter values for a PAD connection.

Format

PARAMETERS *[@VCONn]*

where

@VCONn specifies a virtual console number.

Description

The PARAMETERS command displays the current parameter values for the PAD connection of a virtual console. These parameters reflect the characteristics of the PAD console. If you omit the @VCONn value, the command displays the default parameter values for all PAD connections.

Table 13-2 lists the parameters and explains their functions.

Table 13-2. PAD Parameters

Parameter	Function
Escape from Data Transfer	Allows a user to switch from data transfer to command mode.
Echo Mode	Determines whether characters are echoed on the terminal.
Data Forwarding Signal	Determines which characters cause data to be sent to the remote host.
Idle Timer Interval	Determines, in seconds, how frequently the current character buffer contents are sent to the AOS/VS host.
Ancillary Device Control	(Data General does not use this parameter.)
Network Message Display	Controls the display of network information messages at the terminal.
Procedure on Break	Indicates how the PDN reacts to a break signal from the terminal.
Disregard Output	Prevents output to the screen.
Carriage Return Padding	Determines whether to include a time delay after Carriage Return or other delimiters to allow time for the completion of electro-mechanical functions.
Line Folding	Determines, in characters, the size of the line.
DTE - DCE Flow Control	Determines whether the control sequences, CTRL-S and CTRL-Q, start and stop input.

Command Switches

None.

PARAMETERS (continued)

Example

The following command displays the current parameters for PAD virtual consoles:

```
) CONTROL @SVTA PARAMETERS ↓
) .
  .
  .
```

FROM PID 5: (SVTA)

PARAMETER REPORT GLOBAL
X.3 PARAMETER

PARAMETER NUMBER		*PARAMETER VALUE*
1	*ESCAPE FROM DATA TRANFER*	*1*
2	*ECHO MODE*	*1*
3	*DATA FORWARDING SIGNAL*	*126*

TIME: 13:46:12

FROM PID 5: (SVTA)

PARAMETER REPORT GLOBAL
X.3 PARAMETER

PARAMETER NUMBER		*PARAMETER VALUE*
4	*IDLE TIME*	*0*
5	*ANCILLARY DEVICE CONTROL*	*0*
6	*NETWORK MESSAGE DISPLAY*	*1*

TIME: 13:46:12

FROM PID 5: (SVTA)

PARAMETER REPORT GLOBAL
X.3 PARAMETER

PARAMETER NUMBER		*PARAMETER VALUE*
7	*PROCEDURE ON BREAK*	*21*
8	*DISREGARD OUTPUT*	*0*
9	*CARRIAGE RETURN PADDING*	*0*

TIME: 13:46:12

FROM PID 5: (SVTA)

PARAMETER REPORT GLOBAL
X.3 PARAMETER

PARAMETER NUMBER		*PARAMETER VALUE*
10	*LINE FOLDING*	*0*
12	*DTE - DCE FLOW CONTROL*	*1*

TIME: 13:46:12

REVERSE

Allows or prevents remote PAD users from reversing the charges on a PAD connection.

Format

REVERSE { ON / OFF }

Description

The REVERSE command specifies whether your host will accept the charges if a PAD user wants to reverse them. The command applies only to connections through a public data network.

The argument, ON, allows users to reverse the charges when calling your host. The argument, OFF, prevents users from reversing the charges. The default is OFF.

Command Switches

None.

Example

The following command specifies that your host will accept reversed charges:

```
) CONTROL @SVTA REVERSE ON ↓
) .
  .
  .
FROM PID 5: (SVTA)
    REVERSE REPORT
    REVERSE CALL CHARGING WILL BE ACCEPTED

    TIME: 13:49:41
```

SET

Sets conditions for logging and message display.

Format

SET*[/switches]*

Description

The SET command sets internal NETOP parameters that determine the nature and destination of system reports. You can use the SET command before starting SVTA or at any subsequent time.

Normally, the console of NETOP's father process displays reports from SVTA. You can change the destination console for reports by using the /OUTPUT switch. If NETOP encounters an error while sending a report to the console you specify, it resets the output destination to the console of its father process. If an error occurs when it sends a report to that console, however, the report will be lost.

You can also send reports to a log file by using the /LOG switch.

Command Switches

/LOG*[=pathname]*	Enables logging and creates a new log file. Without an argument, the log file has a default filename and is in the directory :NET:LOGFILES. With a pathname argument, the log file name and directory are those that you specify.
/NOLOG	Disables logging.
/NOOUTPUT	Disables reporting to a console.
/NOPROMPT	Suppresses the following NETOP prompt: *FROM PID n : (NETOP)* *TIME: nn:nn:nn*
/NOTIME	Suppresses the time in reports.
/OUTPUT [*=@console-name* / *=pid* / *=process-name*]	Enables message reporting to a console. Without an argument, the destination for reports is the console of NETOP's father process. With an argument, the destination is @console-name, or the console owned by the PID or process-name that you specify.

/PARAMETERS	Displays the current SVTA log file and output destination.
/PROMPT	Includes the NETOP prompt. This is the default setting.
/TIME	Includes the time in operator messages. This is the default setting.

Example

The following command specifies that console 13 will display all messages. Notice that the terminal displays the NETOP prompt, but no confirmation message.

```
) CONTROL @SVTA SET/OUTPUT=@CON13 ↓
) .
  .
  .
FROM PID  6 : (SVTA)
```

START
Starts the SVTA process.

Format

START*[/switches]*

Description

The START command creates the SVTA process.

If an error occurs while NETOP is starting SVTA, NETOP sends the error message to the console of its father process, unless you have previously used the SET command to specify a different output console.

Command Switches

/NODUMP	Suppresses the dump option. If you omit this switch, AOS/VS creates a memory dump when SVTA terminates. This switch applies to AOS/VS systems only.
/PREEMPTIBLE	Initiates SVTA as a pre-emptible process.
/PRIORITY=n	Sets the initial priority for the SVTA process to a number you specify (n). The default priority is 2.
/RESIDENT	Initiates SVTA as a resident process.
/SWAPPABLE	Initiates SVTA as a swappable process. This is the default setting.
/VCONS=n	Specifies how many (n) virtual consoles SVTA creates. N can be from 0 to 32. The default is 5.
/WSMAX=x	Sets the maximum working set size for SVTA to x. This switch applies to AOS/VS systems only.
/WSMIN=y	Sets the minimum working set size for SVTA to y. This switch applies to AOS/VS systems only.

These switches relate to operating system concepts explained in the programmer's manual for your operating system.

Example

The following command creates the SVTA process, with 15 virtual consoles:

```
) CONTROL @SVTA START/VCONS=15 ↓
) .
  .
  .
FROM PID  6 : (SVTA)
  STARTED
  PID = 6
```

STATUS

Reports the current connection status of virtual consoles.

Format

STATUS [*pid* | *@VCONn*]

where

pid is the identification number for the process associated with a virtual console.

@VCONn indicates a virtual console number.

Description

This command displays statistics about the entire SVTA process, a specific process, or a virtual console.

With no argument, the STATUS command displays a global status report. With am argument, the command displays a report on the process or virtual console that you specify.

The global status report includes the following for each virtual console:

VCON The virtual console's number.

OWNER The PID number of its current owner process.

CONSOLE NETWORK The type of connection: VTA or PAD.

VC The number of its virtual connection.

If you specify a PID number, the status report includes the following information:

PDN The public data network through which this connection was made. (For PAD connections only.)

If you specify a virtual console number, the command displays the following about that virtual console:

OWNER The PID of its owner process.

VCON The virtual console number.

REQS Its total number of current outstanding system calls.

OPENS The number of processes currently using it.

VC The number of its virtual connection.

PDN	The name of the public data network through which the connection came. (For PAD connections only.)
STATE	The state of the connection.
CONSOLE NETWORK	The type of connection: VTA or PAD.

Command Switches

None.

Examples

The following command displays a global status report:

```
) CONTROL @SVTA STATUS ↓
) .
  .
  .
FROM PID  6 : (SVTA)
  STATUS REPORT (GLOBAL)
  VCON  OWNER    VC    CONSOLE NETWORK
   1      55      7     VTA
   10     46      4     VTA
   TIME:  13:48:14
```

The next command displays a status report for virtual console 1. This virtual console has a PAD connection through the public data network, Datapac.

```
) CONTROL @SVTA STATUS @VCON1 ↓
) .
  .
  .
FROM PID  6 : (SVTA)
  STATUS REPORT
  OWNER: 55
  VCON  REQS  OPENS  VC    PDN       STATE
   1      1      3     7    DATAPAC   CONNECTED
```

End of Chapter

Chapter 14
Using XODIAC to Load Software and Back Up Files

This chapter describes how you, as a system manager or operator, can use XODIAC to perform the basic tasks of loading software and backing up and restoring files. The procedures are general enough to apply to any network. They are designed, however, for the specific situation where one large host (for example, an ECLIPSE MV/10000™) is on a network with one or more smaller machines (for example, an ECLIPSE MV/4000®). The small host has limited resources. It has less memory, and it may not have a sophisticated initial loading device. For efficiency, the smaller host should be able to use the resources of the larger host. The procedures in this chapter permit that kind of sharing.

The procedures are described in terms of two hosts: CENTRAL, the larger machine, and LOCALHOST, the smaller machine. Where necessary, you substitute the names of the actual hosts in your network.

This chapter describes the following procedures:

- loading AOS/VS system files from the large host to the small host
- loading other software from the large host to the small host
- backing up files from the small host to the large host
- restoring files from the large host to the small host

These procedures all use the Resource Management Agent (RMA). For a complete discussion of RMA, see *Using the XODIAC Network Management System.*

Loading AOS/VS System Files

This section describes loading AOS/VS system files, specifically on a system such as an MV/4000 SC or DS 4000-series. These machines have a built-in Intelligent Controller Board (ICB) to connect them to a local area network (LAN). You usually load AOS/VS onto these systems from diskettes.

The procedure described in this section lets you load the second AOS/VS dump file over the LAN rather than from diskette. You must still load the first dump file from the release medium, but the second file is much larger than the first. In addition, the procedure lets you avoid duplicating certain files, such as those in :SYSGEN, and saves disk space.

Most of this section assumes you are loading the AOS/VS system files for the first time. You can also use this procedure for installing a revision of AOS/VS. See the end of the section for details about installing revisions.

When you install AOS/VS, you load the first AOS/VS dump file from diskette. This provides a starter system for subsequent loading. The starter system has two limitations:

- It does not provide usernames. To perform any tasks, you must be a user. The procedure described here has a method for giving you a temporary username.
- It does not return network error messages, because the XODIAC error messages are not yet part of the :ERMES file. The system returns only numeric error codes. To find the meaning of a code, use the CLI command MESSAGE on the central, large host.

The procedure uses macros and a specification file that are specifically tailored to machines with an ICB:

- OP_TEMP.CLI, a macro that creates a temporary user profile with the necessary privileges (provided on file 6 of the first AOS/VS dump file).
- UP.LAN.NETWORK.CLI, a macro that brings up the LAN (provided with the XTS software). You use this macro only within the context of loading AOS/VS system files. For the standard procedure of bringing up the LAN, use UP.NETWORK, as described in Chapter 8 of this book.
- BASIC_SPEC, a NETGEN specification file for configuring the smaller host (provided with the XTS software).

You can adapt the macros and specification file to other configurations.

The following list is an overview of the loading procedure. Some steps are combined or omitted. A complete description appears later in this section. Note that the small host is called LOCALHOST, and the large host is CENTRAL.

Step	On Host	Action
1	LOCALHOST	Load the first AOS/VS dump file from the release medium. This installs a starter system.
2	LOCALHOST	Install the XODIAC network software.
3	LOCALHOST	Use NETGEN to tailor BASIC_SPEC to your host.
4	LOCALHOST	Execute UP.LAN.NETWORK.CLI to bring up the network on your host.
5	LOCALHOST	Execute OP_TEMP.CLI to create a temporary user profile.
6	CENTRAL	Make sure the link to LOCALHOST is properly configured.

7	CENTRAL	Use PREDITOR to create a user profile for OP_TEMP.
8	CENTRAL	Load the AOS/VS system files onto CENTRAL.
9	CENTRAL	Use RMA to move the system files to LOCALHOST.
10	LOCALHOST	Install the AOS/VS system files in the root directory, and use SYSGEN to generate a tailored operating system.
11	LOCALHOST, CENTRAL	Delete the OP_TEMP profiles and any temporary CENTRAL directories.

The following sections give details about this procedure. Some sections are directed to the manager of the smaller host (LOCALHOST) and some to the manager of the larger host (CENTRAL).

Preparing the Smaller Host for Loading AOS/VS System Files

As manager of the smaller host (LOCALHOST), you must generate a starter AOS/VS system and install the XODIAC software before you can receive the AOS/VS system files. Follow these steps:

1. Load the first AOS/VS dump file from the release medium. To do so, follow the steps, in *How to Generate and Run AOS/VS,* up to the point at which it explains how to load AOS/VS system files from diskettes.
2. Load the XODIAC software, following the steps in Chapter 2 of this book.
3. Execute NETGEN, choosing the option to access or update a specification file. Use BASIC_SPEC as the specification file. Make the following changes. (The list skips irrelevant fields; press NEW LINE to accept the current value.)
   a. Change the local host, as follows:
      - Select the option "Manage Local Host Configuration."
      - NETGEN displays the host name LOCALHOST. Enter the actual name of your host, as provided by your network manager.
   b. Change the device specification, as follows:
      - Select the option "Manage Device Configuration," followed by the option "Change Device Configuration." Enter the device name LAN.
      - NETGEN asks "Do you wish to specify the ICB Station Address?" Answer Y. NETGEN displays the first 6 hexadecimal digits of the address. You must enter the last 6 digits. Get this address from your network manager.

c. Change the remote host specification, as follows:

- Select the option "Manage Remote Host Configuration," followed by the option "Change Remote Host Configuration." Enter the host name CENTRAL.
- NETGEN displays the prompt "Path(1)." Press NEW LINE. NETGEN asks if you want to delete this path, insert this path, and configure the path for any PMGR switched line. Press NEW LINE three times, to answer No to each question.
- NETGEN displays the link name LANLINK. It asks for the station address. Enter the full 12 digits, as provided by your network manager.

NOTE: You can use this remote host configuration only if the large host is actually named CENTRAL. If it has a different name, you must add a new remote host with that name. Use exactly the same values that are given for CENTRAL, then delete CENTRAL.

d. Return to the first menu level. Select the option "Create Configuration Files." Enter the specification file name BASIC_SPEC.

4. Execute the macro UP.LAN.NETWORK to bring up the network.

5. Move to the root directory and execute the macro OP_TEMP:

```
) DIRECTORY : ⤸
) OP_TEMP ⤸
```

This creates a temporary user profile with the username and password OP_TEMP.

6. Create a directory to receive the AOS/VS system files from larger host:

```
) SUPERUSER ON ⤸
*) CREATE/DIRECTORY  :LOCAL_ROOT ⤸
```

The smaller host is now ready to receive the AOS/VS system files from the larger host.

Loading AOS/VS Files from the Larger Host

As manager of the larger host (CENTRAL), you must make sure your network is configured correctly, create an OP_TEMP profile, and then move the files. It is assumed that you are OP on this system. Your profile must at least include the Change Username privilege. Follow these steps:

1. Make sure the NETGEN specification agrees with the specifications on the smaller host:
   - The smaller host must be configured as a remote host.
   - The ICB link to the smaller host must have a packet size of 1024 bytes and must specify 25 switched virtual connections (SVCs). BASIC_SPEC on the smaller host sets these values, which must agree between the two hosts.

2. Use PREDITOR to create a user profile with the username and password OP_TEMP. Give OP_TEMP at least these privileges: Superuser and Access Local Resources from Remote Machines. This profile matches the OP_TEMP profile on the smaller host.

3. Create a directory to receive the AOS/VS system files from tape:

```
) SUPERUSER ON ⤸
*) DIRECTORY : ⤸
*) CREATE/DIRECTORY CENTRAL_ROOT ⤸
*) DIRECTORY CENTRAL_ROOT ⤸
```

4. Mount the system tape on the drive and load the system files from the tape. The relevant AOS/VS files are on file 7 of the tape. Use the pound sign (#) template to load the entire subdirectory structure of file 7. For example, if the tape drive is MTB0, use this command line:

```
*) LOAD/V @MTB0:7 # ⤸
```

5. Create a CLI process for the user OP_TEMP, blocking your own CLI process. This step lets you use the OP_TEMP username/password. To use RMA, the username/password combination must be the same on both hosts.

```
*) PROCESS/DEFAULT/IOC/BLOCK/USER=OP_TEMP  CLI ⤸
```

6. Move the contents of CENTRAL_ROOT to the temporary directory created on the smaller host (here named LOCALHOST):

```
*) MOVE/V :NET:LOCALHOST:LOCAL_ROOT # ⤸
```

7. Delete the temporary directory and temporary profile. To do the latter, either use PREDITOR or (as shown here) explicitly delete the profile's files:

```
*) DIRECTORY : ⤸
*) DELETE/V CENTRAL_ROOT:# ⤸
*) DELETE/V :UDD:OP_TEMP ⤸
*) DELETE/V :UPD:OP_TEMP ⤸
```

Installing the AOS/VS System Files on the Smaller Host

As system manager of the smaller host (LOCALHOST), you must now install the files that have been moved into the directory :LOCAL_ROOT from the larger host. Follow these steps:

1. Delete from LOCAL_ROOT any files you do not need: for example, the files in :HELP or :SYSGEN. This saves disk space on your system. For example, the following command line deletes the HELP files:

```
) DELETE/V :LOCAL_ROOT:HELP:# ⤸
```

2. Move the remaining system files from the temporary directory to the root directory:

```
) DIRECTORY :LOCAL_ROOT ⤸
) MOVE/V/RECENT : # ⤸
```

3. If you need to tailor the system files, run SYSGEN as described in *How to Generate and Run AOS/VS*.

1. Delete the temporary directory and temporary profile. To do the latter, either use PREDITOR or (as shown here) explicitly delete the profile's files:

```
) SUPERUSER ON ⤸
*) DIRECTORY : ⤸
*) DELETE/V CENTRAL_ROOT:# ⤸
*) DELETE/V :UDD:OP_TEMP ⤸
*) DELETE/V :UPD:OP_TEMP ⤸
```

Installing a Revision of AOS/VS

The previous description has assumed that you are installing AOS/VS for the first time on the smaller host. If you intend to use these procedures to install revisions of AOS/VS as well, consider these points:

- Once the network is installed on the smaller host, you omit the steps that generate and install the network.
- You may not want to delete the temporary user profile OP_TEMP, which you can use to load future revisions. (OP_TEMP has the matching username/password that RMA requires. It is better not to give OP the same username/password on the two systems.) Because OP_TEMP has Superuser privilege, you may not want to keep the profile active on this system. In this case, you can recreate the profile when you need it.
- You can keep the temporary directory LOCAL_ROOT to receive future revisions of AOS/VS. It is best, however, to delete the contents of this directory after you have successfully installed AOS/VS in the root directory.

Loading Programs over the Network

You can also use XODIAC to move other software products over the network. This method is often more efficient than loading the software directly from diskettes onto a small system.

This discussion focuses on a smaller host called LOCALHOST and a larger host called CENTRAL. The procedure, however, works for any two hosts that can communicate on a XODIAC network. The procedure makes the following assumptions:

- Both hosts have correctly used NETGEN and therefore can communicate with each other.
- The hosts can use RMA, which requires profiles with the same username/password combination on both systems. The profiles must also have the privilege to Access Local Resources from Remote Machines. The OP_TEMP profile, described in the previous section, is useful in this context.

There are two versions of this procedure:

1. The system manager of the larger host (CENTRAL) can load the software onto the larger host and then move it to the smaller host (LOCALHOST).
2. The system manager of the smaller host (LOCALHOST) can move the software directly from the tape unit of the larger host (CENTRAL) to the smaller host.

The method you use can depend on the number of hosts in your configuration. If you want to load the software onto a few smaller hosts, the second version may be simpler, because it involves fewer steps. If, however, you want to load the software onto a large number of smaller hosts, the first version may be better, because you need to load from tape only once.

The following sections describe these two versions.

Loading Software from the Central System

As the system manager of the larger host (CENTRAL), you load the software from tape onto disk and then move the software over the network to the smaller host (LOCALHOST). This procedure assumes that you know what directory on LOCALHOST has been prepared to receive the software. Follow these steps:

1. Create a temporary directory to receive the software from tape. Mount the tape and load the software. The following command lines assume that the tape unit is MTB0 and that the relevant software is in the second tape file:

```
) CREATE/DIRECTORY CENTRAL_DIRECTORY ↓
) DIRECTORY CENTRAL_DIRECTORY ↓
) LOAD/V @MTB0:2 ↓
```

2. Move the software to the remote smaller host. The following command line assumes that the target directory on LOCALHOST is :LOCAL_DIRECTORY:

```
) MOVE/V/RECENT :NET:LOCAL_HOST:LOCAL_DIRECTORY # ↓
```

3. Delete the temporary directory:

```
) DIRECTORY ^ ↓
) DELETE/V CENTRAL_DIRECTORY:# ↓
```

The system manager of the smaller host can now install the software.

If you are the system manager of the smaller host, you can perform this procedure yourself. First, use the Virtual Terminal Agent (VTA) to log on the larger host, and then follow these steps.

Loading Software from the Tape Drive of the Larger Host

As the system manager of the smaller host, you can use RMA to load software directly from the tape drive of the larger host. Follow these steps:

1. Ask the manager or operator of the larger host to load the appropriate tape on the tape unit.
2. Create a directory to receive the software:

```
) CREATE/DIRECTORY LOCAL_DIRECTORY ↓
) DIRECTORY LOCAL_DIRECTORY ↓
```

3. Load the software from file 2 of the tape on the larger host's tape unit (here assumed to be MTB0):

```
) LOAD/V :NET:CENTRAL:PER:MTB0:2 ↓
```

You can now install the software and delete the local directory.

Backing Up and Restoring Files over the Network

As the system manager of the smaller host, you can use XODIAC to back up files over the network. If memory on your host is limited, you can back up files onto a disk file on the larger host.

This discussion focuses on a smaller host called LOCALHOST and a larger host called CENTRAL. The procedure, however, works for any two hosts that can communicate on a XODIAC network. The procedure makes the following assumptions:

- Both hosts have correctly used NETGEN and therefore can communicate with each other.
- The hosts can use RMA, which requires profiles with the same username/password combination on both systems. The profiles must also have the privilege to Access Local Resources from Remote Machines. The OP_TEMP profile, described earlier in this chapter, is useful in this context.

This section describes various options for backing up files:

- how to back up an entire system
- how to back up an entire directory (full backup macro)
- how to back up only those files that have been modified since the previous backup (incremental backup macro)

This section also describes how to restore files from the larger host to the smaller host.

Backing Up an Entire System

As system manager of the smaller host (LOCALHOST), you back up your system by moving all files, beginning at the root directory, to the larger host (CENTRAL). Follow these steps:

1. If necessary, create a backup directory on the larger system:

   ```
   ) SUPERUSER ON ⤸
   *) CREATE/DIRECTORY :NET:CENTRAL:REMOTE1 ⤸
   ```

2. Before backing up an entire system, check to see if it is running the CEO® system. You must bring down both CEO and the INFOS® II system before you can do a full system backup. The macros for bringing down these systems are :UTIL:CEO_DIR:CEO.SYSTEM.CLI (with the STOP option) and :UTIL:INFOS_II.DOWN.CLI. See *Managing Your CEO System* and the *INFOS II System User's Manual.*

3. Go to the root directory and move the entire directory tree to the remote backup directory:

   ```
   *) DIRECTORY : ⤸
   *) MOVE/V/RECENT :NET:CENTRAL:REMOTE1 ⤸
   ```

The Backup Macros

The release medium for XTS contains two macros for doing a backup over a network from a smaller host to a larger host. FULL_BACKUP_NET.CLI does a full backup, beginning in whatever directory you execute the macro. (This can be the root directory, for a full backup of the entire system.) INC_BACKUP_NET.CLI backs up only those files that have been created or modified since the previous backup.

Note these points:

- Both macros assume that the larger host is named CENTRAL. If the name is different, edit the macro.
- Both macros assume that a directory named :REMOTE1 exists on CENTRAL to receive your backup files. If the directory has a different name, edit the macro.
- If you execute either macro in the root directory, the macro first turns on Superuser.
- If you execute either macro in a directory other than the root directory, you must have Write access to the directory.
- Both macros automatically include the /V and /RECENT options of the MOVE command. You can also specify the /L[=pathname] option to get a list of the files moved.

- Both macros back up all directories subordinate to the directory where you execute the macro, *except* for the following directories: HELP, PATCH, SYSGEN, UTIL, SWAP, PAGE, PER, PROC, QUEUE, SWAP.SWAP. To back up these directories or specific files in these directories, edit the macro as indicated by a comment in the macro itself.
- Before you can execute INC_BACKUP_NET.CLI from a specific directory, you must already have executed FULL_BACKUP_NET.CLI in that directory. FULL_BACKUP_NET.CLI creates a file, LAST_NET_BACKUP, that records the date and the time of the backup. INC_BACKUP_NET.CLI uses this file as the starting point for its incremental backup and then updates the file for the next incremental backup. Do not delete this file between incremental backups.
- INC_BACKUP_NET.CLI assumes that the date and time on your system are correct each time you do a backup. If they are not correct, INC_BACKUP_NET.CLI may not back up the most recent version of your files.

Figure 14-1 is the text of the FULL_BACKUP_NET.CLI macro, the full backup macro. Figure 14-2 is the text of the INC_BACKUP_NET.CLI macro, the incremental backup macro.

```
comment  This macro does a full backup over the network from the working
comment  directory. To do a full system backup, from the root, it requires
comment  the process that runs it to have Superuser privilege. It assumes
comment  a destination directory named REMOTE1 on the central system. Of
comment  course, the central host can give the backup directory a name
comment  other than REMOTE1. If so, use this name instead of REMOTE1
comment  when you type the text of this macro.
comment  The macro also assumes that the network is up and that the
comment  central hostname is CENTRAL.
comment  The username and password of the person who runs it must be the
comment  same on both systems.
comment  You can run the macro in batch -- which frees your console for
comment  other work and produces a detailed printed listing with dates
comment  -- by typing QBATCH/NOTIFY before the macro name.
push
prompt pop
[!nequal,%1-%,]
  write
  write This macro backs up copyable files in and below [!DIRECTORY] --
  write excluding DG-supplied files in the root and excluding directories
  write HELP,,PATCH,,SYSGEN,,and,,UTIL.
  write It doesn't allow arguments. Please try again via ,, %0% ,, when ready.
  write
[!else]
  [!equal,[!directory],:]
    superuser on
    string root
  [!else]
    comment Not in the root - check for write access. If we can create
    comment and read from a file, assume we have needed access.
    class(1 2) ignore
    permanence =?[!pid].[!username].tmp off
    delete =?[!pid].[!username].tmp
    write/1==?[!pid].[!username].tmp test
    string [=?[!pid].[!username].tmp]
    delete =?[!pid].[!username].tmp
    comment If string does not contain "test", access isn't allowed. Stop.
    [!nequal,[!string],test]
      write
      write Error - [!username] does not have write access to [!directory].
      write ,,,,,,,,,You cannot back up this directory.
    [!end]
    string non_root
  [!end]
  comment Ok to proceed with the backup.
  class1 error
  class2 warning
  write
```

Figure 14-1. The FULL_BACKUP_NET.CLI Macro (continues)

```
  write ** Full backup from directory [!DIRECTORY] at [!TIME] on [!DATE] **
  write
  write ,,,,,,,,,,,,,,,,,,,,  -- Beginning file backup --
  [!equal,[!directory],:]
    MOVE/RECENT/V%O/L%    :NET:CENTRAL:remote1  &
      #\HELP\PATCH\SYSGEN\UTIL\SWAP\PAGE\PER\PROC\QUEUE\SWAP.SWAP
    comment  Note: If you want to back up files in HELP, SYSGEN, or UTIL,
    comment  insert the pathname(s) in the macro BEFORE the #\HELP...
    comment  exclusion. For example, the template UTIL:MYDATA+ before &
    comment  in the MOVE command line will back up all :UTIL:MYDATA+ files.
  [!else]
    MOVE/RECENT/V%O/L%    :NET:CENTRAL:remote1    #
   [!end]
  write
  write ** Full backup of [!DIRECTORY] complete at [!TIME] **
  permanence/2=ignore  =LAST__NET__BACKUP.BU  OFF
  delete/2=ignore  =LAST__NET__BACKUP.BU
  rename/2=ignore  LAST__NET__BACKUP  LAST__NET__BACKUP.BU
  write/1==LAST__NET__BACKUP   [!DATE]:[!TIME]
  write
  write This backup has created file LAST__NET__BACKUP in this directory
  write for future backups. Don't delete this file.
[!end]
```

Figure 14-1. The FULL_BACKUP_NET.CLI Macro (concluded)

```
comment  This macro does an incremental backup over the network from the
comment  working directory. To do a system backup, from the root, it
comment  requires the process that runs it to have Superuser privilege.
comment  Like the full backup macro, it assumes a destination directory
comment  named REMOTE1 on the central system. Of course, the central
comment  host can give the backup directory a name other than REMOTE1.
comment  If so, use this name instead of REMOTE1 when you type the text
comment  of this macro.
comment  The macro also assumes that the network is up and that the
comment  central hostname is CENTRAL.
comment  The username and password of the person who runs it must be the
comment  same on both systems.
comment  You can run the macro in batch -- which frees your console for
commen   other work and produces a detailed printed listing with dates
comment  -- by typing QBATCH/NOTIFY before the macro name.
push
prompt pop
[!equal,[!pathname =LAST__NET__BACKUP],]
  write
  write Error - Incremental backup requires file LAST__NET__BACKUP -- which
  write ,,,,,,,,, does not exist. Suggest either doing FULL__NET__BACKUP or
  write ,,,,,,,,, retry incremental backup from directory in which you
  write ,,,,,,,,, have done your most recent backup.
  write
  [!else]
  comment Check for arguments -- none is allowed.
  [!nequal,%1-%,]
    write
    write This macro backs up copyable files in and below [!DIRECTORY] --
    write excluding DG-supplied files in the root and excluding directories
    write HELP,,PATCH,,SYSGEN,,and,,UTIL.
    write It doesn't allow arguments. Please try again via ,, %0% ,, when ready.
    write
```

Figure 14-2. The INC_BACKUP_NET.CLI Macro (continues)

```
[!else]
  [!equal,[!directory],:]
    superuser on
    string root
  [!else]
    comment Not in the root - check for write access. If we can create
    comment and read from a file, assume we have needed access.
    class(1 2) ignore
    permanence =?[!pid].[!username].tmp off
    delete =?[!pid].[!username].tmp
    write/l==?[!pid].[!username].tmp test
    string [=?[!pid].[!username].tmp]
    delete =?[!pid].[!username].tmp
    comment If string does not contain "test", access isn't allowed. Stop.
    [!nequal,[!string],test]
      write
      write Error - [!username] does not have write access to [!directory].
      write ,,,,,,,,,You cannot back up this directory.
    [!end]
    string non_root
  [!end]
  comment Ok to proceed with the backup.
  class1 error
  class2 warning
  write
  write Incremental backup from directory [!DIRECTORY] at [!TIME] on [!DATE] **
  string [=LAST_NET_BACKUP]
  write This will back up all files created or modified since [!string].
  write
  write ,,,,,,,,,,,,,,,,,,,,  -- Beginning file backup --
  [!equal,[!directory],:]
       MOVE/RECENT/V%O/L%/AFTER/TLM=[!STRING] &
       :NET:CENTRAL:remote1  &
       #\HELP\PATCH\SYSGEN\UTIL\SWAP\PAGE\PER\PROC\QUEUE\SWAP.SWAP
```

Figure 14-2. The INC_BACKUP_NET.CLI Macro (continued)

```
      comment  Note: If you want to back up files in HELP, SYSGEN, or UTIL,
      comment  insert the pathname(s) in the macro BEFORE the #\HELP...
      comment  exclusion. For example, the template UTIL:MYDATA+ before &
      comment  in the MOVE command line will back up all :UTIL:MYDATA+ files.
    [!else]
      MOVE/RECENT/V%O/L%/AFTER/TLM=[!STRING]  :NET:CENTRAL:remote1  #
    [!end]
    write
    write ** Incremental backup of [!DIRECTORY] complete at [!TIME] **
    permanence/2=ignore  =LAST_NET_BACKUP.BU OFF
    delete/2=ignore  =LAST_NET_BACKUP.BU
    rename/2=ignore  LAST_NET_BACKUP  LAST_NET_BACKUP.BU
    write/1= =LAST_NET_BACKUP   [!DATE]:[!TIME]
    write
    write This backup has created file LAST_NET_BACKUP in this directory
    write for future backups. Don't delete this file.
  [!end]
[!end]
```

Figure 14-2. The INC_BACKUP_NET.CLI Macro (concluded)

Restoring Files over the Network

As the system manager of the smaller host, you can use the network to restore files that you previously backed up onto the larger system. You can restore either selected files or the entire disk. AOS/VS and XODIAC must be up and running on both hosts. If system or network files have been destroyed, you must load them on your host. To restore an entire disk, you must first install AOS/VS and XODIAC software as you did originally.

Note these points about the procedure:

- You must have the same username/password combination on both hosts, as well as Superuser privilege on the larger host. If you do not have Superuser privilege, the system manager of the larger host must perform the recovery procedure for you.
- Make sure that the working directory for the restoration corresponds to the one used for the backup. All pathnames are relative to the directory in which you executed the backup macro.

The following descriptions assume that the larger host is named CENTRAL, the smaller host is LOCALHOST, and the backup directory on CENTRAL is REMOTE1.

To restore the smaller host's entire file system, you move the entire backup directory from the larger host. Follow these steps:

1. Log on the larger host using VTA:

```
) XEQ UVTA CENTRAL ⤸
Virtual Terminal Agent Rev 5.10
Call is complete.
Username: OP_TEMP ⤸
Password:         ⤸
AOS/VS CLI REV 7.00
```

2. Go to the backup directory and move its contents back to your host:

```
) SUPERUSER ON ⤸
*) DIRECTORY REMOTE1 ⤸
*) MOVE/V/RECENT :NET:LOCALHOST ⤸
```

To restore only a few files, use a pathname template in the MOVE command. For example, if user DAVID accidentally deleted some files in his directory, MEMOS, the following steps would restore them:

1. Log on the larger host using VTA:

```
) XEQ UVTA CENTRAL ⤸
Virtual Terminal Agent Rev 5.10
Call is complete.
Username: OP_TEMP ⤸
Password:         ⤸
AOS/VS CLI REV 7.00
```

2. Go to the backup directory; use a filename template to move the specific files back to the target directory on your host:

```
) SUPERUSER ON ⤸
*) DIRECTORY REMOTE1 ⤸
*) MOVE/V/RECENT :NET:LOCALHOST:UDD:DAVID:MEMOS &
&*) UDD:DAVID:MEMOS:# ⤸
```

   Note that the pathname of the files to be restored is relative to the working directory on the larger host. In other words, the root directory on the smaller host corresponds to the backup directory on the larger host.

End of Chapter

Appendix A
SYSLOG Formats for Accounting Information

This appendix shows the parameters that network processes use for putting accounting and exception information into the system log file.

Table A-1. Logging Format for Accounting Information

Offset	Octal Value	Contents
ALINK	0	Logical link name
ALCI	10	Logical channel identifier (logical group number and logical channel number)
AVCTE	11	Virtual call number
ATYPE	12	Circuit establishment type: 1 = ?NCALL 2 = ?NACALL 3 = ?NATTACH
ATERM	13	Logging reason: 1 = connection passed 2 = connection closed
AUSERP	14	The username:process-name
ARADR	34	Remote address (The first byte indicates the address length. The actual address may be up to ?NMHAL digits in length.)
ATCH	44	Connect time (days)
ATCL	45	Connect time (bi-seconds)
APAKT	46	Number of packets transmitted
APAKR	47	Number of packets received
ABTH ABTL	50 51	Number of bytes transmitted
ABRH ABRL	52 53	Number of bytes received
AALTH	54	Word length of entry

Table A-2. Logging Formats for Exception Information

Offset	Octal Value	Contents
ALINK	0	Logical link name
ALCI	10	Logical channel identifier (logical group number and logical channel number)
AVCTE	11	Virtual connection number
ATRF	12	Transmitted/received flag 1=transmitted 2=received
ACODE	13	Network error code
ADIAG	14	Network error diagnostic (–1 indicates that no diagnostic applies to this error.)
AERR	15	Error message text (available via ?ERMES)
AELTH	16	Word length of entry

End of Appendix

Appendix B
The NTRACE Program

The trace display program, NTRACE, is a tool for examining the contents of a trace file. The X25 or XTS TRACE command creates the trace file, which contains images of packets sent and/or received on the network. You determine the file's contents by using TRACE command switches that specify which packets the trace will dump into the file.

The NTRACE program lets you examine all or part of the contents in the trace file. By using switches when you execute NTRACE, you can set criteria on which packet images to display. We discuss these switches in the next sections.

You can use the NTRACE program to display only the results of a packet trace, and not an XTS link-layer trace, which traces frames. To display a link layer trace, consult your Data General representative.

The Trace Display

The trace display has a specific format. A heading gives the trace file's pathname. Column headings identify the displayed items, such as packet number, virtual connection number, packet direction, packet type, link name, and the ASCII and octal or hexadecimal representations of the packet contents. Figure B-1 is an example of a trace display.

NTRACE displays the ASCII representation of the packet contents, using a period (.) for every nonprintable character. A numeric representation of the packet contents appears below the corresponding ASCII values; in the example, the numeric representation is in octal radix. The upper digit describes the first four bits of the word (bits 0 through 3); the lower digit describes the last four bits (bits 4 through 7). Refer to the X.25 packet format diagrams in *Programming with the XODIAC Network Management System* for information on interpreting the trace file fields.

To create a trace display that you can print, you must use the /LIST=listname switch when you execute NTRACE. The filename that you specify must have a .LS extension. Use the CLI command, QPRINT, to print the file.

```
Trace file was generated by AOS/VS X25 Revision 04.20.00.20
Trace file is :UDD1:SAL:PACKETS1
Packet  Virtual  Direction  Link Name        Unit  Packet Type  Mod 8/128
Number  Circuit

        ..........  ..........  ...TANYA..  ..........  .HEAD.....
        0000000000  0000000000  0001111111  0000000000  0111100000
        0000000000  0000000000  0001022001  0000000000  0111100000
    1   0000000000  0000000000  0075152556  0000000000  4473100000

        .........A  .....j....  ..........  ..4....Sep  ard T:MRKT
        0000000021  0002312000  0000000000  0000300111  1110101110
        0000000020  0025352000  0000000001  2060000246  4644170106
    2   0000000061  0002126000  0000000000  6040000357  1240324735

        ...0...Rep  ly to Mana  ging Your   Printers..  ...I think
    3   0200200111  1101101111  1111011110  1111111100  0021011111
        0006503246  5746541454  4554435664  2655646600  0001465555
        0000207250  4104705161  7167017520  0216452300  0021040163

    4       2   outgoing   GREEN__NBS__LINK     30  RcvR        8
          LGN=0   LCN=1    LCI=1     P(R)=3
        ..a
        001
        204
        011

Trace file was generated by AOS/VS X25 Revision 04.20.00.20
Trace file is :UDD1:SAL:PACKETS1
Packet  Virtual  Direction  Link Name        Unit  Packet Type  Mod 8/128
Number  Circuit

    5       2   outgoing   GREEN__NBS__LINK     30  Data        8

     D=0  LGN=0   LCN=1    LCI=1     P(S)=1    P(R)=3    M=0  Q=0
       ..b....
       0012000
       2040000
       0125000

    6       2   incoming   GREEN__NBS__LINK     30  Data        8
     D=0  LGN=0   LCN=1    LCI=1       P(S)=3    P(R)=2    M=0  Q=0
       ..F....
       0010000
       2000000
       0166001
```

Figure B-1. Trace Display Example

Executing NTRACE

The following CLI command-line format executes the NTRACE program, allowing you to view the contents of the trace file.

XEQ NTRACE*[/switches]* pathname

where

switches are one or more of the optional packet-type and/or other switches.

pathname is the pathname of a trace file created by NETOP.

The command line can have up to 512 characters.

NTRACE Switches

There are two types of NTRACE switches. Packet type switches specify the type of packets you want the NTRACE program to select, while other NTRACE switches specify further attributes of the packets you want to display. For example, packet type switches allow you to specify that you want a display of Reset Confirmation packets or Interrupt packets, while other switches allow you to specify that you want to start at the second packet, that you want to display every fifth packet, and so forth.

The Packet-Type Switches

The format for the packet-type switches is as follows:

NTRACE*[/packet-type-switch]...*

where

packet-type-switch is one of the following:

/CALL
/CONNECT
/CI
/CCFM
/DATA
/INTERRUPT
/INTCFM
/RCVR
/RNR
/REJ
/RSTIND
/RSTCFM
/RRTIND
/RRTCFM

These switches allow you to restrict the packet images that the NTRACE program selects to one or more specific packet types.

Each switch displays a specific incoming packet type and outgoing packet type. Table B-1 lists the packet types that each switch displays. For each switch, Column 1 lists the switch name; Column 2, the incoming packet type; and Column 3, the outgoing packet type.

The /DIRECTION switch affects the results of these packet-type switches, since it determines whether the switch will display its incoming or outgoing packet type. If you have not used the /DIRECTION switch, NTRACE will display both incoming and outgoing packet images for each packet-type switch you specify.

If you execute the NTRACE program without using a packet-type switch, the program displays packets of all types. If you do use a packet-type switch, but the trace has not found any packets of the type you specify, the trace file will exist but it will be empty.

Table B-1. X25 Packet-Type Switches

Switch	Incoming Packet Type (DCE to DTE)	Outgoing Packet Type
/CALL	Incoming Call	Call Request
/CONNECT	Call Connected	Call Accepted
/CI	Clear Indication	Clear Request
/CCFM	DCE Clear Confirmation	DTE Clear Confirmation
/DATA	DCE Data	DTE Data
/INTERRUPT	DCE Interrupt	DTE Interrupt
/INTCFM	DCE Interrupt Confirmation	DTE Interrupt Confirmation
/RCVR	DCE Receive Ready (RR)	DTE Receive Ready (RR)
/RNR	DCE Receive Not Ready (RNR)	DTE Receive Not Ready (RNR)
/REJ	—	DTE Reject (REJ)
/RSTIND	DCE Reset Indication	DTE Reset Request
/RSTCFM	DCE Reset Confirmation	DTE Reset Confirmation
/RRTIND	Restart Indication	Restart Request
/RRTCFM	DCE Restart Confirmation	DTE Restart Confirmation

Other NTRACE Switches

The NTRACE switches that Table B-2 lists specify various attributes of the packets you want to trace.

You can truncate both switch and argument names to create unique abbreviations. If a switch takes an equal sign, include it, even to enter the switch with its default value, except with the /LIST switch. For example, /DIR= is a valid entry for the default value of the /DIRECTION switch, but /DIR is not.

If you execute NTRACE without using any switches, the default settings are /DIRECTION=BOTH, /INCREMENT=1, /LIST=@OUTPUT, /PACKETS=ALL, /RLENGTH=ALL, and /START=1; the NTRACE program will display packets of all virtual connections.

Table B-2. NTRACE Switches

Switch	Description
/DIRECTION= { BOTH | INCOMING | OUTGOING }	This switch specifies that NTRACE selects and displays packet images according to origin. INCOMING displays images of packets that X25 received. OUTGOING displays images of packets that X25 transmitted. BOTH displays both incoming and outgoing packets. The default setting is /DIRECTION=BOTH.
/INCREMENT=n	The /INCREMENT switch specifies the increment that NTRACE uses to select packet images for display. NTRACE displays the first packet image, and then every nth image until it reaches the end of the trace file. You can specify a decimal number from 1 through 32767. The default setting is /INCREMENT=1.
/LIST[=*listfile*]	The /LIST switch determines the destination file for the trace display. NTRACE sends the trace display to the *listfile* that you specify; however, if you enter the switch in the format, /LIST, omitting the equal sign (=) and *listfile* name, the trace display goes to the current CLI @LIST. If you execute NTRACE without this switch, the trace display goes to the current CLI @OUTPUT. You might want to print the trace display. To enable printing, give the *listfile* name a .LS extension.

(continues)

Table B-2. NTRACE Switches

Switch	Description
/PACKETS= { ALL / n }	The /PACKETS switch specifies a limit on the number of packet images NTRACE displays. You can specify ALL to display all the images in the file, or you can enter n, a decimal number from 1 to 32767. NTRACE then displays the specified number of packet images. The NTRACE program terminates after displaying the specified number of packets, unless it reaches the end of the trace file first. The default setting is /PACKETS=ALL.
/RADIX= { OCTAL / 16 }	The /RADIX switch determines whether NTRACE uses octal or hexadecimal representation for numeric values. The default setting is /RADIX=OCTAL.
/RLENGTH= { ALL / n }	The /RLENGTH switch specifies how many bytes of each packet image the NTRACE program displays. You can specify ALL to display the entire packet image, or you can enter n, a decimal number in the range 1 through 32767. The NTRACE program then displays the first n bytes of the packet image. The default setting is /RLENGTH=ALL.
/START=n	The /START switch specifies the packet image at which NTRACE begins to apply the selection criteria. NTRACE will skip all packet images before the nth image. For n, you can specify a decimal number from 1 through 32767. The default setting is /START=1.
/vc-no[/*vc-no*]...	This switch directs NTRACE to select packet images related to one or more virtual connections. You can specify from one to ten specific virtual connection numbers. If you do not use this switch, the NTRACE program displays packets of all virtual connections by default.

(concluded)

End of Appendix

Appendix C
Network Problems

A wide variety of errors can cause network problems. This appendix covers the following topics:

- the prerequisites
- error resolution
- physical errors
- files that document errors

When errors occur on a network, detecting the cause of the error can be complex. First make sure that the prerequisites that we describe in the first section have been met. Then try the suggestions that we give throughout the rest of the section to narrow down the cause of the failure. It is beyond the scope of this appendix to describe every possible situation; it can, however, suggest some guidelines that are often helpful in resolving problems.

Detecting the cause of network problems is often a process of elimination. When you learn that one element of the network is down, however, you haven't necessarily ruled out problems elsewhere. For example, suppose a network agent cannot establish a connection to a remote host. You might try the following on your host:

- Check the status of the link to see that it is up and ready.
- Check to see that the agent process is up.
- Check to see that the X25 or XTS process is up.
- Re-enable the link.

At this point, you might conclude that remote X25 or XTS, or the remote host, is down. If that isn't the case, you can look for physical causes for the error, such as cable problems. When you exhaust all ideas, call your Data General support organization.

Always enable logging when you bring up the network, using the SET command's /LOG switch. With logging enabled, NETOP writes error messages to a log file, which you can examine. If you neglect to enable logging, NETOP will display messages on the system console, but you may not see them.

Always install the latest software and patches on your system. Checking to make sure you are using the latest software and have installed the latest patches should be a routine part of resolving errors.

For explanations of the most common XODIAC error messages, refer to the manual, *Using the XODIAC Network Management System.*

Prerequisites for XODIAC Agents: User Profiles and ACLs

Certain problems result from simple errors, such as incorrect profiles. To use network agents, remote user profiles must be correct. User profiles determine whether users can do the following:

- access local resources from remote machines
- use virtual consoles

For each network agent, Table C-1 shows a user's profile requirements. Check the profiles of users who report problems using the agents.

Table C-1. Prerequisites for Using Network Agents

Agent	User Needs
FTA, using the CLI commands, QFTA, MOVE, and COPY	A profile on the remote host with the same username/password combination as the profile on the local host.
FTA, using the UFTA program	A profile on the remote host. The username and password need not be the same as on the local host. The remote profile must allow the user to access local resources from remote hosts.
VTA	A profile on the remote host. The username and password need not be the same as on the local host. The remote profile must allow the user to use virtual consoles.
RMA	A profile on the remote host with the same username/password combination as the profile on the local host. The remote profile must allow the user to access local resources from remote hosts. The user must have a :UDD:username directory on the remote host.

In addition, access control lists (ACLs) on files specify what a user can do to remote files. For example, you cannot use UFTA to retrieve files without Write access to the directory containing those files. The *Command Line Interpreter (CLI) User's Manual (AOS and AOS/VS)* has information on ACLs.

Special Prerequisites for RMA, RIA, and RDA

RMA, the Remote INFOS Agent (RIA), and the Remote Database Agent (RDA), require that your host have a Host Identifier (HID). You assign the HID during a NETGEN session. Without a HID for your own host, your RMA process will come up when you bring up the network but will then terminate.

To give RMA users access to remote hosts, the NETGEN session must also supply the HIDs for those hosts.

More complex errors require that you diagnose and resolve or report them. The rest of this chapter explains how.

Network Problems

Problems on a network can come from a variety of sources. They can originate from local network processes, remote network processes, remote host failure, EXEC problems, and so on. Finding the cause of the failure is your first task in resolving the problem. This section suggests some procedures that you can use to track down the cause of a network failure. Sometimes we suggest that you restart individual processes; we describe how in a later section.

In the rest of this chapter, we sometimes use the term *transport service* to mean X25 or XTS, whichever your system has.

An important first step in dealing with network process problems is to make sure you receive all messages from the process. Use the process' SET command to display the output console:

```
) CONTROL @process-name SET/PARAMETERS ⤸
```

If output is going to another console, send it to yours, as follows:

```
) CONTROL @process-name SET/OUTPUT=@[!CON] ⤸
```

Responding to Errors

This section lists some common situations and describes actions you can take. No one suggestion can pin down the cause of a problem, or its resolution, but these commonly-used techniques may help.

Data General–to–Data General networks provide more detailed error messages than networks that include public data networks. In diagnosing network problems when links for both types of networks connect a remote host, use the Data General–to–Data General network unless your test requires otherwise.

Problem	Comment
Errors from a network process lead you to suspect that it is not responding to commands.	Try to determine the level on which the problem is occurring: check NETOP, X25 or XTS, and when appropriate, agent processes. Because NETOP manages the communication between you and its son processes, an apparent problem with an agent process may really be a NETOP problem. Because the transport service handles communication between remote devices, that apparent problem with the agent process may also be an X25 or XTS problem. First, check NETOP. When you issue a command, NETOP first acknowledges the command, and then the son process answers the command. Issue a command to the suspected son process, using a command that displays, rather than changes, conditions such as STATUS. See whether you get a response from NETOP; if you do, NETOP is up, and if you don't, NETOP is down. If you get a response from NETOP but not from the son process, NETOP is up, and the son process is down. Before concluding that a son process is down, be sure to allow for the normal variations in response time caused by network use conditions. If in checking NETOP, you send a command to X25 or XTS and get a response that shows that both NETOP and the transport service are up, use the same method to see whether the suspected agent process is up.
A *LINK INTERFACE TASK EXCEPTION* error message appears when a user is using a network agent.	See whether the problem lies with the link or agent. First, use the X25 LINKS command or the XTS LIST/LINKS command to see if the link is enabled. If the link appears on the list of active links, use the X25 LSTATUS command or XTS STATUS/LINK command to see whether the link is ready. If the link is not ready, refer to the section that explains what to do when you cannot enable a link. If the link is ready, re-enable it. Enabling loads the X.25 program onto the device that the link uses. If re-enabling the link succeeds, the X25 or XTS process is probably not the source of the problem.

Problem	Comment
	Next, use the agent's ENABLE command to re-establish the agent's connection to X25 or XTS. If enabling the agent succeeds, the agent is not the source of the problem. The error may be on a remote system.
RMA appears hung.	See if RMA or a remote host is causing the problem. RMA, in contrast to FTA and VTA, does not quickly ends its relationship with user processes. Instead, RMA waits for additional user requests before terminating. If a remote host goes down while virtual connections are open, RMA may continue waiting for service from the remote host, instead of timing out. To see whether a failure lies with RMA or the remote host, enter the RMA STATUS command. If RMA does not reply, it is down. If RMA does reply, the remote host may be down. You can then use the X25 or XTS CLEAR or the RMA DISABLE command to clear the virtual connection.
You cannot enable a link.	First, find out if the link is on the list of active links, using the X25 LINKS or XTS LIST/LINKS command. If the link is not listed as active, try again to enable it. If the link is listed as active, see if the link is ready or if a restart is in progress, using the X25 LSTATUS or the XTS STATUS/LINK command. If the link is ready, the problem is probably caused by another type of failure. If a restart is in progress, try again in a minute. If you get the same message on a second try, bring the network down and then up again. If you still cannot enable the link, a hardware problem may be causing the error. Refer to the section on physical problems later in this chapter. Often, you refer physical problems to your Data General support organization.

Problem	Comment
An RMA user queues remote files but does not get a response.	See if the problem is that EXEC is not performing the queueing or that RMA is simply slow. First, check to see that EXEC is performing the queueing operation. Since EXEC performs all system queueing, when you request a queueing operation and specify a remote source, EXEC becomes a customer of RMA. Use RMA's STATUS command to see whether OP is RMA's customer:) CONTROL @RMA STATUS OP:EXEC ♪ The RMA status report tells whether EXEC is an RMA customer and whether outstanding connections exist. If EXEC is a customer, you know that it is performing the queueing, and the problem is probably only slow response time. If you then want to clear the connection, enter the X25 or XTS CLEAR command. Note that if problems between RMA and the transport service exist, X25 or XTS could terminate after you clear the connection. If you suspect this type of problem, check to see that X25 or XTS is still up. If you find that an agent is causing X25 or XTS termination, call your Data General support organization.
The network fails, and you cannot determine the reason for the failure.	Bring the network down and then bring it up again.
NETOP fails and terminates.	Bring the network up again.
Time-out errors during an initial connection lead you to suspect that remote X25 or XTS or a remote host may be down.	If the link to a remote host is a synchronous or MCA link, you receive a *LINK INTERFACE TASK EXCEPTION* error message. On a synchronous line, the message also reports *REMOTE IS DISCONNECTING,* and, after a number of unsuccessful tries at re-establishing the connection, *HDLC LINK INITIALIZATION FAILED.* On an MCA link, the message also reports *DEVICE TIMEOUT*, but does not send the second message. If remote X25 or XTS seems to be down, and the link is of another type, execute one of the Using agents: UFTA or UVTA. You will quickly know that remote X25 or XTS is up if you get a connection. If you get a time-out error, remote X25 or XTS or the remote host is probably unavailable.

Problem	Comment
	When remote X25 or XTS or a remote host is down, that host's operator must bring it back up. However, an error on the physical level may also be at fault—refer to the section *Physical Errors*, later in this chapter.
Network processes are failing, but only over one link.	Find out whether the problem is in the link, the transport service, or the device. The problem may just be that the link is disabled. Try to re-enable it by issuing a DISABLE and then an ENABLE command. If you cannot re-enable the link, check the X25 or XTS process by the method we described earlier, or terminate and then start the process. The problem can also be caused by physical problems on the device; refer to the section on physical errors later in this chapter.
XTS or X25 terminates while agent processes are running.	Use the same methods that you used when you brought the network up to restart XTS or X25, enable the links, and restart the agent processes.
A user's terminal hangs after an RMA request.	Like other CLI commands, commands that invoke RMA services must complete before the terminal returns to CLI control. If RMA fails, the operating system will wait indefinitely for a system call from RMA that indicates the fulfillment of the command's request. On an AOS system, abort the process by entering the control sequence, CTRL-C CTRL-B. On an AOS/VS system, abort the process by entering the control sequence, CTRL-C CTRL-A. If the RMA request involved remote queueing, and therefore remote EXEC, you can bring the network down to get control of the console with less potential change to the process on the terminal.
An RMA surrogate process fails.	A message reports the reason for termination to the output console.
FTA fails.	Restart FTA on the host on which it failed.
SVTA fails.	The transport service sends a message to UVTA users with outstanding connections. EXEC automatically disables all virtual consoles and sends the message, *@VCONconsole-number DISABLED*, to the operator's console. You can now restart SVTA.

Problem	Comment
You get the error message *DTE Clearing.*	This error is on a remote host.
You get the error message *HDLC initialization error. Hard error.*	This error is often caused by problems on a communications board. Consult your Data General support organization.
You get *RESTART - network is operational* messages.	The RESTART message does not indicate error conditions. Restarts are routine under certain circumstances.

Restarting Individual Processes

Table C-2 shows how to start individual processes after failure. The table shows commands in their simplest possible format. For information on all of a command's switches and arguments, refer to the command descriptions in Chapters 9 through 13.

Table C-2. Restarting Network Processes

Process	How to Restart
NETOP	Bring up the network.
X25	Start X25:) CONTROL @X25 START ↓ Enable each link:) CONTROL @X25 ENABLE linkname ↓
XTS	Start XTS:) CONTROL @XTS START ↓ Enable each link:) CONTROL @XTS ENABLE linkname ↓
RMA	Start RMA, making both URMA and SRMA available:) CONTROL @RMA START ↓
SVTA	Start SVTA, using the /VCONS switch if you want to create more or fewer virtual consoles than the default, five:) CONTROL @SVTA START ↓ Enable the virtual consoles:) CONTROL @SVTA ENABLE @VCON(0,...,n) ↓
FTA	Start FTA, enabling both UFTA and SFTA:) CONTROL @FTA START ↓

Physical Problems

When you suspect physical problems as the cause of network problems, you can check three groups of hardware:

- modems
- controllers
- cables

Modems

When you cannot enable a link on a synchronous line using a modem, check the modem's indicator lights. First, the MODEM READY light should be on to indicate that the modem is powered up. The DATA TERMINAL READY and CLEAR TO SEND lights should also be on. These lights indicate the modem's acknowledgement of the link. If these lights are off, check the modem cabling. If the cabling is not faulty, the modem itself may be the problem. Recurring *Link Restart in Progress* messages may indicate modem problems.

If your modem's CARRIER DETECT or RECEIVE READY light goes out, the remote modem is not sending carrier signals. The problem may be with the remote modem or the cabling between the two modems.

Controllers

When you attempt to enable a link on an intelligent controller that has a hardware problem, the ENABLE command returns an error.

Sometimes errors can be traced back to the NETGEN files. The message *DEVICE DOES NOT RESPOND* may indicate that you incorrectly entered a controller's device code during your NETGEN session. Check the device code by executing NETGEN and viewing the specification file.

If the controller board has two lines, you can physically swap ports on the board and use NETGEN to swap the links. If a link was bad on one line, but can now be enabled on another line, the problem may lie with the original port on the board.

The messages — *CONTROLLER LOAD SEQUENCE FAILED, PARITY ERROR IN SERIAL LOAD COMMAND*, and *CONTROLLER FAILED MEMORY CHECK* — reflect hardware errors for which you must call your Data General support organization.

An NBS device is a special case. It has two classes of errors: initialization errors and connect errors. Each error message has the prefix *NBS INIT* or *NBS CONNECT*. An NBS INIT error indicates failure on the NBS controller board. An NBS CONNECT error indicates failure of the wall box or cable.

Refer hardware problems to your Data General support organization.

Cables

Cables are an obvious but likely cause of hardware problems. If cables are hidden from view, and hardware problems seem likely, you may find it useful to check the cables' entire length. A breakout box lets you check signals at various places in the network and is an excellent tool for finding out where on a network an error is occurring.

Files that Document Errors

XODIAC has methods for handling the usual problems that can occur on a network. If an unexpected error occurs, however, you might have to submit a Software Trouble Report (STR) to Data General. With the STR, you include the following files:

- break files
- dumps of intelligent controllers
- log files
- NETGEN specification files

Break Files

If an unexpected error occurs, the process causing the error terminates, dumping memory to a file. This file is called a *break file.*

Either XODIAC or the operating system can create the break file, depending on the nature of the error. When XODIAC creates the file, its name has the format

?process-name_month.date_time_error-code.BRK

If FTA terminated on October 25 at 22:49, the filename might be

?FTA_10.25_11.49_000213110.BRK

When the operating system creates the file, its name has the format

?pid.hours_minutes_seconds.BRK

For example, if the error occurred on PID 12, the break file name might be

?012.13_57_26.BRK

Break files are placed in the :NET directory, with the following exceptions:

- UVTA break files are placed in the user's current working directory.
- Break files that result from errors of a surrogate process are placed in the user directory, :UDD:username.

Intelligent Controller Dumps

If a problem occurs on an intelligent controller, you can take a memory dump of that controller by one of the following methods:

- If XTS is the current owner of the controller, you can use the XTS DUMP command.
- If X25 owns the controller, or if XTS no longer owns the controller (because, for example, the controller has gone down), you can use the dump macros in Table C-3. These macros create memory dumps from ILCs, ISCs, IBCs, LSCs, and MCP1s.

Table C-3 lists the macros that dump the memory of intelligent controllers. These macros are in the directory :NET:UTIL.

Table C-3. Dump Macros

Device	Macro	Format for Break File Name
ILC IBC	ILCDUMP.CLI	?pid.hh_mm_ss_ILC.BRK
ISC MCP1 LSC	ISCDUMP.CLI	?pid.hh_mm_ss_ISC.BRK

The macro will ask you for the controller's device code. Enter the same code that you gave the device in the device configuration file that your NETGEN session created.

Log Files

Network processes other than NETOP and UVTA also report errors to log files, if you previously enabled logging. You will find log files useful if errors occur, since console messages may be overlooked when they appear.

Specification Files

Your Software Trouble Report should also include the network specification file, which contains information needed for duplicating and solving the problem.

End of Appendix

Index

Within this index, f or ff after a page number means "and the following page" (or "pages"). In addition, primary page references for each topic are listed first. Commands, and acronyms are in uppercase letters (e.g., START).

E

F

G

M

N

O

S

Data General Corporation, Westboro, MA 01580

093-000260-02