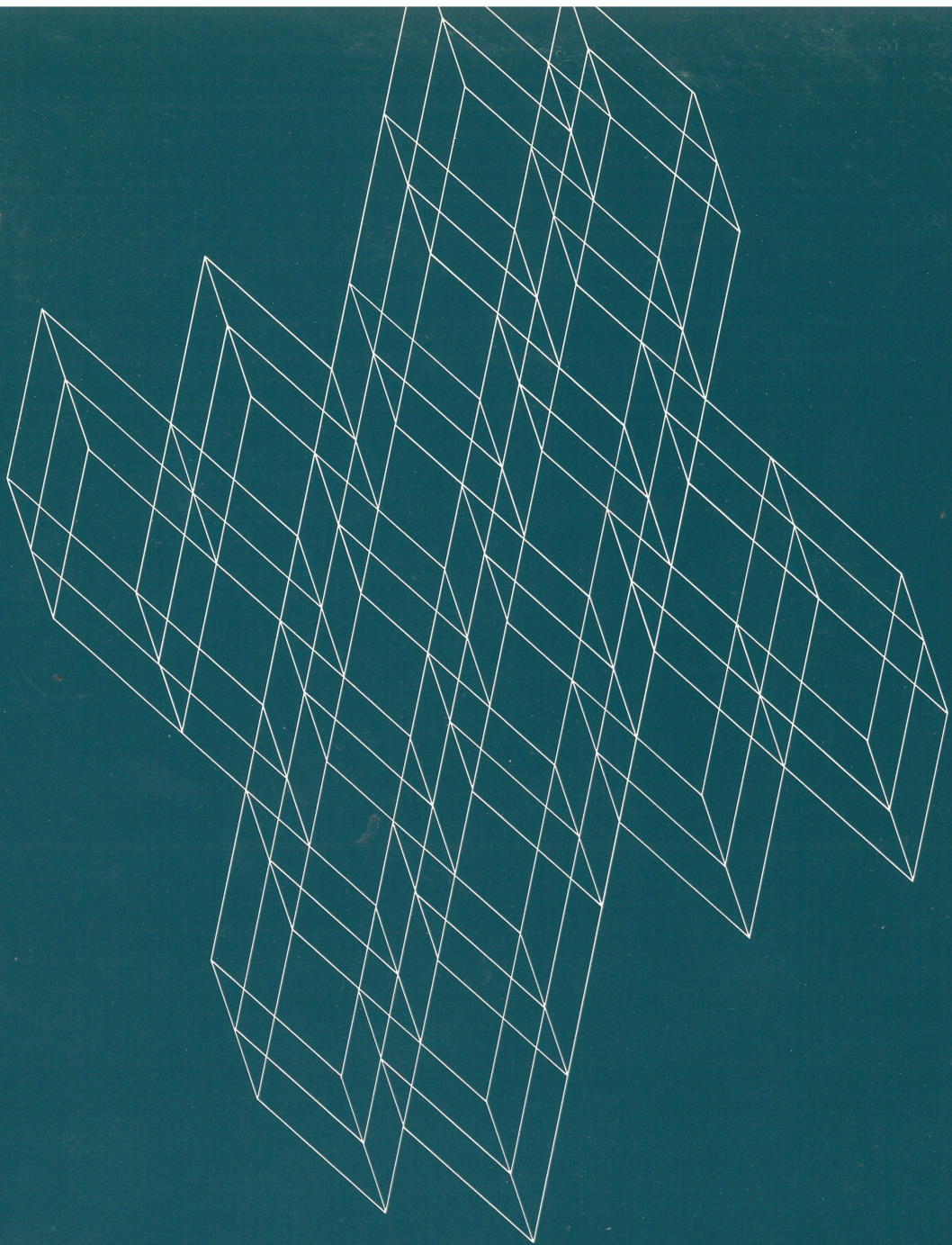




**Bridge
Communications
Inc.**

Connection Service User's Guide



BRIDGE COMMUNICATIONS, INC.

CONNECTION SERVICE USER'S GUIDE

09-0063-01

August 1986

©1986 by Bridge Communications, Inc. All rights reserved. No part of this publication may be reproduced, in any form or by any means, without the prior written consent of Bridge Communications, Inc.

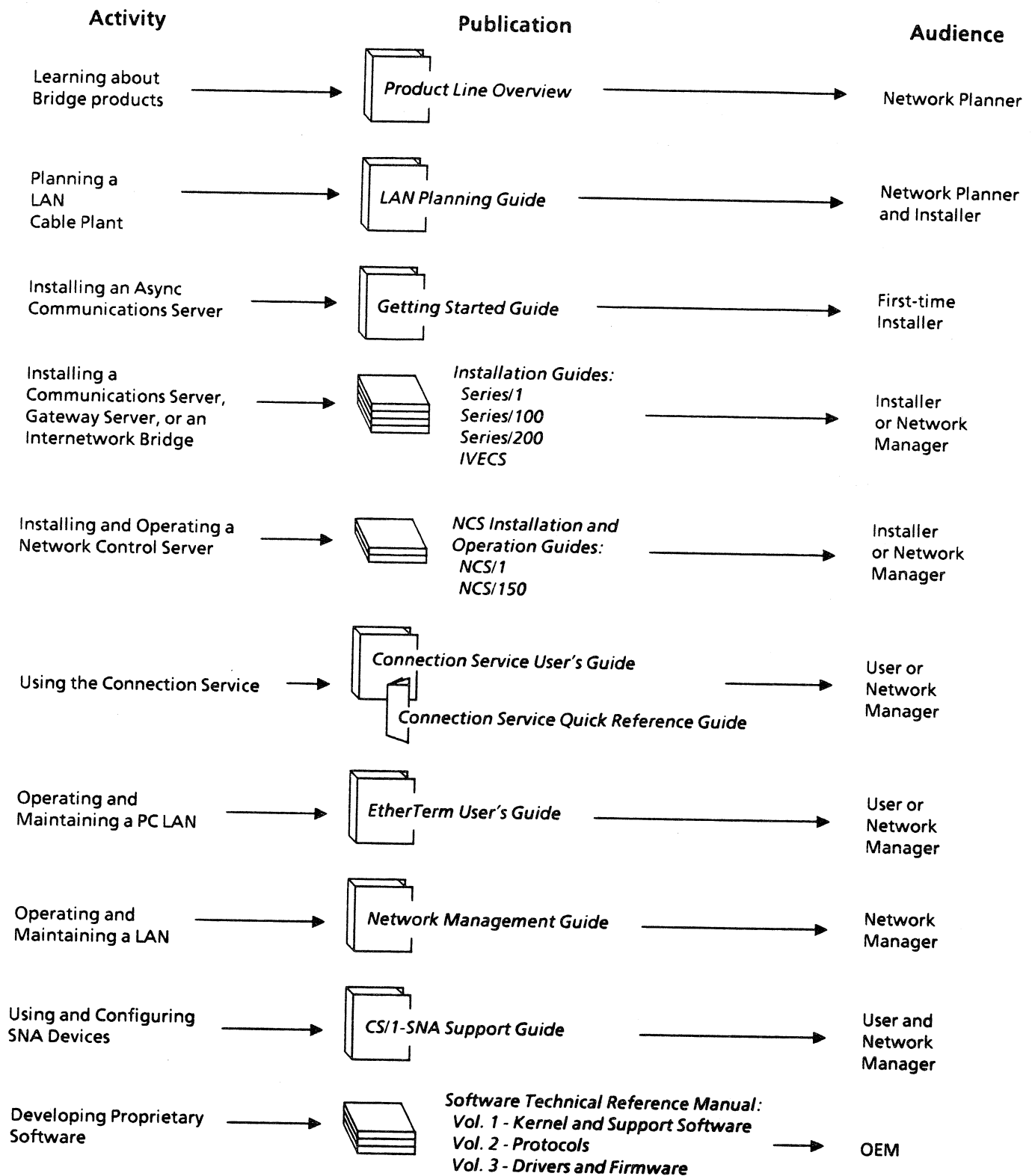
Bridge Communications, Inc., reserves the right to revise this publication and to make changes in content from time to time without obligation on the part of Bridge Communications to provide notification of such revision or change.

Comments on this publication or its use are invited and should be directed to:

Bridge Communications, Inc.
Attn: Technical Publications
2081 Stierlin Road
Mountain View, CA 94043

**** WARNING ****

This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instructions in this manual, may cause interference to radio communications. It has been tested and found to comply with the limits for a Class A computing device pursuant to Subpart J of Part 15 of FCC Rules, which are designed to provide reasonable protection against such interference when the equipment is operated in a commercial environment. Operation of this equipment in a residential area is likely to cause interference, in which case the user at his or her own expense will be required to take whatever measures may be required to correct the interference.



PUBLICATION CHANGE RECORD

This page records all revisions to this publication, as well as any Publication Change Notices (PCNs) posted against each revision. The first entry posted is always the publication's initial release. Revisions and PCNs subsequently posted are numbered sequentially and dated, and include a brief description of the changes made. A revision always incorporates both the previous revision and any PCNs posted against it. The part numbers assigned to revisions and PCNs use the following format:

aa-bbbb-cc-dd

where "aa-bbbb" identifies the publication, "cc" identifies the revision, and "dd" (if present) identifies the PCN.

Change bars are used in page margins to indicate changes made to the technical content of the publication since the previous PCN or revision.

Part Number	Date	Description	Affected Pages
09-0063-00	01/86	First Release	All
09-0063-01	08/86	Second Release; reflects the following software releases: SW/1/A-BSC-SDLC release 20050, SW/100/A-BSC-SDLC release 20050, SW/200 release 20050, and release of the Internetwork Bridges	All

PREFACE

This guide provides the information necessary to use the Bridge Communications Connection Service.

Planning and installation instructions for each server appear in its *Planning and Installation Guide* or in the *LAN Planning Guide* and appropriate *Installation Guide*.

Most Connection Service users need only the information that appears in this manual and in the *Getting Started Guide*. The system installer and network manager also need the technical information that appears in the appropriate *Installation Guide* for the product, and in the *Network Management Guide*. If the installation includes a Network Control Server, the network manager also needs the appropriate *Network Control Server Installation and Operation Guide*.

This guide is grouped into the following major sections and appendices:

- Section 1.0 Introduction: Describes the purpose and scope of this guide and offers recommendations on how to use it.
- Section 2.0 Connection Service Overview: Describes the Connection Service and explains where the Connection Service is available on the network.
- Section 3.0 Connection Service Command Guide: Describes command format and syntax, provides a complete description of each command, and lists the error messages generated for each command by the Connection Service.
- Section 4.0 Port Configuration: Describes port configuration parameters for asynchronous or 3270 ports on the Communications Servers and for virtual ports on the Gateway Server/1.
- Appendix A Contains a comprehensive list of error messages generated by the Connection Service.
- Appendix B Describes setup mode for the SIO-3270.
- Appendix C Describes making connections involving the GS/1 and CS/1-X.25.

CONTENTS

1.0	INTRODUCTION.....	1-1
1.1	Purpose and Scope	1-1
1.2	How to Use This Guide	1-1
2.0	CONNECTION SERVICE OVERVIEW	2-1
2.1	The Connection Service.....	2-1
2.2	Software Configuration	2-4
2.3	Connection Service Features.....	2-5
2.3.1	Connections Among Different Server Types	2-5
2.3.2	Session Management	2-7
2.3.3	Physical and Virtual Ports.....	2-8
2.3.4	Modes of Operation	2-9
2.3.5	Privilege Levels.....	2-11
2.3.6	Help Facility.....	2-12
2.3.7	Macro Facility	2-13
2.3.8	Naming Ports and Rotaries.....	2-14
2.3.9	Access Control.....	2-16
2.3.10	Call Queueing.....	2-16
2.3.11	Audit Trail.....	2-17
2.3.12	Access to the Network Management Functions.....	2-18
2.4	Connections Involving a GS/1 or CS/1-X.25	2-19
2.5	Diskless Systems	2-22
2.6	Software and Firmware Release Numbers.....	2-24
3.0	CONNECTION SERVICE COMMAND GUIDE.....	3-1
3.1	Command Format and Syntax	3-1
3.1.1	Format	3-1
3.1.2	Special Characters	3-2
3.1.3	Command Abbreviation.....	3-4
3.1.4	Syntax Notation	3-5
3.1.5	Specifying Parameter Values.....	3-6
3.1.6	Specifying XNS Ethernet Addresses	3-8
3.1.7	Establishing and Using Clearinghouse Names	3-10
3.1.8	Specifying TCP Addresses	3-11
3.1.9	Establishing and Using TCP/IP Internet Names.....	3-13
3.2	Commands.....	3-14
3.2.1	Broadcast Command	3-16
3.2.2	Connect Command	3-17
3.2.3	DEFine Command.....	3-21
3.2.4	DEQueue Command	3-25
3.2.5	DisConnect Command	3-26
3.2.6	DO Command	3-27
3.2.7	Echo Command	3-28
3.2.8	Listen Command	3-29
3.2.9	Name Command.....	3-30
3.2.10	Pause Command	3-33
3.2.11	ReAD Command.....	3-34
3.2.12	REMOTE Command	3-36

3.2.13	REMOteSET Command.....	3-38
3.2.14	REMOteSHoW Command.....	3-39
3.2.15	RESume Command.....	3-40
3.2.16	ROtary Command.....	3-41
3.2.17	SAVe Command	3-43
3.2.18	SEt Command	3-45
3.2.19	SEtDefault Command.....	3-47
3.2.20	SHoW Command	3-49
3.2.21	SWitch Command.....	3-55
3.2.22	TranSMit Command.....	3-56
3.2.23	UNDefine Command	3-57
3.2.24	UNName Command	3-58
3.2.25	UNSave Command.....	3-59
3.2.26	ZeroStats Command.....	3-60
4.0	PORT CONFIGURATION	4-1
4.1	Asynchronous and 3270 Server Configuration Parameters	4-4
4.1.1	Asynchronous and 3270 Port Transmission Parameters	4-6
4.1.2	Asynchronous Port Physical Parameters.....	4-11
4.1.3	Asynchronous and 3270 Session Transmission Parameters	4-14
4.1.4	Session Editing Parameters.....	4-21
4.1.5	Global Parameters.....	4-23
4.1.6	Asynchronous Host Configuration.....	4-26
4.1.7	Asynchronous Terminal Configuration.....	4-26
4.1.8	Asynchronous Modem Control Lines.....	4-29
4.2	GS/1 Virtual Port Configuration Parameters.....	4-32
4.2.1	GS/1 Port Transmission Parameters	4-33
4.2.2	GS/1 Port Physical Parameters.....	4-37
4.2.3	GS/1 Session Transmission Parameters	4-38
4.2.4	GS/1 Session Editing Parameters	4-42
4.2.5	GS/1 Global Parameters.....	4-43
4.2.6	Bridge Implementation of X.3 Protocol.....	4-44
APPENDIX A	CONNECTION SERVICE ERROR MESSAGES.....	A-1
A.1	Text Messages.....	A-1
A.2	Error Codes.....	A-14
APPENDIX B	3270 SETUP MODE.....	B-1
B.1	Setup Mode Commands.....	B-1
B.2	Main Menus	B-2
B.2.1	Main Menu 1 Options	B-3
B.2.2	Main Menu 2 Options	B-6
B.2.3	Main Menu 3 Options	B-8
B.3	Submenus.....	B-10
B.3.1	Tab Setting Submenu	B-10
B.3.2	Function Keys Submenu	B-11
B.3.3	Keyboard Definition Submenu.....	B-13

APPENDIX C CONNECTIONS INVOLVING A GS/1 OR CS/1-X.25	C-1
C.1 PDN Terminal to LAN Host	C-3
C.1.1 Using the Connection Service	C-3
C.1.2 Using the Automatic Connection Service.....	C-3
C.2 LAN Terminal to PDN Host	C-5
C.3 PDN Host to X.25 LAN Host	C-6
C.4 X.25 Host to X.25 Host	C-8
INDEX	Index-1

TABLES

2-1 Typical Connections Among Some Server Types.....2-7

2-2 Software Release Number Prefixes.....2-24

2-3 Firmware Release Number Prefixes.....2-25

3-1 Notation of Keyboard Symbols3-2

3-2 Default Local Editing Characters.....3-3

3-3 Conventions for Entering Numbers.....3-6

3-4 Conventions for Entering Strings.....3-7

3-5 Form Effectors in String Text.....3-7

3-6 TCP/IP Address Format.....3-11

3-7 Connection Service Command Summary3-15

4-1 Asynchronous and 3270 Configuration Parameter Summary4-5

4-2 Asynchronous and 3270 Port Transmission Parameters4-6

4-3 Asynchronous Port Physical Parameters.....4-11

4-4 Asynchronous and 3270 Session Transmission Parameters4-15

4-5 Editing Parameters4-21

4-6 Global Parameters.....4-23

4-7 Recommended Settings of UseDCDout and UseDTRin4-31

4-8 GS/1 Configuration Parameter Summary4-32

4-9 GS/1 Port Transmission Parameters4-33

4-10 GS/1 Port Physical Parameters4-37

4-11 GS/1 Session Transmission Parameters.....4-38

4-12 GS/1 Session Editing Parameters.....4-42

4-13 GS/1 Global Parameters.....4-43

4-14 Bridge-to-X.3 Parameter Conversions4-44

A-1 Brief Mode Error Codes.....A-15

B-1 ASCII Codes Generated in Available LanguagesB-4

C-1 Format of Call User Data Area.....C-7

FIGURES

2-1	Establishing a Virtual Circuit.....	2-2
2-2	Terminal Port Modes of Operation.....	2-10
2-3	Typical Help Facility Dialogue.....	2-12
2-4	Difference Between Local and Global Rotaries.....	2-15
2-5	Network with GS/1 and CS/1-X.25s.....	2-19
4-1	Effects of the ReaD, SAve, SET, and SETDefault Commands.....	4-3
4-2	Effect of UseDCDout Parameter Settings.....	4-30
B-1	Main Menu 1.....	B-3
B-2	Main Menu 2.....	B-6
B-3	Main Menu 3.....	B-8
B-4	Tab Setting Submenu.....	B-10
B-5	Function Keys Submenu.....	B-11
B-6	Keyboard Definition Submenu.....	B-13
C-1	Network with GS/1 and CS/1-X.25s.....	C-2
C-2	Format of X.25 Call Request Packet.....	C-6

1.0 INTRODUCTION

This guide provides the information necessary to configure and use the Bridge Connection Service within a Bridge Communications, Inc., network environment.

This section defines the purpose, scope, and audience of the publication and offers recommendations on how to use this guide.

1.1 Purpose and Scope

The information in this publication has been prepared for the customer who uses the Connection Service available on Communications and Gateway Servers. The Connection Service is a turnkey service and requires no programming or other enhancement by the user.

Information about the X.25 Automatic Connection service is provided in this guide for the user interacting with the Connection Service via a CS/1-X.25 or a Gateway Server/1.

Most interactions initiated by the user or network manager are accomplished through Connection Service commands. These commands are issued from a terminal or a packet assembly/disassembly (PAD) device, depending on the server type, to create or terminate connections, to specify port characteristics, and to perform network administration. Some network management functions, however, are accomplished through the system monitor or a utilities diskette. Network administration and management functions are discussed in detail in the *Network Management Guide*.

Information about the physical installation and hardware configuration of each server is provided in its *Planning and Installation Guide* or in the *LAN Planning Guide* and appropriate *Installation Guide*.

1.2 How to Use This Guide

This publication provides a comprehensive list of the Connection Service commands and describes configuration parameters for asynchronous or 3270 ports on the Communications Servers and for virtual ports on the Gateway Server/1. The material in this guide is grouped into the following major sections:

- *Background Information.* Section 2.0 provides an overview of the Connection Service software and explains where the service is available on the network.
- *Command Guide.* Section 3.0 describes the format and syntax of the Connection Service commands, provides a complete description of each command with examples of how the command is used, normal system responses, and possible error messages.
- *Port Configuration Parameters.* Section 4.0 describes port configuration parameters for Communications Servers with asynchronous or 3270 interfaces and virtual port configuration procedures for the Gateway Server/1.
- *Error Messages.* Appendix A provides a comprehensive list of error messages.
- *CS/1-3270 Setup Mode.* Appendix B describes setup mode for the CS/1-3270.
- *Connections Involving a GS/1 or CS/1-X.25.* Appendix C describes the types of connections that involve these servers and the steps required to automate some of these connections.

2.0 CONNECTION SERVICE OVERVIEW

This section describes the major features and uses of the Connection Service software. The section contains a summary of the following:

- How the Connection Service is used on each server
- The steps necessary to configure the software for Communications Server ports with asynchronous or 3270 interfaces and virtual ports on the Gateway Server/1
- The features of the Connection Service
- Connections involving a GS/1 or CS/1-X.25
- Special considerations for diskless systems
- Software and firmware release numbers

Configuration information for Communications Server ports with asynchronous or 3270 interfaces and virtual ports on the Gateway Server/1 is covered in detail in Section 4.0. Configuration information for all other servers is provided in the *Network Management Guide*.

Throughout this guide, the generic term "server" is used to include Communications Servers and Gateway Servers, except where otherwise indicated. Where information applies to a particular product, the server model or interface type is included for clarity.

Connection Service commands are described in detail in Section 3.0.

2.1 The Connection Service

The Connection Service is the software that enables servers to communicate with each other and enables terminals, hosts, and other computer equipment to communicate with the servers. This software runs on the GS/1 and on every Communications Server, including those to which no terminals are attached, such as host servers (e.g., the IVECS or CS/1-SNA).

The Connection Service runs on the server at each end of a connection, sending data from the origin and receiving data at the destination. The service is involved at the user end of a connection, at the host end of a connection, and when a server is accessed in remote mode. This guide describes the Connection Service as it operates in each of these circumstances.

To understand how a connection is established, consider Figure 2-1. This figure is used to show how three different connections are established:

- Terminal A to host1 (CS/100 to IVECS)
- Terminal A to host2 (CS/100 to GS/1)
- Terminal B to host1 (GS/1 to IVECS)

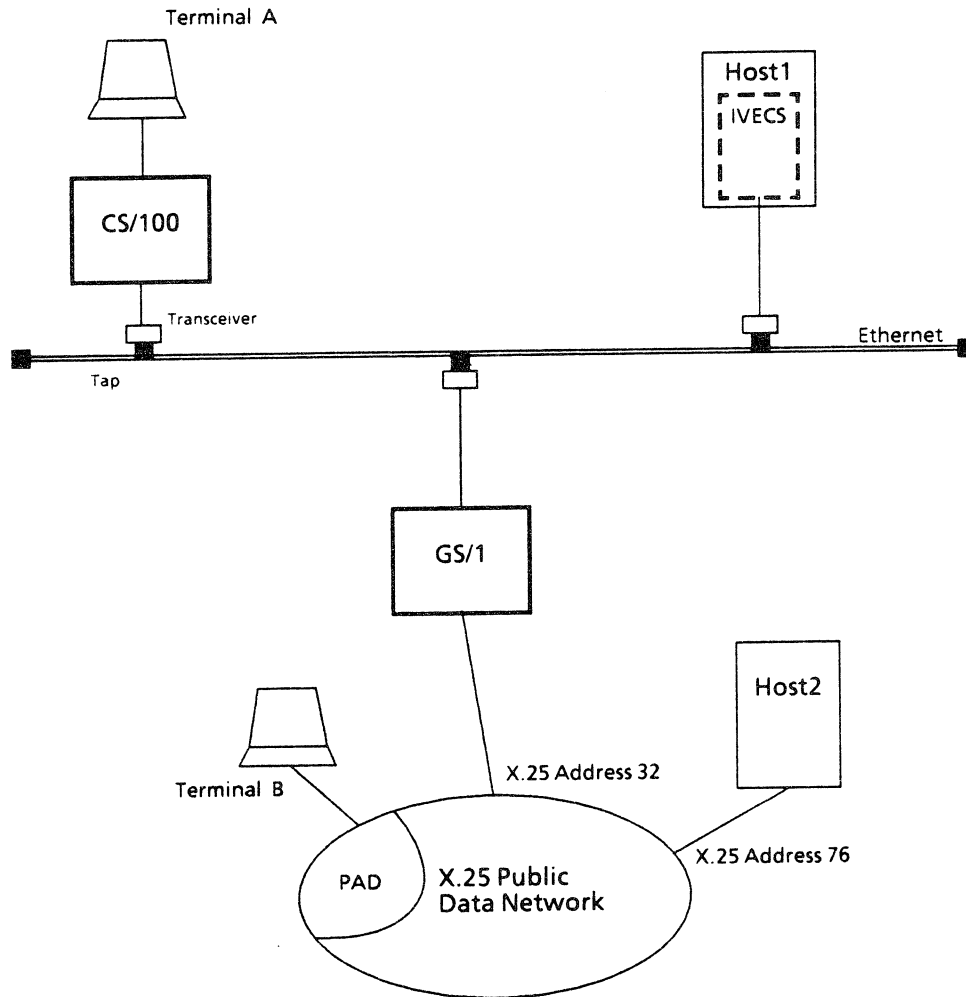


Figure 2-1 Establishing a Virtual Circuit

Terminal A to Host1

Suppose a user at terminal A in Figure 2-1 enters the following command:

Connect Host1

The Connection Service running on the CS/100 determines the address of Host1 and then tells the Connection Service running on the IVECS to open a connection on an IVECS port. The Connection Service running on the IVECS notifies Host1 of the connection request and then tells the CS/100 that the connection is open. The CS/100 outputs the following message to terminal A:

`session <n> -- connected to Host1`

Terminal A and Host1 now communicate via this logical connection.

Terminal A to Host2

Suppose a user at terminal A in Figure 2-1 enters the following command:

```
Connect Host2
```

The Connection Service running on the CS/100 determines the address of Host2 (in this case, the address of the Gateway Server through which the host may be accessed plus the X.25 address of the host itself). It then tells the GS/1 to open a connection to X.25 address 76. The GS/1 issues an X.25 call to Host2 and Host2 responds to the request. The Connection Service running on the GS/1 then tells the Connection Service running on the CS/100 that the connection is open. The CS/100 outputs the following message to terminal A:

```
session <n> -- connected to Host2
```

Terminal A and Host2 now communicate via this logical connection.

Terminal B to Host1

Suppose a user at terminal B in Figure 2-1 connects to the GS/1 (X.25 address 32) through the PAD and then enters the following command:

```
Connect Host1
```

The Connection Service running on the GS/1 determines the address of Host1 and then tells the Connection Service running on the IVECS to open a connection on an IVECS port. The IVECS notifies Host1 of the connection request and then tells the GS/1 that the connection is open. The GS/1 outputs the following message to terminal B:

```
session <n> -- connected to Host1
```

Terminal B and Host1 now communicate via this logical connection.

2.2 Software Configuration

Once a server has been installed according to the instructions in the appropriate *Installation Guide*, some software configuration may be necessary. The server has two sets of software-controlled parameters: system generation parameters and configuration parameters.

System generation parameters apply to the server as a whole and typically need to be changed only once for a given installation, usually by the network manager. The parameters are modified through the Sysgen program described in the *Network Management Guide*.

Configuration parameters, which apply to individual ports or to the whole server, may need to be changed more frequently than system generation parameters. Configuration parameters can be changed dynamically by the user through the SET, SETDefault, and REMoteSET commands (described in Section 3.2). After the network manager runs the Sysgen program, default values for the configuration parameters should be adjusted to reflect local requirements (Section 4.0 describes configuration parameters).

2.3 Connection Service Features

The Connection Service provides a collection of commands for performing the following basic functions:

- Establishing and terminating connections between different devices on one or more networks
- Examining and altering configuration parameters (e.g., device type, baud rate, parity, flow control, data forward conditions, and local editing capability)
- Sending and receiving in-band and out-of-band signals (e.g., interrupts)
- Switching among multiple connections
- Assigning and using a logical name service
- Establishing an X.25 automatic connection service
- Examining error and traffic statistics

Connection Service commands are available locally to each port configured to support an asynchronous terminal device on a Communications Server or to a virtual port configured on a GS/1. A subset of the Connection Service commands is available when accessing a server in remote mode as a network manager. To obtain a list of commands available during direct or remote access, enter a question mark (?).

Remote mode access is described in Section 2.3.12. Connection Service commands are described in detail in Section 3.2.

2.3.1 Connections Among Different Server Types

Except for protocol transparent servers like the Internetwork Bridges, every server belongs to one of two groups, depending on which high-level protocols it supports. The two sets of high-level protocols are Xerox Network Systems (XNS) and Transport Control Protocol/Internet Protocol (TCP/IP). Communication between members of the same group is supported; however, communication between members of different groups is not.

All servers provide an interface between a network and a variety of different devices. The following Communications Servers support the XNS protocols:

- Communication with asynchronous devices is accomplished through the CS/1 with an SIO-A, SIO-16, or SIO-3270 interface; the CS/100 with an asynchronous interface; the CS/1-HSM; the CS/200; and the IVECS.
- Communication with character-synchronous devices is accomplished through the CS/1 or CS/100 with a bisynchronous interface.
- Communication with Sperry character-synchronous terminal devices is accomplished through the CS/1 with a bisynchronous interface running SPMUX multiplexer software; communication with the Sperry character-synchronous host is accomplished through the standard CS/1 with a bisynchronous interface.
- Communication with bit-synchronous devices is accomplished through the CS/1 with a bit-synchronous interface.
- Communication with an SNA host is accomplished through the CS/1-SNA.

- Communication with an X.25 host or network is accomplished through the CS/1-X.25 and the GS/1.

The following Communications Servers support the TCP/IP protocols:

- Communication with asynchronous devices is accomplished through the CS/1 with an SIO-A, SIO-16, or SIO-3270 interface; the CS/100 with an SIO-A interface; and the CS/200.
- Communication with character-synchronous devices is accomplished through the CS/200.
- Communication with an SNA host is accomplished through the CS/1-SNA.

A single CS/1 may provide more than one kind of device interface. For instance, a CS/1 may contain one asynchronous SIO board and two synchronous SIO boards, and thus be able to provide network connections to asynchronous, character-synchronous, and bit-synchronous devices. Or, for example, a CS/1 may contain one SIO-A board and two SIO-16 boards, for a total of 40 asynchronous ports, plus an SIO-3270 board for communication with 3270 display stations. However, each individual SIO board in the CS/1 supports only one kind of interface. The CS/100 does not support hybrid interfaces.

The Connection Service commands are available to ports configured as asynchronous terminal ports and to virtual ports configured on the GS/1. Some of the commands are available on other servers when accessed in remote mode.

Connections between an asynchronous terminal port and another device can be established with a connection request issued at the terminal. Connections among non-asynchronous devices (e.g., from a port on one CS/1 with bisynchronous interface to a port on another CS/1 with bisynchronous interface) can be established remotely via a third-party connection request from an asynchronous terminal port or virtual port on a GS/1, locally via a port initialization macro, or via the PermanentVC parameter. Section 3.2.2 describes the Connect command; macros are covered in Section 2.3.7 and in the *Network Management Guide*; the PermanentVC parameter is described in Section 4.1.1.

Table 2-1 illustrates typical connections among some server types and how they are established. The table does not indicate all possible connections, only those most typical.

Table 2-1
Typical Connections Among Some Server Types

Source Server	Destination Server						
	XNS Async & 3270	XNS IVECS & HSM	XNS Bisync	XNS Bit-sync	XNS SNA	XNS X.25	TCP Async & 3270
XNS Async & 3270	d,t	d,t			d,t	d,t	
XNS IVECS & HSM	t	p,t					
XNS Bisync			t				
XNS SPMUX			t,p				
XNS Bit-sync				t			
XNS X.25	d,t	d,t			d		
TCP Async & 3270							d,t

d = Direct connection by request from source port.
t = Third-party connection by user's request at remote port, or via port initialization macro.
p = Permanent virtual circuit initiated via the PermanentVC parameter or by the system on behalf of one of the ports.

2.3.2 Session Management

A session, or virtual connection, is a logical connection between two devices through one or more servers. A session is initiated with the Connect command, usually entered on a terminal device at one end of the connection. Sessions can also be initiated by a network manager on either a local or a remote server.

The port that initiates the connection is the active end of the connection, and the destination port is the passive end. Both ports are passive if the connection is established remotely by a network manager (a third-party connection).

The user at the active end of a connection can change session parameters and disconnect the session. A host port cannot issue commands to establish or disconnect a session; it can disconnect a session only by dropping DTR. The server can terminate a session automatically after activity on the port ceases if the destination port has been configured with an automatic disconnect interval (refer to Sections 4.1.1 and 4.2.1).

In most installations, the Connection Service can be configured to allow more than one connection at a time on a single terminal port. The maximum number of simultaneous sessions permitted per port depends both on site requirements and on the high-level protocols running in the server; the number is specified at the time of system generation.

Only one session at a time is active; all other sessions are suspended and flow-controlled.

2.3.3 Physical and Virtual Ports

Communications Servers with asynchronous, character-synchronous, or bit-synchronous interfaces all offer clear-cut mapping between ports and physical lines. The server ports are numbered starting from 0. Each physical port can be connected over a physical line to an individual device. The port parameters described in Section 4.0 are designed to adjust the port to the physical needs of the attached device.

On the CS/1-HSM, the IVECS, the CS/1-SNA, the CS/1-X.25, and the GS/1, the Connection Service is provided on virtual ports rather than physical ports; the correlation between virtual ports and physical lines is more complex than that of the physical ports on the other Communications Servers.

- The CS/1-HSM supports up to 64 virtual ports on one or two physical lines. These virtual ports are numbered 32 through 95.
- The IVECS supports up to 64 virtual ports on one physical interface. These virtual ports are numbered 0 through 65; virtual ports 64 and 65 are reserved for network management access.
- The CS/1-SNA supports up to 32 virtual ports on one physical line. These virtual ports are numbered 32 through 55.
- The GS/1 and CS/1-X.25 each support up to 48 virtual ports on up to eight physical lines. These virtual ports are numbered 0 through 47.

Virtual ports have most of the properties of physical ports on the asynchronous, 3270, character synchronous, and bit-synchronous Communications Servers.

The only limitations imposed on virtual ports relate to physical characteristics. Since the virtual ports share one or more physical lines, they are restricted to the physical characteristics possessed by the line to which they are attached. Therefore, the user cannot use the SET or SETDefault commands to specify the physical characteristics of a virtual port in the same way as for a physical port on another type of server. Section 4.0 discusses port configuration and indicates the physical parameters for physical and virtual ports.

For the X.25 servers, virtual ports are not mapped directly to the number of SIO boards, the number of lines connected to the SIO boards, or the number of X.25 networks connected to the lines. For connections coming into the server from the X.25 network, the 48 virtual ports are dynamically allocated on a round-robin basis. For connections going to the X.25 network from the Ethernet network, the server assigns a virtual port number from the port numbers that have been allocated to the line going to the destination X.25 network. Virtual port numbers are allocated to physical lines through the Sysgen program, which is described in the *Network Management Guide*.

2.3.4 Modes of Operation

Each device port on a server has its own independent user interface, with three different modes of operation:

- Listening Mode
- Command Mode
- Data Transfer Mode

Each port operates independently of other ports, except when two ports are interconnected. Figure 2-2 illustrates the three modes and shows the typical commands and events that cause a port to change modes. The list below defines the modes:

- A port is in *Listening mode* before any activity takes place on the device. On Communications Servers, the port is in Listening mode when the attached device is first powered on. A virtual port on a GS/1 is in Listening mode when no connection to the port exists.

A port in Listening mode is available to become the passive end of a connection originated by another port. A terminal port in Listening mode enters Command mode as soon as any key is pressed on the attached device.

A port in any other mode reverts automatically to Listening mode if no activity takes place for the length of time specified during system generation as the Autolisten interval. A port also enters Listening mode in response to the Listen command. The Listen command can be entered locally by the user or remotely by a network manager.

When a port changes to Listening mode, an "at" sign (@) may appear on the attached device. Pressing any key on the device keyboard then causes the terminal port to enter Command mode.

A host port reverts to Listening mode whenever a session to the port is terminated.

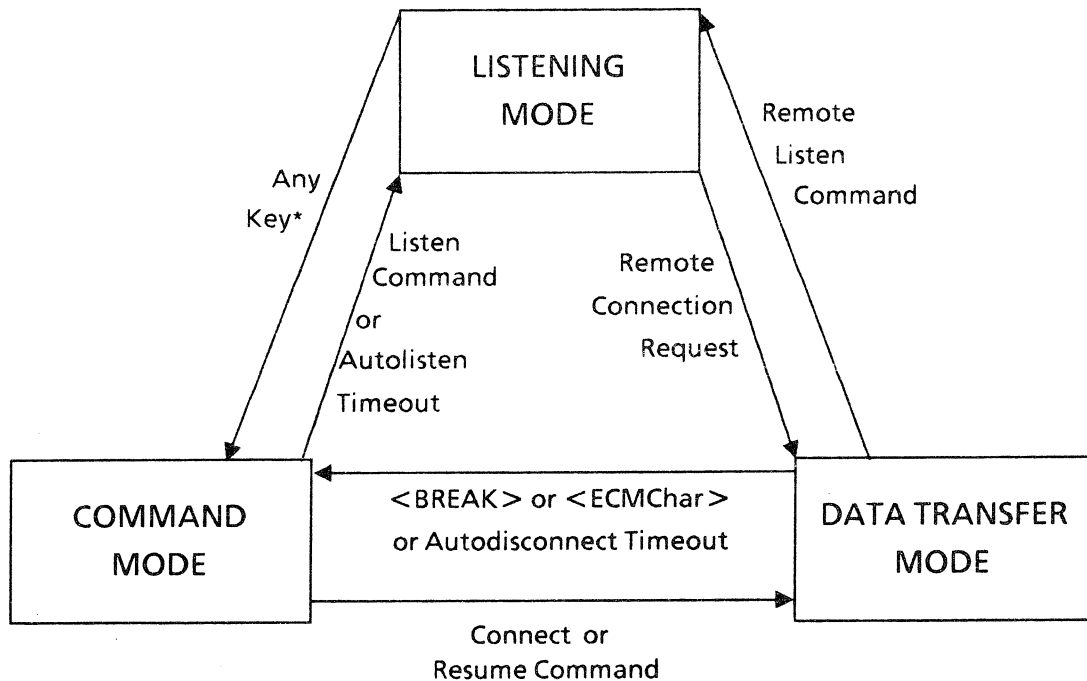
- In *Command mode*, which occurs only on a terminal port, the port responds to commands entered on the local, attached device. If the commands are performed locally (e.g., setting or altering device characteristics) or if a connection request fails, the port remains in Command mode. If the request succeeds, the port enters Data Transfer mode and subsequent input is transmitted to the destination. The port reverts to Listening mode if no activity takes place in Command mode during the specified Autolisten interval. As long as a port is in Command mode, no connections can be made to it, but connections can be formed from the port to another device. The port must be in Listening mode in order to be available for a connection.
- A port is in *Data Transfer mode* when it is actively communicating with another port. The server scans the data stream entered on the attached device for a predetermined set of attention characters; all other data is passed as entered, with no further interpretation or translation. The attention characters can be limited to the enter-command-mode character (<ECMChar>) or can include a set of local editing characters, depending on the setting of the LocalEDiting parameter (described in Sections 4.1.4 and 4.2.4).

At a port in Data Transfer mode, the user can interrupt a session with the break key (if BReakAction is set to EDTM) or the enter-command-mode character (if these parameters are set). The user's port enters Command mode, and the destination (e.g., host) port remains in Data Transfer mode. The user can then enter the RESume command to change back to Data Transfer mode, thereby resuming transmission of data to the destination. Alternatively, the user can terminate the session with the DisConnect command,

in which case the destination port returns to Listening mode and the user's port remains in Command mode.

While a device is in Data Transfer mode, no connection may be established to it from a remote device.

A host port in Data Transfer mode terminates the connection if the automatic disconnect feature is enabled and no activity is detected during the interval specified by the AUTODISCONNECT parameter (discussed in Sections 4.1.1 and 4.2.1). The host port then returns to Listening mode and the terminal port returns to Command mode. The default AUTODISCONNECT interval is 60 minutes; a different interval may be specified with the SETDEFAULT command. The automatic disconnect feature applies only to host ports.



* A defined sequence may be required; see Section 4.1.6

Figure 2-2 Terminal Port Modes of Operation

2.3.5 Privilege Levels

The commands available to a user vary depending on the user's established privilege level. Three privilege levels are available to the Connection Service user:

- User
- Local Network Manager
- Global Network Manager

A *User* ordinarily uses the Connection Service only for accessing other devices. A port with User privilege on a Communications Server, for instance, can make connections between that port and another device. A User can switch among multiple sessions, execute macros, and can change certain parameters for compatibility between the local and remote devices.

A *Local Network Manager* can create or dissolve connections between any port on the local server and any other port on the network. The Local Network Manager can also define or review port configuration parameters, set up logical names and rotaries, display the performance statistics gathered by the Connection Service, define macro files, and broadcast messages to ports on the local server.

A *Global Network Manager* can do everything the Local Network Manager can do, but for all ports and servers on the network. The Global Network Manager can also set up access groups, define the passwords used for access control, and monitor network security statistics.

A port cannot be configured for a specific privilege level. The default privilege level for all ports is always User. A higher privilege level is acquired using the SET PRIVILEGE command, which requires entry of a password.

The actual set of commands available at each privilege level can be adjusted during system generation (described in the *Network Management Guide*).

The commands available at each privilege level are described in Section 3.0; the privilege level required to execute each command is specified within the command description. The parameters that govern access control are described in Sections 4.1 and 4.2. Network statistics reports are described in the *Network Management Guide*.

2.3.6 Help Facility

The Help facility is provided as a memory aid. If the user types a question mark (?) in response to the Connection Service prompt, or after partially typing a command, the system responds with a list of all commands or parameters that are valid at that point. The Help screen always lists the command format appropriate to the user's privilege level. The list of commands and parameters differs depending on whether or not a session exists for the port.

Figure 2-3 shows a typical dialogue between the user and a Communications Server involving the help facility. In the figure, "CS/1>" represents the CS/1 prompt. For clarity in the figure, the user's input is underlined. All other text represents the server's response. This example shows the help screen that appears if a current session exists from the user's port to a host port.

```

CS/1> ?
Connect      <address>[,<address>] [ECM] [Q]
DEQueue     [<session number>]
DisConnect  [<session number>]
DO          <macro name>
Echo        <string>
Listen
Pause       [<seconds>]
REMOteSET   <param-name> = <value> ...
REMOteSHoW [<param-name>] ...
RESume      [<session number>]
SET         <param-name> = <value> ...
SHoW        <argument> ...
Switch      [<session number>]
Transmit    <string> | InBandBreak | OutBandBreak

CS/1> s?
SET         <param-name> = <value> ...
SHoW        <argument> ...
Switch      [<session number>]

CS/1> set l?
SET LFDelay      = [ None | <number> (1-127 sixtieths of a second) ]
SET LFPad        = [ None | <number> (1-127 nulls of padding) ]
SET LFInsertion  = [ None | ( OutputCrLf , EchoCrLf ) ]
SET LineERase    = [ Disabled | <char> ]
SET LocalEditing = ( [ NoDataEditing | DataEditing ]
                    , [ NoCmdEditing | CmdEditing ] )
SET LongBReakAction= [ Ignore | (Listen, OutofBand, InBand) ]

CS/1> set lfp = none

```

Figure 2-3 Typical Help Facility Dialogue

2.3.7 Macro Facility

All servers that run the Connection Service support macros, which are named files that contain a series of individual commands. Typically, the network manager defines a macro file containing the commands necessary to perform a specific function. The user executes the macro file using the DO command at any terminal device port on the network.

The Connection Service supports two kinds of initialization macros: system initialization macros and port initialization macros.

A system initialization macro is executed automatically every time the server is reset, powered on, or booted. The network manager establishes the system initialization macro by defining a macro whose name begins with the letters "init". The *Network Management Guide* discusses these special filenames in detail.

A system initialization macro can be used, for example, to establish one or more connections automatically between devices that do not have the Connection Service available (such as a host and a lineprinter, or a synchronous terminal and a synchronous host) whenever the server is booted. A system initialization macro runs at global network management level; the privilege cannot be set to a lower level in a system initialization macro. System initialization macros cannot be defined on servers that provide a host interface via one or more virtual ports (e.g., CS/1-SNA or GS/1). Therefore, a system initialization macro that connects a host attached to one of these servers and a device attached to another server must be defined on the other server.

A port initialization macro is executed every time the device attached to the port changes from Listening mode to Command mode. Port initialization macros are assigned via the InitMacro configuration parameter. A port initialization macro can be used, for example, to request a connection with a specific host and initiate the login procedure every time a user powers on the terminal.

Macros are also useful for setting configuration parameters for compatibility with different devices. If a port is used with more than one terminal, for example, a different macro can be defined for each terminal. Before switching to an alternative device, the user executes a macro to make the port compatible with that device. Similarly, macros can be defined that set up a terminal port for communication with multiple host computers having different terminal requirements.

The commands used to define, execute, and remove macros are described in Section 3.2. The InitMacro configuration parameter is described in Sections 4.1.1 and 4.2.1.

Macros are discussed in detail in the *Network Management Guide*.

2.3.8 Naming Ports and Rotaries

To simplify the process of making connections, the servers include facilities for assigning logical names to individual ports or to groups of ports called rotaries. The logical name may be either a clearinghouse name (on XNS servers) or an internet name (on TCP servers).

Assigning logical names allows the user to establish a connection to a device without knowing the network address of the device. If the logical name is associated with a rotary number that represents multiple ports to one device, the user can make a connection to the device without knowing if a specific port is available.

Logical names can be assigned to ports on any server on the network, including the following:

- a single port on a single server
- a local rotary: more than one port on a single server
- a global rotary: a set of ports on two or more different XNS servers or a combination of local rotaries that provide access to a single host

Figure 2-4 clarifies the differences between local and global rotaries by showing an example of each.

Local rotaries are useful when a number of ports are connected to one device (e.g., a host computer). If a device can be accessed through more than one port on a given server, the network manager assigns a single rotary number to the group of ports.

Global rotaries are useful when ports on more than one server are connected to one device (e.g., a host computer). The network manager establishes a global rotary by associating a logical name with a list of addresses. The addresses need not be on a single server; more than one server may be grouped into a global rotary. Each address in the list may represent a single port or a local rotary of ports. (The user can also specify a connection to a global rotary by including an address list as the destination of the Connect command.) Global rotaries are not available on servers running TCP/IP protocols.

When local or global rotaries are used, the system handles port contention and selection without repeated connection attempts by the user.

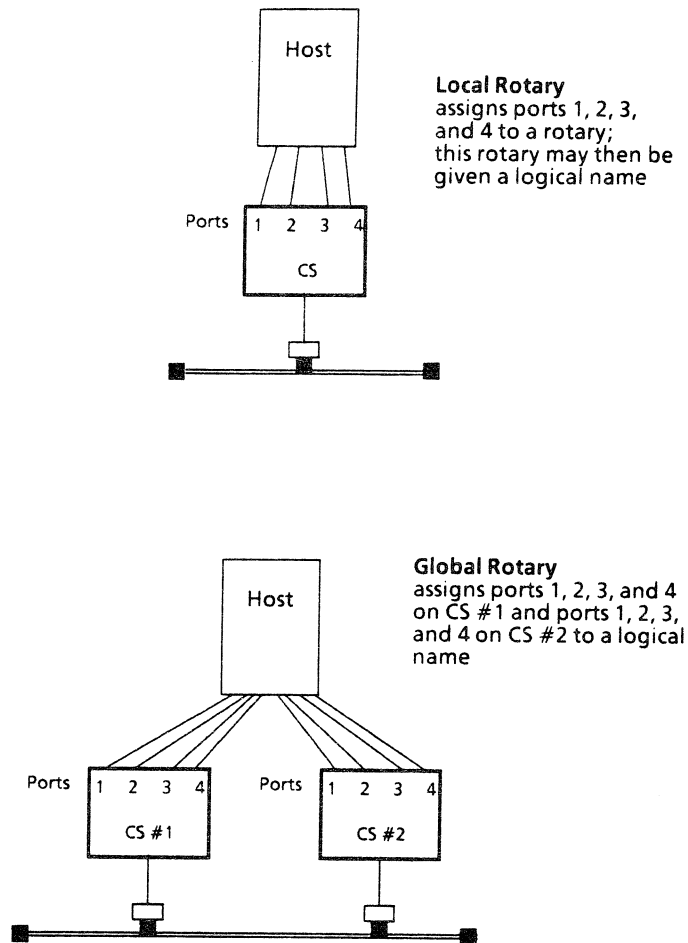


Figure 2-4 Difference Between Local and Global Rotaries

On the GS/1 or CS/1-X.25, the network manager can assign rotary numbers and logical names to virtual ports. By using the port numbers assigned to individual lines during system generation, the network manager can associate logical names and rotaries with individual lines going to the Public Data Network. This is described in detail in Appendix C.

Names and rotaries established for the virtual ports on a GS/1 are not used for communication with the server from a terminal device on a PDN. When a terminal device on a PDN initiates contact with the GS/1, the session is assigned an arbitrary virtual port number, regardless of which line on the server is being used for the communication.

The commands used to assign rotary numbers and logical names are described in Section 3.2.

2.3.9 Access Control

The Connection Service provides a way to control access to destination ports in the network by establishing access groups. Access groups are defined using the `AccessGroup`, `AccessWord`, and `GroupxPasswd` configuration parameters:

- `AccessGroup` Assigns one or more destination ports to an access group
- `AccessWord` Assigns an access word to one or more source ports
- `GroupxPasswd` Assigns a password to each access group
(where x is a group number, from 1 to 16)

These parameters determine which ports can make connections to which ports. Each of these parameters is described in Section 4.1.

When a user requests a connection to a port in an access group, the system compares the `AccessWord` of the requesting port with the `AccessGroup` of the destination port. If the `AccessGroup` and `AccessWord` match, the server completes the connection. If the `AccessGroup` and `AccessWord` do not match, the server notifies the user that the port is access-controlled and prompts for the password assigned to the access group. Unless the password is entered correctly, the connection request fails. The password is defined by the `GroupxPasswd` parameter.

For example, suppose the network manager assigns all hosts and server ports in the accounting department to one group, and all hosts and server ports in engineering to another group. A user in accounting could then access an accounting host as usual; however, any accounting user attempting to access a port in the engineering group would be required to enter the correct password before the connection could be established.

Only a Global Network Manager can establish access groups, access words, and group passwords, or display the current values of these parameters. Each server supports up to 16 access groups, 16 group passwords, and 16 access words per port. The *Network Management Guide* provides further information on access control.

Access control is not supported by TCP servers.

2.3.10 Call Queueing

The Connection Service includes a call queueing feature. If a connection request cannot be completed because the destination port is already connected with another device, the user can ask to be alerted as soon as the port becomes available. The queueing feature is invoked by adding the parameter "q" to a connection request, as described in Section 3.2.2. If the destination device is available at the time the command is entered, the connection is established immediately and the queueing request is ignored.

The system tracks all queue requests on a first-come, first-served basis. The port that has been waiting the longest is always given the next available connection. Call queueing can be invoked for connections to either a single port or a rotary port.

When a destination port with queued requests becomes available, the server puts the port in a reserved state, so that no connection can be established except by the first port in the connection queue. Meanwhile, the system sends a terminal bell signal and a message to the first port in the queue. The user at the queued port then has five minutes to complete the connection by issuing the `RESume` command. If the user fails to complete the connection, the

destination port becomes available to the next port in the connection queue, if any.

While the destination port is in a reserved state, and before the connection is completed by the user at the requesting port, a network manager at another port can interrupt the queue with the Listen command. One Listen command directed at the destination port removes the first requesting port from the queue. If only one port was in the queue, the destination port is then in Listening mode. If more than one port was in the queue, a second Listen command issued within approximately one minute removes all remaining ports from the queue and puts the destination port in Listening mode.

A user at the requesting port can remove the port from the connection queue at any time using the DEQueue command.

The commands used to queue, manipulate, and dequeue connections are described in Section 3.2.

Call queuing is not supported by the TCP servers.

2.3.11 Audit Trail

The audit trail is a record of bootstrap, connection, disconnection, and error statistics sent to a Network Control Server (NCS) by reporting Communications Servers. For networks that have one or more NCSs, the Connection Service is used to send Communications Server audit trail records to an NCS. Any Communications Server, including one not booted from an NCS, can be configured to output its audit trail to any NCS on the network that is running the same set of high-level protocols (XNS or TCP) as the server.

The audit trail is described in detail in each *NCS Installation and Operation Guide*.

The AUditServerAddr and BootServerAddr parameters govern which NCS receives a server's audit trail. The audit trail may be sent:

- To the NCS which boots the server
- To any NCS on the network, regardless of whether or not the server boots from that NCS

If the server's AUditServerAddr parameter is set to its default*, then the audit trail is sent to the address specified by the server's BootServerAddr parameter. If the server's AUditServerAddr parameter is set to any address other than the default, then the audit trail is sent to that address, regardless of the value of the BootServerAddr parameter.

To send the audit trail to the NCS which boots the server, leave the server's AUditServerAddr set to its default. The audit trail is then sent to the address specified by the server's BootServerAddr parameter, which is the address of the NCS that boots the server.

To send the audit trail to any other NCS on the network, set the AUditServerAddr parameter to the address of the desired NCS. In this case, the audit trail is sent to the specified address, regardless of the value of the BootServerAddr parameter.

* The default is the broadcast address, which specifies all servers on the network.

2.3.12 Access to the Network Management Functions

Access to the Connection Service network management functions is available through several methods. The choice of a particular access method depends on several factors:

- Type of function to be performed
- Type and location of the server affected by the procedure
- Type and location of the device from which the network manager performs the functions

The management functions, such as examining or altering port configurations, assigning logical names, and obtaining network management reports, are usually performed from a terminal attached to an asynchronous I/O port using the commands described in Section 3.2.

With Local Network Manager privilege, the network manager can perform these functions on behalf of any port on the local server. With Global Network Manager privilege, the network manager can also perform them on behalf of remote ports (provided the remote server is running the same family of protocols as the local server).

To perform a single-command function on a remote server, the network manager can access the destination server in remote mode. In remote mode, all commands entered affect the destination server until the network manager exits remote mode. However, remote mode access limits the amount of data that can be transmitted to the requesting port, and long displays such as statistical reports may be truncated.

To perform multiple-command functions remotely, or to display reports that are too long to display in remote mode, the network manager can make a connection to a special network management port on the remote server. Port number 136 on any XNS server running the Connection Service is reserved for remote network management access. When a connection is made to this special port number, the default privilege level is User. After establishing the required privilege level, the network manager has access to all of the management functions provided by the Connection Service. Port 136 supports only one connection at a time.

Access to the network management functions on an XNS server is also available from some non-Bridge devices that are attached directly to the network (e.g., personal computers running EtherTerm software). From one of these devices, the network manager can connect to port 136 on the destination Bridge Communications, Inc., server and perform any Connection Service network management functions available on that server.

The *Network Management Guide* describes network management functions in detail.

2.4 Connections Involving a GS/1 or CS/1-X.25

Connections across GS/1s and connections involving CS/1-X.25s are easily accomplished. Consider Figure 2-5, which shows a Public Data Network attached to a local area network, such as Ethernet, via a GS/1. The connections typically used in such a network configuration include the following:

- PDN terminal to LAN host: terminal P on the Public Data Network to host L on the LAN
- LAN terminal to PDN host: terminal L on the LAN to host P on the Public Data Network
- PDN host to X.25 LAN host: host P on the Public Data Network to host X1 on the LAN
- X.25 host to X.25 host: host X1 to host X2, both on the LAN

Each of these types is described in the following subsections, which refer to Figure 2-5. For details on setting up and establishing each of these types of connections, refer to Appendix C.

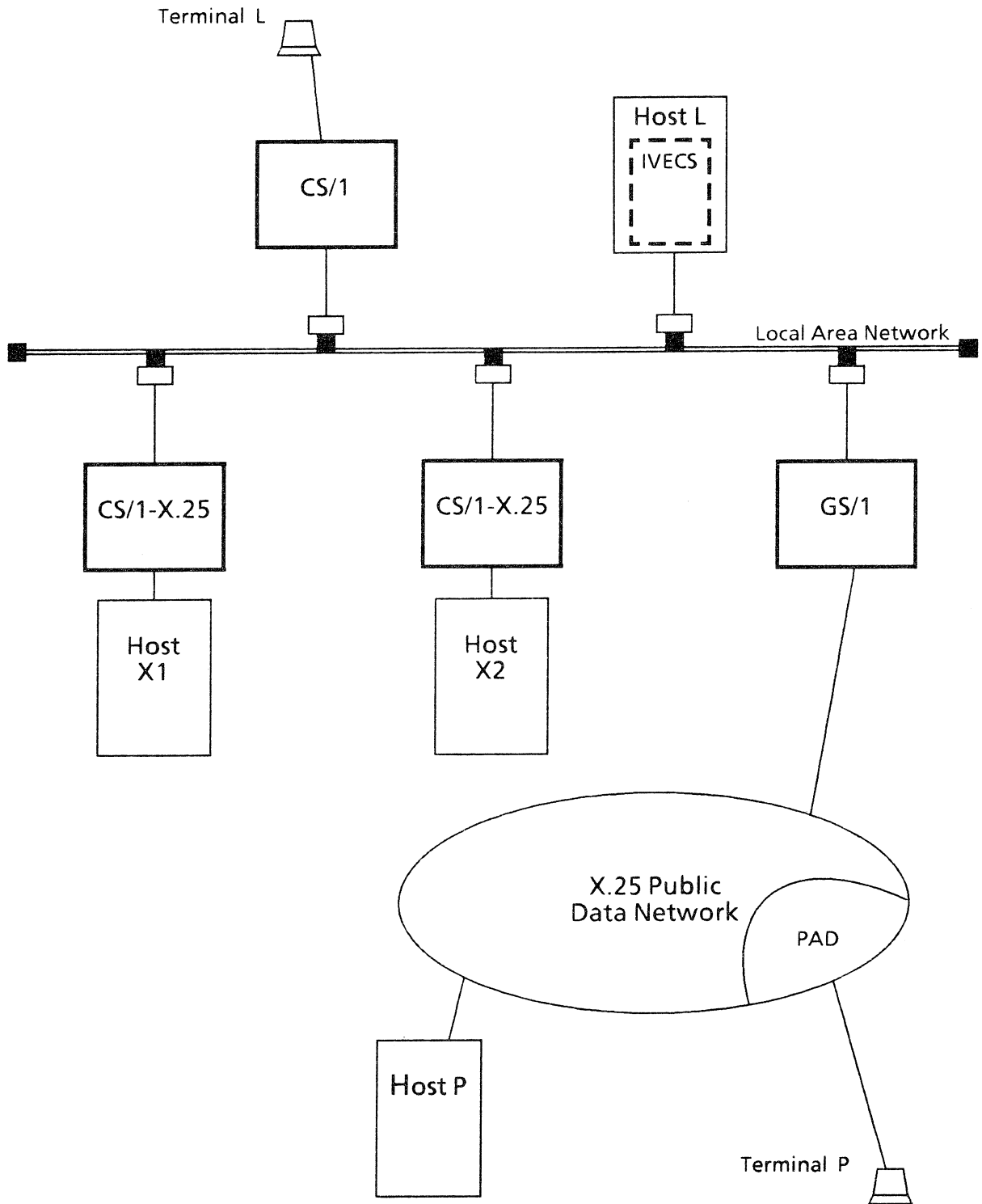


Figure 2-5 Network with GS/1 and CS/1-X.25s

PDN Terminal to LAN Host

A connection from a terminal on a PDN (such as terminal P in Figure 2-5), through a GS/1, to a host on an LAN (such as host L) may be established in two ways:

- Using standard Connection Service commands
- Using the X.25 automatic connection service

To establish the connection using standard Connection Service commands, the user at terminal P issues an X.25 call request to the X.25 address of the GS/1. The GS/1 responds with a Connection Service prompt. To complete the connection to host L, the user then issues a Connect command.

The X.25 automatic connection service automatically establishes a connection from terminal P to host L without any interaction by the user with the Connection Service. This feature enhances security on incoming calls by preventing users from accessing the Connection Service, and, as a result, from accessing any other devices on the LAN.

For information on setting up X.25 automatic connection service, refer to Appendix C.

LAN Terminal to PDN Host

A connection from a terminal attached to a Communications Server on the LAN (such as terminal L in Figure 2-5) to an X.25 host on the Public Data Network (such as host P) is established using standard Connection Service commands.

The network manager can facilitate such a connection using clearinghouse names, as described in Appendix C.

PDN Host to X.25 LAN Host

A connection from an X.25 host attached to a Public Data Network (such as host P in Figure 2-5) to an X.25 host attached to a CS/1-X.25 on the LAN (such as host X1) is established using the GS/1 call extension feature. Call extension allows a host-to-host connection through the GS/1.

This feature derives its name from the fact that the X.25 call request packet issued by host P contains an "extension" address. With call extension appropriately configured, the GS/1 automatically establishes a connection to the device indicated by the extension.

For information on setting up call extension, refer to Appendix C.

X.25 Host to X.25 Host

A connection can be established from an X.25 host attached to a CS/1-X.25 on the LAN (such as host X1 in Figure 2-5) to another X.25 host (such as host X2). The destination X.25 host may be attached to a CS/1-X.25 on the LAN or to a Public Data Network.

This type of connection requires host programming and can be facilitated using clearinghouse names, as described in Appendix C.

2.5 Diskless Systems

This section discusses the diskless systems available from Bridge Communications, Inc. Some Communications Servers are available with or without an internal disk drive option; other systems are available as diskless servers only (e.g., the CS/200 and the IVECS). Systems without an internal disk drive must be booted from an NCS.

Servers that can be supported by NCSs running the XNS protocols include the following:

- CS/1 with an asynchronous, bisynchronous, bit-synchronous, or 3270 interface
- CS/100 with an asynchronous or bisynchronous interface
- CS/200
- IVECS

Servers that can be supported by NCSs running the TCP/IP protocols include the following:

- CS/1 with an asynchronous or 3270 interface
- CS/100 with an asynchronous interface
- CS/200

Other types of servers require an internal disk drive.

In general, the Connection Service operates the same way regardless of the server's bootstrap source. There are, however, a few differences.

If a Communications Server is to be fully supported by an NCS, the NCS must first be configured to support the server. Configuration procedures for the NCSs are described in the NCS/150 and NCS/1 *Installation and Operation Guides*.

An NCS contains a separate set of configuration files for each server that it supports. Once the files are established on the NCS, the network manager can configure individual ports on the client servers by following the same procedures used on a server with a local disk drive. All servers using the services of a single NCS share a single set of logical names, access group passwords, macro files, and named configuration files. In order to define or remove a macro or to establish or delete a named configuration file, the network manager follows the same procedures used on a server with a local disk drive. Since they are all shared, the network manager should be careful not to overwrite an existing macro or configuration table established from another server supported by the same NCS.

Logical names, access groups, and Global Network Manager privilege level passwords can only be established or changed from the NCS console or while accessing the NCS in remote mode from a terminal connected to a Communications Server. Remote mode is described in Section 3.2.

Each NCS keeps a set of named configuration tables that match the sample configurations listed in Section 4.0. The network manager can use the `ReaD` and `SAve` commands in conjunction with these named files to configure individual ports for communication with various kinds of devices. Refer to Section 3.2 for examples of this process.

A Communications Server with an internal disk drive can be booted either locally or from an NCS. The early model CS/1s and CS/100s shipped with disk drives, however, do not automatically support the network bootstrap option. In order to boot from a network boot server, an early model CS/1 or CS/100 must have a firmware update. On the CS/1, network bootstrap is supported by MCPROMs designated M1 MMON 01D or later. On the

CS/100, network bootstrap is supported by MP PROMs designated T1 MMON 01D or later. For more information, contact Bridge Communications, Inc., or a qualified service representative.

2.6 Software and Firmware Release Numbers

Each server is shipped with software and firmware designed for use with that model. The software is contained on a diskette labeled with the product type and software version number. The product type and software version information is also stored as data on the diskette itself, in the form of a software release number. Firmware is contained in PROMs labeled with the firmware type and version number. The type and version information is also stored as data in each PROM.

In the course of troubleshooting a problem with a server, the Bridge Communications technical support staff may need to know the system's software and firmware release numbers. Most software and firmware release numbers can be displayed with the `SHoW VERSioN` command (described in Section 3.2). The software release number of the Series/100 Utilities Diskette is displayed on a terminal attached to port 0 when the utilities diskette is booted.

Each software release number consists of an alphanumeric designator indicating the product type and an alphanumeric suffix indicating the version number of the software. For example:

```
SW/1-A/BSC/SDLC-20050
```

In this case, the string "SW/1-A/BSC/SDLC" indicates the product is a CS/1 with asynchronous, bisynchronous, bit-synchronous, or 3270 interfaces and the number "20050" indicates the software is version number 20050. Higher version numbers represent more recent releases. Table 2-2 lists the meanings of the software designators for all Bridge products.

Each firmware release number consists of an alphanumeric prefix indicating system hardware type and PROM size, an alphanumeric designator indicating the firmware type, and a numeric suffix indicating the firmware version number. For example:

```
M1 MMON 01E
```

In this case, "M1" indicates Series/1 hardware and 32K bytes of PROM, "MMON" indicates the firmware is the MCPU Monitor, and "01E" indicates the firmware is version number 1E. Higher version numbers represent more recent releases. Older versions of firmware may not appear in the `SHoW VERSioN` display. Table 2-3 lists the meanings of the firmware designators for all Bridge Communications, Inc., PROMs.

Table 2-2 Software Release Number Prefixes	
<i>Prefix</i>	<i>Product and Service</i>
PC-ETERM	EtherTerm Connection Service
SW/1-A/BSC/SDLC	CS/1 XNS Connection Service for asynchronous, bisynchronous, bit-synchronous, and 3270 interfaces
SW/1-HSM	CS/1-HSM Connection Service
SW/1-SNA3270	CS/1-SNA Connection Service
SW/1-SNA3270-TCP	CS/1-SNA-TCP Connection Service
SW/1-SPMUX	CS/1-BSC Connection Service with Sperry Multiplexer Software
SW/1-TCP	CS/1 TCP Connection Service for asynchronous, bisynchronous, and bit-synchronous interfaces
SW/1-X.25	CS/1-X.25 Connection Service
SW/1-NCS	NCS/1 System Software
SW/100-A/BSC	CS/100-A and CS/100-BSC XNS Connection Service
SW/100-UTIL	CS/100 XNS Utilities Diskette
SW/100-SNA3270-TCP	CS/100-SNA-TCP Connection Service
SW/100-TCP	CS/100 TCP Connection Service
SW/100-TCP-UTIL	CS/100 TCP Utilities Diskette
SW/150-NCS	NCS/150 System Software
SW/150-NCS-UTIL	NCS/150 Utilities Diskette
SW/150-NCS-TCP	NCS/150-TCP System Software
SW/150-NCS-UTIL	NCS/150-TCP Utilities Diskette
SW/2-CS/ICS	GS/1 Connection and Interconnection Services
SW/200-A	CS/200-A Connection Service
SW/3	GS/3 Interconnection Service
SW/3-IP	GS/3-IP Interconnection Service
SW/300	GS/300 Interconnection Service
SW/4	GS/4 Interconnection Service
SW/6	GS/6 Interconnection Service
SW/6-IP	GS/6-IP Interconnection Service
SW/IB	Internetwork Bridge Interconnection Service
SW/IVECS-A	IVECS Connection Service

Table 2-3 Firmware Release Number Prefixes

<i>Prefix</i>	<i>Product and Service</i>
C1 MMON	Series/200 Monitor firmware
M0 ASYN	Series/1 Asynchronous SIO firmware
M0 BSC- *	Series/1 Bisynchronous SIO firmware
M0 EDL1	Series/1 Ethernet Data Link EC/1 firmware
M0 EDL2	Series/1 Ethernet Data Link EC/2 firmware
M1 IECM	IECM firmware
M1 MMON	Series/1 MCPU monitor firmware
M1 SYNC	Series/1 Synchronous SIO firmware
M2 COAX	Series/1 3270 SIO firmware
M2 IBCM	Broadband Data Link firmware
M3 CURZ	Series/1 3270 SIO firmware
T0 ASYN	Series/100 Asynchronous SIO firmware
T0 BSC- *	Series/100 Bisynchronous SIO firmware
T0 EDL1	Series/100 Ethernet Data Link firmware
T1 MMON	Series/100 MP monitor firmware
T1 SYNC	Series/300 Synchronous SIO firmware
U1 MMON	IVECS MP firmware

* M0 BSC- should be replaced with M1 SYNC;
T0 BSC- should be replaced with T1 SYNC;
contact Bridge Communications Technical Support.

3.0 CONNECTION SERVICE COMMAND GUIDE

This section describes the format and syntax of the Connection Service commands and provides a complete list of all commands, normal responses, and error messages.

The Connection Service is available to all Communications Server ports configured to support asynchronous terminal devices or 3270 display stations and to devices dialing in to the CS/1-X.25 or GS/1 from a PAD device on an X.25 network.

The discussion of the DeVice parameter in Sections 4.1.1 and 4.2.1 describes configuring the port device type.

Some Connection Service commands are also available to devices interacting in remote mode with the CS/1-X.25, GS/1, IVECS, NCS, or the CS/200. The REMOTE command is described in Section 3.2.12.

3.1 Command Format and Syntax

This section describes the general form of the Connection Service commands, the local editing capabilities of the Connection Service, and the specific conventions used for entering different kinds of information.

Commands are usually entered at a user device in response to the Connection Service prompt. In Section 3.2, the default CS/1 prompt (the string "CS/1>") is used in all examples.

3.1.1 Format

The most common command format has two parts: a command verb and one or more parameters. The command verb is always entered first, followed by a space and the parameters; the command is terminated by pressing the return key. Some commands include a keyword between the verb and the parameters. A few commands require only the verb, terminated by the return key.

Most commands have an alternative network manager form, which contains an optional address field so that the network manager can control remote ports. The address, if used, is entered in parentheses after the verb. The following examples of command format (from simple to more complex) show both the user version and the network manager version of each format.

<i>User Version</i>	<i>Network Manager Version</i>
verb	verb (address)
verb parameter	verb (address) parameter
verb keyword parameter	verb (address) keyword parameter

Before a command line is terminated with the return key, the text of the line may be edited with the special editing characters discussed in the next section. These characters can be altered for each port. In some circumstances, the editing characters can be used by a port in Data Transfer mode. For further information, refer to the discussion of local editing parameters in Sections 4.1.4 and 4.2.4 and to the discussion of the MOde parameter in Sections 4.1.3 and 4.2.3.

Commands may be abbreviated to the shortest unambiguous string of characters that can be interpreted by the system, according to the rules listed in Section 3.1.3.

A help facility is provided to remind the user of the valid commands and their parameters, and a macro facility is available so that complex command sequences can be executed with a one-line command.

3.1.2 Special Characters

Table 3-1 describes the notation used in this guide to represent some of the special characters on the typical device keyboard. Table 3-2 lists the default characters used for editing a command locally before terminating the command line by pressing the return key. These characters can be altered with the SET command.

Table 3-1 Notation of Keyboard Symbols	
<i>Symbol</i>	<i>Meaning</i>
<BREAK>	Represents the break key. Usually located at the far right end of the keyboard, labeled BREAK or BRK.
<CTRL-char>	Represents a control character, obtained by holding down the key labeled CTRL or CTL and simultaneously pressing the specified key. Table 3-2 contains a list of the default control characters.
<ESC>	Represents the escape key. Usually located at the left end of the keyboard, typically labeled ESC or ESCAPE. Most terminals have an escape key; some require a control sequence instead (usually <CTRL- >).
<RETURN>	Represents the return key. Usually located at the right end of the keyboard, labeled RETURN or CR.

Table 3-2 Default Local Editing Characters

<i>Key</i>	<i>Function</i>
<CTRL-H>	Erases the last character that was typed. Each additional <CTRL-H> erases an additional character, back to the beginning of the line. If no characters remain on the line, <CTRL-H> causes the terminal bell to ring. This character is defined by the ERase parameter. The <BS> key performs the same function as <CTRL-H>.
<CTRL-R>	Reprints everything entered since the last return. This is useful on a paper terminal, where the ERase character causes a crosshatch (#) to echo on the terminal; when the line is reprinted, crosshatches and deleted characters are removed, making it easier to verify that the line is correct. This character is defined by the ReprintLine parameter.
<CTRL-U>	Erases everything that has been typed since the last return. If the current line contains no text, <CTRL-U> causes the terminal bell to ring. This character is defined by the LineERase parameter.
<CTRL-V>	Instructs the server to transmit the next character entered as data and to ignore any special meaning that the character may have for the system. This character is necessary so that the other characters in this list can be entered as text, with no special meaning. This character is defined by the VERBatim parameter.
<CTRL-W>	Erases all characters back to the last space. For each additional <CTRL-W> entered, an additional word is erased, back to the beginning of the line. If no text is left on the current line, <CTRL-W> causes the terminal bell to ring. This character is defined by the WordERase parameter.

3.1.3 Command Abbreviation

Both commands and parameters can be abbreviated to the smallest number of characters that can be meaningfully interpreted by the system. For example, the Connect command is the only command beginning with a "c", so "c" is the only character needed to issue the Connect command. In contrast, several commands begin with an "s". Therefore, to make a distinction between the SAve, SET, SETDefault, SHow, and SWitch commands, the user must enter at least two characters, that is, "sa", "set", "setd", "sh", or "sw", respectively.

If a command parameter is a composite of two or more words, the abbreviation usually consists of the initial letter of each word. For example, the minimum abbreviation of StopBits is "sb", and DataBits is "db".

When commands and parameters are printed in this guide and in screen messages, the minimum form of each word is printed in uppercase characters; characters that can be left out are printed in lowercase. Commands and parameters can actually be entered in either upper- or lowercase, or a combination of both; the distinction between upper- and lowercase is made in this guide only to simplify abbreviation.

3.1.4 Syntax Notation

The individual command descriptions in Section 3.2 present the syntax of each command. The following notation is used in the descriptions. Of the following characters, only the parentheses are entered; the angle brackets, square brackets, braces, vertical bar, and ellipsis are never entered.

UPPERCASE LETTERS	Represent the shortest unambiguous abbreviation of the command or parameter.
lowercase letters	Represent variable or optional portions of the command or parameter.
angle brackets < >"	Enclose a variable parameter or value.
square brackets []"	Enclose an optional parameter or a list of optional parameters.
parentheses ()	Enclose an optional address field or a list of multiple values being assigned to a single parameter. If the field is included, the parentheses must be entered.
braces { }	Enclose a list of values, one of which must be entered.
vertical bar	Separates mutually exclusive items in a list enclosed by brackets.
ellipsis ...	Following a parameter name or value, indicates that one or more additional parameters may be specified on the same command line.

Most commands accept only a parameter name or value of a particular type. These parameters and values fall into the following categories:

numbers	Numbers represent parameter values or session numbers. Section 3.1.5 discusses the conventions for entering numbers.
names	Names usually represent either system-defined parameter names or parameter values (written as <param-name> or <value>), or user-defined macros or files (written as <macro-name> or <filename>). Section 4.1 discusses system-defined parameters and value names.
strings	Some parameter values can be set to user-defined strings, ranging from a single character (written as <char>) to a multi-character string (written as <string>). String conventions are listed in Section 3.1.5.
addresses	The Connection Service recognizes a number of different address types, including physical addresses, port identification numbers, network identification numbers, and clearinghouse names (written as <physical address>, <portid>, <netid>, and <clearinghouse name>, respectively). The notation "<address>" means that the command accepts various combinations of these address types. Addressing and naming conventions are listed in Sections 3.1.6 and 3.1.7 (Ethernet addresses) and Sections 3.1.8 and 3.1.9 (TCP addresses).

3.1.5 Specifying Parameter Values

Depending on the parameter, parameter values can be expressed as names, sets of names, numbers, string text, or addresses. This section describes the rules that govern the way these values are specified.

The parameter and value names that may be specified are listed in Section 4.0. The rules for specifying addresses in commands are described in Section 3.1.6.

The SET and SETDefault commands require both parameter names and parameter values. Each parameter name is followed by an equal sign (=) and one or more values. Spaces are permitted, but not required, before and after the equal sign. If more than one parameter value is being assigned to a single parameter, the values must be enclosed in parentheses and separated from one another by commas. For example:

```
set dataforward = alphanum
set device = (terminal,glass)
set baud = 9600
```

Numbers may be expressed in any of four bases, according to the conventions shown in Table 3-3.

Table 3-3 Conventions for Entering Numbers		
<i>Number Base</i>	<i>Precede Number with</i>	<i>Examples</i>
Decimal	nothing	128 1486
Hexadecimal *	%	%40FF %27ae
Octal	%(8)	%(8)107
Binary	%(2)	%(2)0000101

* Hexadecimal alphabetic digits may be entered in upper- or lowercase.

A **session number** is a single-digit identifier assigned by the Connection Service to each connection that exists on a port. If no session number is specified in a command that allows a session number, the current session is assumed.

String values fall into three categories: single characters, control characters, and variable-length strings. All characters may be entered in upper- or lowercase, although control characters are always displayed by SHow in uppercase. Table 3-4 lists the conventions for entering string values.

<i>String Type</i>	<i>Convention</i>	<i>Valid Characters</i>	<i>Examples</i>
Single Character *	Enclose in apostrophes	All alphanumeric characters and symbols	'S' 's' '\$'
Control Characters *	Caret symbol followed by character	<CTRL-@>, <CTRL-A> through <CTRL-Z>, <CTRL- >, <CTRL- \ >, <CTRL- >, <CTRL- ^ >, and <CTRL- _ >	^g ^G
Variable-length Strings	Enclose in quotation marks	All numbers, symbols, alphanumeric characters, and control characters	"Hello!"
* Both single and control characters may be represented by their numeric ASCII values, although they will be displayed by SHow as uppercase characters. To specify characters numerically, follow the rules for entering numbers instead of those for entering characters.			

A few characters with special meaning to the server must be preceded by a backslash (\) in string text to prevent the characters from being misinterpreted. These symbols are the apostrophe ('), backslash (\), caret (^), and quotation mark ("). For example, to include an apostrophe in string text, enter a backslash followed by an apostrophe (\'). To specify one backslash (\) as part of string text, enter two backslashes (\\); the first prevents the Connection Service from treating the second as a special character. (The caret referred to in this paragraph is a literal caret, used to denote control characters, not the <CTRL> key held down in a control-character sequence.)

Form effectors (carriage control characters) may be included in string text either as control characters or as single-letter identifiers preceded by a backslash. Table 3-5 lists the form effectors.

<i>Form Effector</i>	<i>Letter Identifier</i>	<i>Control Character</i>
Backspace	\b	^H
Return	\r	^M
Escape	\e	^I
Formfeed	\f	^L
Newline (linefeed)	\n	^J
Tab	\t	^I

For instance, to generate the default CS/1 Connection Service welcome message followed by a return-linefeed sequence, enter this string:

```
"Welcome to your Communications Server \r \n"
```

Numeric characters may be included in string text and will print exactly as entered. A number preceded by a backslash, however, will be interpreted as an octal number representing a control character or other single character. For example:

```
\010
```

3.1.6 Specifying XNS Ethernet Addresses

Ethernet addresses apply to servers running the XNS protocols. For the equivalent addressing conventions for servers running the TCP protocols, refer to Section 3.1.8.

This section describes the rules that govern the way Ethernet addresses are specified. In general, an address can be expressed as a single physical address, a clearinghouse name, an address list, or a combination of all three.

A **physical address** contains up to four fields: a network address, an Ethernet address, a port number, and an optional phone number field. For example:

```
&00003333%080002001326!17#4159694400
```

- The network address field contains 8 hexadecimal digits and is always preceded by an ampersand (&). The network address uniquely distinguishes one Ethernet network from all other Ethernet networks. If the network address is omitted, the local network address is assumed.
- An Ethernet address field contains 12 hexadecimal digits and is always preceded by a percent sign (%). The Ethernet address uniquely identifies each server on a single network. If this field is omitted, the local server's Ethernet address is assumed.

The Ethernet address of each server is assigned by Bridge Communications with the authority of Xerox Corporation. The address is stored in PROM and can be displayed with either the SHow NetMap command or the SHow ADDRess command. SHow NetMap lists the addresses of all servers on the network that run the same set of high-level protocols; the first address listed is the address of the local server.

- The port number field contains up to 3 decimal digits and is preceded by an exclamation point (!). The port number uniquely identifies each port on a server. For most destination servers, a port number is the smallest possible legal address. (For a connection made via an X.25 server, however, a port number alone is insufficient; the destination X.25 address must be entered in the number field.)
- The optional phone number field contains up to 20 decimal digits. The number, if entered, is always preceded by a crosshatch symbol (#). If the destination of the session is a host connected to an X.25 network or an X.25 host connected to an Ethernet network via a CS/1-X.25, this field must be used to specify the destination X.25 address. An X.25 address contains a 4-digit Data Network Identification Code (DNIC), 6 to 8

digits of destination host address, and, optionally, 2 to 4 digits of subhost address (usually a port number). Trailing zeros may be omitted, but leading zeros may not.

On the GS/1, the subhost address field can be used to request a specific virtual port number.

A **clearinghouse name** consists of three hierarchically arranged fields: a local name, a domain name, and an organization name, separated by "at" signs (@).

If the organization name (and the "at" sign preceding it) or both the domain name and the organization name (and the "at" signs preceding them) are omitted, the system supplies the default names (see Section 3.1.7). A valid clearinghouse name must contain at least a local name. For example, the following are valid clearinghouse names:

```
localname@domain@organization
localname@domain
localname
```

The local name field may have a maximum of 14 alphanumeric characters or 18 numeric characters. If any characters in the name are alphabetic, the first character must also be alphabetic. Typically, numeric clearinghouse names are used only in conjunction with the GS/1 Connection Service to facilitate connections from devices on an X.25 network.

The domain and organization fields may each have a maximum of 10 alphanumeric characters, the first of which must be an alphabetic character. Subsequent characters may be either alphabetic or numeric. The only non-alphanumeric characters permitted in the names are the underscore (_) and the period (.).

In the SHow CHN command, which displays the rotary number or physical address of a clearinghouse name, an asterisk (*) may be substituted for one or more fields of the clearinghouse name. The asterisk represents a wildcard character, and means "any value" for that field.

Section 3.1.7 discusses clearinghouse names in detail.

An **address list** consists of up to eight addresses and/or names separated by commas. The list specifies a global rotary, that is, a set of addresses that are equally acceptable as the destination of a circuit. The addresses or names in the list may represent ports on the same server or on different servers.

In the syntax descriptions of each command, the generic term <address> means that any of the following forms of address is acceptable:

- A physical address
- A clearinghouse name
- A clearinghouse name (which represents part of a physical address) followed by part of a physical address

For example, all of the following are valid addresses:

```
&abff5678%1234abcdffff!1#31104081234507      cs15!8
%080000200018!3                                host2
modem#3212345                                  !2
```

In the syntax definitions, the generic term <address list> means that a list of addresses, a list of names, or a mixed list of both is acceptable. For example, all of the following are valid:

```
%080002000123,%080002000101  
host1a,host1b,host1c  
!10,!128
```

3.1.7 Establishing and Using Clearinghouse Names

The network manager uses the Name command (discussed in Section 3.2.9) to associate a local clearinghouse name with a specific port or list of addresses. The ports or addresses must be on servers running the XNS protocols. A user can then request a connection to a device using the clearinghouse name, without knowing the physical address of that device.

For the X.25 automatic connection service, the network manager uses the Name command to associate a port or rotary number with an X.25 address. For a description of automatic connection service, refer to Section 2.4. For information on setting up this service, refer to Appendix C.

To set up a local rotary, the network manager first uses the ROtary command (discussed in Section 3.2.16) to establish an array of ports on a single server, and then uses the Name command to associate a single clearinghouse name with the array. To set up a global rotary, the network manager uses the Name command to associate a clearinghouse name with a list of addresses. Local and global rotaries are described in Section 2.3.8.

For servers that boot from a local disk drive, the network manager uses the SETDefault command to establish default domain and organization strings for each server. The locally defined default strings are assumed automatically whenever the user enters a clearinghouse name without specifying these fields.

For servers that boot from an NCS, the network manager uses the SETDefault command on the NCS to specify default domain and organization strings; these strings then apply both to the NCS/150 itself and to all of the NCS's client servers. Each client server has the same default strings, unless the network manager subsequently uses the SET command on a client server to establish different settings. These new settings, however, remain in effect only until the next time the server is booted; at that time, the server reverts to the default strings established on the NCS.

The XNS clearinghouse scheme uses sets of centralized Name Servers. The Bridge implementation, however, distributes this function among the servers. If a requested name is not found in the local database, the server broadcasts a lookup request to all servers on the network. Each server that boots from a local disk drive maintains its own clearinghouse name database. The clearinghouse name database for all servers supported by a single NCS is stored on the NCS. On a network with multiple NCSs, the clearinghouse name database may be distributed among them.

Whenever a clearinghouse name or a command that affects clearinghouse names is entered without specified domain and organization strings, the Connection Service appends the default strings of the local server. This convention facilitates a hierarchical naming strategy for networks that support a number of different groups and resources.

Within a network or group of interconnected networks, if the same clearinghouse name is defined more than once and mapped to different addresses or address lists, sessions to that name can be misrouted and data can be lost. To prevent this, ensure that no logical name is defined more than once within the network. To simplify network administration and maintenance, the clearinghouse name database on each server should include only entries for ports on that server. Similarly, the clearinghouse name database on each Network Control Server should include only entries for ports on servers bound to that NCS. An NCS/1 or an NCS/150 may be backed up by one or more secondary NCS/150s. In a network containing both a primary NCS and a secondary NCS/150, the clearinghouse name database on the secondary NCS/150 should always be identical to the database on the primary NCS. The *NCS Installation and Operation Guides* discuss the Network Control Servers in detail.

3.1.8 Specifying TCP Addresses

This section describes the rules that govern the way TCP/IP addresses are specified, and applies only to servers running the TCP/IP protocols. In general, a TCP/IP address can be expressed as an Internet address, a physical port number, or an internet name.

An **Internet address** consists of up to 12 decimal digits, which are arranged in four fields. Each field consists of up to 3 digits, and the fields are separated by periods:

xxx.xxx.xxx.xxx

Leading zeros in any single field may be omitted.

The address includes both a network number and a host number. The actual format of these two numbers varies depending on the class of address being designated. Address class is determined by the value in the first address field. Table 3-6 lists the valid address classes, the values used to specify them, and the resulting address format. The maximum value for any single field is 255.

<i>Class</i>	<i>Range of First Address Field</i>	<i>Address Format *</i>
A	0 - 127	nnn.hhh.hhh.hhh
B	128 - 191	nnn.nnn.hhh.hhh
C	192 - 223	nnn.nnn.nnn.hhh

* "n" represents a digit of the network number;
"h" represents a digit of the host number.

For example, 126.0.0.100 is a class A address, with a network number of 126 and a host number of 0.0.100; 135.1.0.200 is a class B address, with a network number of 135.1 and a host number of 0.200; 192.2.3.254 is a class C address, with a network number of 192.2.3 and a host number of 254.

The values 0 and 255 are special in TCP addressing. The value 0 means "local", as in "local host"; and the value 255 means "all", as in "all networks". For instance, the class B address 128.255.255.255 indicates all hosts on the network 128. The class A address 0.0.0.37 indicates host 37 on the local network.

The important feature of address class is the fact that the class determines which part of the Internet address is the network number. In order to be able to communicate with one another, all devices on the same network should be assigned addresses containing identical network numbers. Two devices whose network numbers are different cannot communicate with each other without a gateway. In addition, each host number must be unique within its network.

The Internet address format does not provide any means of specifying port numbers. Therefore, the Bridge implementation uses different Internet addresses to represent different physical ports on a TCP server. Up to 41 different addresses may be assigned to a given TCP server:

- One server address. This address is mandatory, and is used as the source address on the active side of all connections.
- One address for each physical port. These addresses are optional; they are used only as destination addresses on the passive side of all connections and are assigned only to ports used as circuit destinations (e.g., hosts or dial-out modems).
- One address for each rotary number, up to a maximum of eight rotaries (numbered 128 through 135). These addresses are also optional, since they need to be assigned only to rotaries actually used as circuit destinations, but not to unused rotary numbers.

A **port number** consists of up to three decimal digits preceded by an exclamation point. Some Connection Service commands permit either physical port numbers or Internet addresses to be specified; others permit only physical port numbers, but not Internet addresses. Similarly, some command displays (e.g., SHow ADDRess) include only physical port numbers, but not Internet addresses. The command and display descriptions indicate when only physical port numbers apply.

An **internet name** consists of a simple character string. The maximum length of the internet name is 40 alphanumeric characters; the first character of which must be alphabetic. Subsequent characters may be either alphabetic or numeric. The nonalphanumeric characters permitted are the underscore (_), the period (.), and the dash (-).

In the SHow NAMES command, which displays the Internet address associated with an internet name, an asterisk (*) may be substituted for all or part of the name. The asterisk represents a wildcard character, and indicates "any value".

3.1.9 Establishing and Using TCP/IP Internet Names

The network manager uses the system generation procedure to assign the mandatory Internet address to a Communications Server running the TCP/IP protocols, or, if the server boots from an NCS, the network manager can assign the Internet address when the server is bound to its NCS. The addresses must be assigned using the conventions outlined in the previous section.

If any of the ports on the TCP server represent destinations to which circuits will be established, the network manager assigns Internet addresses to those individual ports via the SETDefault command (discussed in Section 3.2.19).

If more than one port on a TCP server provides connections to the same device (i.e., a host computer), the network manager should allocate a rotary number for the ports and assign an Internet address on the rotary via the SETDefault command. No Internet address need be assigned to any port that only originates circuits but is never the destination of a circuit.

The network manager uses the ROTary command to assign ports to a rotary number. The user can then request a connection to the rotary, without knowing if a specific host port is available; the connection is made to the first available port in the rotary.

The network manager uses the Name command to associate an internet name with an Internet address (which may represent an individual port or a rotary). The user can request a connection to a resource using its name, without knowing the Internet address or rotary number of that resource.

Global rotaries are not currently supported on TCP/IP networks.

The Internet Name Service may be implemented as a local or remote database, depending on the setting of the PrimaryNS parameter: If a requested name is not found in the local database, the server returns an error message.

However, if an Internet Name Server is present on the network, each TCP server can be directed to send all name lookup requests to the Name Server instead of searching the local database. A primary and secondary Name Server may be assigned. The secondary Name Server is queried if the primary cannot resolve the address.

Alternatively, a TCP server may be selected to function as a Name Server.

3.2 Commands

The following section provides detailed descriptions of all the Connection Service commands. The descriptions include the syntax of each command, examples showing how the command is used, and a list of possible system responses and error messages. A comprehensive list of all Connection Service error messages is provided in Appendix A.

An explanation of the syntax notation and the rules governing how parameters and values are entered are provided in Section 3.1.

Section 4.0 provides a comprehensive list of the parameters that can be used with the SET, SETDefault, REMoteSET, REMoteSHow, and SHow PARAMeters commands (Section 4.1 for asynchronous or 3270 ports and Section 4.2 for virtual ports on the GS/1). Table 3-7 contains a summary of the Connection Service commands.

Table 3-7 Connection Service Command Summary

<i>Section</i>	<i>Command</i>	<i>Description</i>
3.2.1	Broadcast	Send message to user device(s)
3.2.2	Connect	Request virtual circuit
3.2.3	DEFine	Define macro command file
3.2.4	DEQueue *	Remove port from connection queue
3.2.5	DisConnect	Terminate virtual circuit
3.2.6	DO	Execute macro
3.2.7	Echo	Echo a string on the terminal
3.2.8	Listen	Permit connections to port
3.2.9	Name	Assign logical name to address
3.2.10	Pause	Pause for specified number of seconds
3.2.11	Read	Read and save default port configuration parameters; read statistics report from diskette
3.2.12	REMOTE	Execute network management commands on another server
3.2.13	REMOteSET *	Set remote device parameters
3.2.14	REMOteSHoW *	Display remote device parameters
3.2.15	RESume	Return to Data Transfer mode
3.2.16	ROtary	Assign ports to rotary
3.2.17	SAve	Save configuration onto diskette
3.2.18	SET	Set active parameters
3.2.19	SETDefault	Specify default or fixed parameters; specify and save Internet addresses
3.2.20	SHoW	Display parameters, sessions, etc.
3.2.21	SWitch	Change to different session
3.2.22	Transmit	Transmit string to remote device
3.2.23	UNDefine	Remove macro definition
3.2.24	UNName	Remove clearinghouse name
3.2.25	UNSave	Remove configuration file
3.2.26	ZeroStats	Set value of busiest minutes and busiest sample data statistics to 0

* Not available on TCP servers.

3.2.1 Broadcast Command

Syntax

Broadcast <string>

Broadcast (<address>) <string>

Default Privilege Level

Local Network Manager

Description

The Broadcast command transmits string text messages within the server and across the network. The text must follow the syntax described in Section 3.1.5. The maximum permissible length of the string text is 82 characters; if more are specified, an error message is generated and the string is truncated.

If no address is specified, the message is sent to all terminal ports on the local server. If an address is specified, and if reception of broadcast messages is disabled for the specified port (i.e., if the InterAction parameter is set to BroadcastOFF), the server returns an error message.

For XNS servers, the special address %ffffffff can be used to specify all terminal ports on all servers in the local network, including the local server.

For TCP servers, the address specified can be either a port number (if the destination port is on the same server as the requesting port) or an Internet address (for either local or remote ports). The address 255.255.255.255 broadcasts to all terminal ports on all servers in the local network, including the local server.

If the InterAction parameter for the destination port is set to Verbose, the message is prefixed by the text "Broadcast msg from <portid>". If the InterAction parameter is set to Brief, the message text is displayed without the prefix.

Example 1

```
broadcast (!1) "Printing requests are due by 1700 today"
```

In this example, the specified text will be transmitted only to port 1 of the local server.

Example 2

```
b (%ffffffff) "Meeting in the lunch room in 5 minutes"
```

This example sends the message to all terminal ports on all servers on the XNS network.

Normal Response

A new prompt appears on the requesting port, and the message text appears on the destination port.

Error Messages

"Broadcast is not enabled on that port"

"Insufficient privilege"

"Invalid Broadcast syntax"

"Invalid network manager syntax"

"String truncated to 82 characters"

3.2.2 Connect Command

Syntax

```
Connect <address>[,<address>] [ECM] [Q]
Connect (<address>) <address>[,<address>]
```

Default Privilege Level

User

Description

The Connect command requests a connection to the specified address. On an XNS server, the address can take the form of an Ethernet address, or a clearinghouse name. On a TCP server, the address can take the form of a TCP/IP Internet address, or an internet name. The address or name can represent either a single port, a local rotary, or, for XNS servers, a global rotary. A global rotary can be specified as a list of up to eight names or addresses, or as a single name to which an address list has previously been assigned.

In the network manager form of the command, the connection is requested from the address or name enclosed in parentheses to the subsequent address. The address or name enclosed in parentheses must be a simple address, or a name that represents a simple address. A simple address consists only of the network number (optional), Ethernet address (optional), and port number; rotary numbers, phone numbers, or X.25 addresses are not allowed. The subsequent address can be either a physical address or a name; can represent either a single port, a local rotary, or a global rotary; and can contain a phone number or an X.25 address. The rules governing Ethernet and Internet addresses are described in Section 3.1.6 and 3.1.8, respectively.

Connections cannot be made from a device attached to an XNS server to a TCP device, or vice versa.

When a connection is requested from an XNS server, the system first compares the AccessWord of the requesting port with the AccessGroup of the destination port. If at least one common group number appears in both sets, the connection is established. If no common group number appears, the system prompts the requestor for a password associated with the AccessGroup parameter of the destination port. If the AccessGroup has more than one value, the password for any one of the values is accepted. Access control does not apply to TCP servers. For asynchronous or 3270 ports, these parameters are described in Section 4.1.1. For GS/1 virtual ports, these parameters are described in Section 4.2.1.

In the first form of the command, the destination port must be in Listening mode before the connection can be established. Once the connection is initiated, both ports are placed in Data Transfer mode. If the optional parameter ecm is appended, however, the local port is left in Command mode rather than Data Transfer mode. The ECMChar parameter is not permitted in the network manager form of the command.

In the network manager form of the command, both of the ports being connected must be in Listening mode. When the network manager uses this command to form a connection, neither of the connected ports can use the ECMChar to change from Data Transfer mode to Command mode. Therefore, the connection can be broken only remotely by the network manager or locally by the expiration of the AUtodisconnect interval on the destination port. Call queuing and the ECMChar parameter are not available in the network manager form of the command.

Devices being connected remotely by the network manager through a GS/1 may be on different networks. However, if one device is on an Ethernet network and the other device is on an X.25 network, the first address specified in the Connect command (the address in parentheses) must represent the device attached to the Ethernet network; the second address specified must represent the device on the X.25 network. Rotary numbers and X.25 addresses cannot be used in the first address.

For XNS servers only, the optional parameter "q" is the call queueing designation. If this parameter is included, and if the destination port is not in Listening mode when the connection request is issued, then the requesting port is put in a queue for eventual connection. The queued connection constitutes a session for the requesting port. When the destination port becomes available, the system sends the requesting port a terminal bell signal and a message that the destination device is available. The user then has five minutes in which to claim the connection by issuing the RESume command. If the port is in Data Transfer mode and is communicating with a third port when the message is received, then the user must first return to Command mode and then either switch to the queued session or specify the queued session number when issuing the RESume command. Section 2.3.10 describes the call queueing feature. Call queueing does not apply to TCP servers.

For XNS servers, if the Connect command specifies a clearinghouse name as the destination address, but does not include domain and organization fields, the local server automatically appends the default strings.

Port number 136 on any Bridge XNS server supporting the Connection Service is reserved for network management access from non-Bridge devices that are attached directly to the Ethernet (e.g., personal computers running EtherTerm software). Port 136 supports only one such connection at a time.

Example 1

```
connect host1
```

This example requests a connection from the local port to the name "host1", which can represent a rotary of ports.

Example 2

```
c host1_a.host1_b
```

This example requests a connection from the local port to a global rotary consisting of the port(s) represented by the name "host1_a" and the port(s) represented by the name "host1_b". This example applies only to servers running the XNS protocols.

Example 3

```
c (!4) host1
```

This example requests a connection from port 4 on the local server to the clearinghouse name "host1". This example applies to all XNS and TCP servers.

Example 4

```
c %1234abcdf ecm
```

This XNS example requests a connection from the local port to the physical address "%1234abcdf". The addition of the letters "ecm" causes the port to return to Command mode once the connection is made instead of entering Data Transfer mode with the destination port.

Example 5

```
c host1 q
```

This example requests a connection to the clearinghouse name "host1". The addition of the letter "q" requests that if no port to that device is available, the requesting port is to be put into a queue for connection with the first available destination port. This example applies only to servers running the XNS protocols.

Example 6

```
c (%080002000010!1) !2
```

This XNS example requests a connection from port 1 on the server with the Ethernet address %080002000010 to port 2 on the same server. The use of a complete address within the parentheses implies that the same address applies to the destination port. If the two devices are on different Communications Servers, full Ethernet addresses must be used for both. Only a Global Network Manager can make a connection between two ports that are both on remote servers (i.e., a third-party interconnect).

Example 7

```
c 192.000.000.128
```

This TCP/IP example requests a connection to a TCP/IP Internet address. The local port must be on a server with TCP/IP protocols.

Example 8

```
c host1
```

This TCP/IP example requests a connection to the TCP/IP device named "host1" on the network. The local port must be on a server running TCP/IP protocols.

Example 9

```
name x25host = %080002000010!128#314140812345
c (printer2) x25host
```

In this X.25 example, the first command assigns the name "x25host" to a destination host on an X.25 PDN. The string "%080002000010" is the Ethernet address of the CS/1-X.25 or GS/1 connected to the X.25 network, "!128" is a rotary of virtual ports on that GS/1, and "314140812345" is the X.25 address of the destination host. The second command requests a connection from "printer2" (which must be on the Ethernet network) to the host.

Normal Response

```
"Connecting ... Session <n> connected to <address>"
"Connecting ... Interconnection formed"
"Connecting ... Access controlled Group <n> Password:"
"Connecting ... Remote is busy session <n> -- queued to <address>"
```

Error Messages

```
"Connecting ... No more sessions for this port"
"Connecting ... No response"
"Connecting ... Remote is busy"
"Connecting ... Remote is disabled or nonexistent"
"Connecting ... Timeout failure"
```

"Disconnecting ... session <n> disconnected from <address>"
"Insufficient PRiVilege"
"Invalid Connect syntax"
"Invalid <physical-address> syntax"
"Querying Clearinghouse... Clearinghouse name not found" (XNS only)
"Querying Name Server... internet name not found" (TCP only)
"Session <n> -- dequeued ... No response"
"Session <n> -- dequeued ... Reserved timer expired"

3.2.3 DEFine Command

Syntax

DEFine <macro name> = (<text>)

Default Privilege Level

Local Network Manager

Description

The DEFine command creates a macro file and specifies its contents. A macro is executable by all terminal ports on the server on which it was created. When a new macro is created with the same name as an existing macro, the new macro contents replace the old macro contents. When a macro is defined for a Communications Server that boots from an NCS, that macro is available to all servers that boot from the same NCS. On a server that boots from an NCS, the DEFine command requires Global Network Manager privilege level.

Macro names can be up to 14 characters long; the first character must be alphabetic. The Connection Service does not distinguish between upper- and lowercase in macro names.

Macro names beginning with the letters "init" are reserved for system initialization macros. Every time the server is booted locally, it checks the diskette for a file called "init"; if the file exists, the server automatically executes it. Each time a server is booted from an NCS, it also checks the NCS' diskette for an initialization macro.

For XNS servers that boot from an NCS, the system initialization macro is called `init.<address>`, where <address> depends on the server's Ethernet address. If the address begins with 08000200, then <address> is the last four digits of the server's Ethernet address; if it begins with 08000201, then <address> is the last six digits of the server's Ethernet address. For servers running TCP protocols that boot from an NCS/150-TCP, the system initialization macro is called `init.<Internet address>`, where the Internet address is specified in hexadecimal. If the file exists, the server executes the macro.

If a macro name appears as the value of the `InitMacro` parameter for a port, that macro is executed automatically each time the device attached to the physical port is powered on or otherwise detected by the server. The `InitMacro` parameter is described in Section 4.1.1 for asynchronous or 3270 ports and 4.2.1 for virtual ports on the GS/1.

For a virtual port on the GS/1, the macro is executed automatically each time the port makes the transition from Listening mode to Command mode (discussed in Section 2.3.4). A virtual port on the GS/1 is assigned randomly to a session initiated by a device on the PDN. The port initialization macro is appropriate in this case, only if a single initialization macro on the server is equally applicable to all devices that can connect to the GS/1 from an X.25 PDN.

Macro contents must begin with a left parenthesis. If the definition requires more than one line, the user must type a return after the opening left parenthesis; the "macro:" prompt appears as a locator for the user. All characters entered between the opening and closing parentheses are part of the macro. Nested parentheses in balanced pairs are allowed.

The text of the macro must conform to the conventions for entering strings listed in Section 3.1.5. The normal server prompt returns when the user ends the macro with the closing right parenthesis.

A single macro may contain no more than 256 characters. A macro may include the DO command to call another macro, but should not call itself or another macro that calls the macro being defined, since this will result in an endless loop.

Except for the DEFine command, a macro can contain any valid Connection Service commands, including commands requesting a connection to a specific port or clearinghouse name and commands associated with a login procedure. The Pause command is usually included in a login macro to give the host time to produce a prompt before the login process starts (see the examples below).

Several commands consume large amounts of system memory when executed within a macro. These basic guidelines should be observed:

- Avoid commands that result in long screen displays (e.g., SHow STATistics). If a macro uses up all the buffers in the system, the request is aborted and the requesting port placed in Listening mode. To display more than one screenful of text from within one macro, follow each display command with a pause long enough to allow the terminal device to complete the display.
- Avoid pauses longer than 30 seconds.
- Avoid complex sequences of SHow commands in nested macros.
- Never use the REMOTE command in a macro; there is no way to escape remote mode from within the macro.
- The Connect command can be used only to form an interconnection, as the last line of the macro, or with the ECM argument.
- The RESume command can be used only as the last line of the macro.

Ordinarily, each line of the macro is printed on the terminal screen just before the line is executed. To suppress this display, set the InterAction parameter to NoMacroEcho at the beginning of the macro (see example 2, below). Only the line setting the InterAction parameter will be printed when the macro is executed.

The break key (or BReakChar) can be used to cancel the DEFine command at any time before the terminating right parenthesis is entered. The break key also cancels the execution of a macro once it has started, unless the InterAction parameter has been set to NoMacroBreak. The InterAction parameter is described in 4.1.1 for asynchronous or 3270 ports and in Section 4.2.1 for virtual ports on the GS/1.

Once defined, a macro is executed with the DO command, displayed with the SHow MACros <macro-name> command, and deleted with the UNDefine command.

Example 1

```
define TEK = (
    set interaction=nolfi
    set localeediting=(nce,nde)
)
```

This example defines a macro called "TEK" that sets a number of terminal characteristic parameters.

Example 2

```

define connect_printer = (
    set interaction = (nomacroecho, nomacrobreak)
    set privilege = gnm
    <password>
    set interaction = macroecho
    connect (host1!13) &00003140%08000200001F!25
    set priv = user
    set interaction = macrobreak
)

```

This macro allows a terminal with User privilege to establish an interconnection between a host computer and a printer attached to a remote server. The macro first changes the privilege level of the port without printing the password on the screen and prevents the user from pressing the Break key to interrupt execution of the macro. The macro then requests a connection between two remote devices, changes the privilege level back to User, and enables pressing Break to interrupt execution of other macros.

Example 3

```

def init.001f = (
    connect (!25) host1!13
)

```

This macro accomplishes a connection similar to that shown in example 2, but using a system initialization macro. The connection from port 25 of the first server (Ethernet address ending in "001f") to port 13 of the second server ("host1") is established whenever the first server is booted.

For the macro to initiate the connection successfully, a similar macro should be defined on the destination server in case the destination server is down when the macro is executed. This way, a connection will be established when the destination server boots.

To be triggered reliably on a GS/1 or CS/1-X.25, the macro must be defined as the Init-Macro for all virtual port numbers on the server (i.e., any virtual port number can be assigned to the interaction when a device on an X.25 PDN makes a connection to the GS/1 or CS/1-X.25).

Example 4

```

def inithost1 = (
    c host1 ecm
    pause 1
    t "abc"
    resume
)

setd InitMacro = "inithost1"

```

The first command defines a port initialization macro called "inithost1", which requests a connection to "host1" and then performs the login steps for user abc. The second command sets the InitMacro parameter for the local port so that the connection will be requested whenever the attached terminal is powered on.

Example 5

```
def callout = (  
  c modem ecm  
  pause 1  
  t "ATDT9,,4083212345 ^M"  
  resume  
)
```

This macro first makes a connection to an intelligent modem and pauses long enough for the modem to respond. The macro then transmits a command that causes the modem to dial out to a host computer.

Normal Response

If a macro is defined successfully, the system responds only with a new prompt.

Error Messages

```
"Can't save - directory full"  
"Insufficient privilege"  
"Invalid DEFine syntax"  
"Macro definition too long"
```

3.2.4 DEQueue Command

Syntax

DEQueue [<session number>]

Default Privilege Level

User

Description

The DEQueue command removes the specified session from the port connection queue. If no session number is specified, the current session is dequeued, if appropriate.

This command is not available on TCP servers.

Example 1

```
dequeue
```

This example removes the connection queueing request for the current session.

Example 2

```
deq 3
```

This example removes the connection queueing request for session 3.

Normal Response

```
"Dequeueing ... session <n> -- dequeued from <address>"
```

Error Messages

```
"Illegal request -- wrong state"
```

```
"Invalid DEQueue syntax"
```

```
"Invalid session number"
```

```
"No current session"
```

3.2.5 Disconnect Command

Syntax

```
Disconnect [<session number>]
Disconnect (<address>)
```

Default Privilege Level

User

Description

The first form of the Disconnect command requests that the specified session be disconnected. If no session number is specified, the current session is disconnected.

The network manager form of the command disconnects all of the specified port's sessions and places the port in Listen mode.

Example 1

```
disconnect
```

This example terminates the current session.

Example 2

```
dc 3
```

This example terminates session 3.

Example 3

```
dc (!14)
```

This example terminates all sessions on port 14 of the local server and places that port in Listening mode.

Example 4

```
dc (!18)
```

On a GS/1, this example terminates the current session on virtual port 18 of the server.

Normal Response

```
"Disconnecting ... Session <n> disconnected from <address>"
```

Error Messages

```
"Invalid Disconnect syntax"
"Invalid network manager syntax"
"Invalid session number"
"No current session"
```

3.2.6 DO Command

Syntax

DO <macro name>

Default Privilege Level

User

Description

The DO command executes the specified macro. The macro name may be entered in either upper- or lowercase.

The break key can be used to interrupt the execution of a macro, unless the port's InterAction parameter has been set to NoMacroBreak (described in 4.1.1 for asynchronous or 3270 ports and in Section 4.2.1 for virtual ports on the GS/1).

The procedure for creating a macro is described under the DEFine command, Section 3.2.3.

Example

```
do TEK
```

This example executes the command file named "TEK".

Normal Response

Ordinarily, each command in the macro file, and the system responses to it, appear on the screen as the command is executed. This echo to the terminal is inhibited if the port's InterAction parameter is set to NoMacroEcho.

Other normal responses vary depending on the contents of the macro.

Error Messages

"Can't DEFine from a macro"

"File not found or in use"

"Insufficient privilege"

"Invalid <command name> syntax"

"Macro does not exist"

"Macros nested too deeply"

Other error messages can be produced if a command contained in the macro fails. Refer to the section that describes the particular command.

3.2.7 Echo Command

Syntax

Echo <string>

Default Privilege Level

User

Description

The Echo command echoes the specified string on the terminal. The string must be specified according to the syntax described in Section 3.1.5. The maximum permissible length of the string is 500 characters; if more are specified, the string is truncated to 500 characters and only the truncated string is echoed.

The most common use of the Echo command is within a macro. The string is sent to the terminal executing the macro even if normal echoing is turned off by setting the InterAction parameter to NoEcho or to NoMacroEcho.

Example

```
(  
set interaction = nomacroecho  
set privilege = gnm  
<password>  
echo "Sessions on the letter-quality printer:"  
show (lq_prtr) sessions  
set privilege = user  
)
```

This example shows the contents of a macro that includes an Echo command. The macro is executed by a port with User privilege to determine the availability of a printer. The macro first turns off echo during macro execution in order to prevent the password from echoing on the terminal when the port's privilege level is set to Global Network Manager. The string enclosed in quotation marks echoes on the terminal, then the output of the SHow command. Finally, the port's privilege level is reset to User.

Normal Response

The specified string is displayed on the terminal, followed by a new prompt. If the command is executed within a macro, the new prompt appears after any output from commands within the macro, when macro execution is complete.

Error Messages

"Invalid Echo syntax"

3.2.8 Listen Command

Syntax

Listen
Listen (<address>)

Default Privilege Level

User

Description

If a port is in Command or Data Transfer mode, the Listen command disconnects all sessions on the port and puts the port in Listening mode. While a port is in Command mode, no connection can be established to that port from a remote device until either the Listen command is given or the Autolisten interval elapses.

If a port is in a reserved state waiting for a passive connection from a queued port, a Listen command directed at the reserved port removes the requesting port from the queue and frees the destination port for connection with the next port in the queue, if any. A second Listen command within a minute clears all remaining ports from the connection queue and puts the port in Listening mode. Section 2.3.4 describes the modes of operation; Section 2.3.10 describes call queueing.

Call queueing does not apply to servers running the TCP protocols.

Example 1

```
listen
```

This example breaks any existing connections and puts the local port in Listening mode so that connections can be made to it.

Example 2

```
l (!3)
```

This example terminates all existing sessions and puts port 3 on the local server in Listening mode.

Normal Response

If a terminal is attached to the affected port, the Listen command usually causes a single "at" sign (@) to appear on the screen. A new prompt appears on the screen, too, if the requesting port is not the affected port.

Error Messages

```
"Insufficient privilege"  
"Invalid Listen syntax"  
"Invalid network manager syntax"  
"Invalid <physical-address> syntax"
```

3.2.9 Name Command

Syntax

Name <clearinghouse name> = <address> [,<address>]

Name <internet name> = <address>

Default Privilege Level

Local Network Manager

Description

The Name command assigns a logical name to either a physical address or another logical name. The address or name specified after the equal sign can represent a single port, a local rotary (a port number in the range from 128 to 135), or a global rotary (up to eight addresses separated by commas). The maximum permitted length of the address (or address list) specified in the Name command is 120 characters. Sections 3.1.6 and 3.1.7 describe XNS clearinghouse names and addresses; Sections 3.1.8 and 3.1.9 describe TCP/IP internet names and addresses.

For servers running the XNS protocols, the specified name typically represents only the first field in the three-part clearinghouse name (the local name, described in Section 3.1.6). The default strings for the second and third fields (domain and organization) are set with the SETDefault command, either locally (for servers that boot from a local disk drive), or remotely (for servers that boot from an NCS). These default strings are automatically assumed if the Name command is entered with only a local name. All the servers supported by an NCS share the same default domain and organization strings.

The Name command can specify all three fields of a clearinghouse name on an XNS server. In this case, the newly defined domain and organization strings can be different from the default strings defined for the server; if the strings are different, the name does not appear in the display generated by the SHow CHName command (refer to the description of the SHow command).

Each internet name consists of a simple character string. The only non-alphanumeric characters permitted in internet names are the underscore (_), the period (.), and the dash (-).

If the XNS server boots from an NCS, the network manager must establish all names on the NCS that supports the server. The Name command is not valid on diskless servers.

Series/1 and Series/100 servers that boot from an internal disk drive and Series/200 servers can be set during system generation to differentiate or not to differentiate between upper- and lowercase in names. The IVECS does not differentiate between cases in names.

If the Name command cannot be completed because the diskette is write-protected, the system puts a protective lock on the name database. The database will not be available again until the server is rebooted with a diskette that is not write-protected.

The Series/1 servers that boot from a local disk drive can each support up to 64 names; a CS/100 that boots locally can support up to 24 names; an NCS/150 can support up to 256 names; an NCS/1 can support up to 4,096 names.

Each TCP server, including the NCS/150-T, can support up to 100 names.

Names are removed using the UNName command.

Example 1

```
name modem = %1234abcdf
```

This example assigns the clearinghouse name "modem" to port 1 on the device whose Ethernet address is %1234abcdf

Example 2

```
n hosta = %080002000015!128
```

This example assigns the clearinghouse name "hosta" to rotary number 128 on the server with the Ethernet address %080002000015. Rotary number 128 must be assigned one or more physical ports through the ROTary command.

Example 3

```
n acctg = host1!132
```

This example assigns the clearinghouse name "acctg" to rotary number 132 on the server named "host1". Rotary number 132 must be assigned one or more physical ports through the ROTary command.

Example 4

```
n x25host = %080002010020!128#31144151234501
```

This example assigns the clearinghouse name "x25host" to rotary number 128 on the CS/1-X.25 or Gateway Server/1 through which the X.25 network is accessible. The number following the number symbol (#) represents the host's X.25 address. Rotary 128 must also be associated with one or more port numbers through the ROTary command.

Example 5

```
n cs_8a = %08000200008a
```

This example assigns the clearinghouse name "cs_8a" to the server with Ethernet address %08000200008a. This clearinghouse name can be used as shorthand for the server's full Ethernet address in the REMOTE command or in conjunction with a port number in the Connect command.

Example 6

```
n modem@acctg@finance = %080002010024!12
```

This example, which specifies all three fields of the clearinghouse name (localname@domain@organization), assigns a name to port 12 on the server whose Ethernet address is %080002010024.

Example 7

```
n hostb = cs_1!128,cs_2!128
```

This example assigns the clearinghouse name "hostb" to a global rotary. The global rotary itself consists of two local rotaries, one on the server named "cs_1", and the other on the server named "cs_2". Local rotaries apply on both XNS and TCP servers; global rotaries apply only to XNS servers.

Example 8

```
n host1 = 192.000.000.254
```

This example assigns the TCP/IP internet name "host1" to the Internet address "192.000.000.254". The address can represent a single port or a rotary. Example 8 applies only to TCP servers.

Normal Response

If the command is successful, the system responds with a new prompt.

Error Messages

"Clearinghouse name in use" (XNS only)

"Clearinghouse name table is full" (XNS only)

"Insufficient privilege"

"Invalid Name syntax"

"Invalid <physical-address> syntax"

"Name in use" (TCP only)

"Name table is full" (TCP only)

3.2.10 Pause Command

Syntax

Pause [<number>]

Default Privilege Level

User

Description

The Pause command causes the system to pause for the number of seconds specified. This command is normally used only within a macro. It can be used in conjunction with other commands to create a macro that makes a connection to a host, pauses long enough for the host to respond, and then transmits a login sequence. A pause between making a connection and transmitting a string is useful for automatic dial-out through an intelligent modem (see the discussion of the DEFine command). The Pause command is also used with a sequence of SHow commands, which can fill up all available buffers unless separated by a Pause.

If no number of seconds is specified, the system pauses for one second. The maximum length of a pause is one day (86400 seconds).

Example

```
pause 2
```

This example causes the system to pause for two seconds before executing the next command of the macro in which the pause appears.

Normal Response

The system pauses for the number of seconds specified, up to a maximum of 86400. No other confirmation is displayed.

Error Messages

"Invalid Pause syntax"

3.2.11 ReaD Command

Syntax

```
ReaD DefaultParameters <filename>  
ReaD (!<portid>) DefaultParameters <filename>
```

Default Privilege Level

Local Network Manager

Description

The ReaD command is used to restore the in-memory copy of a port's configuration table (a set of parameter values) from a specified file on the diskette. Before entering the command, verify that the diskette is in place in the disk drive. The restored configuration applies to the port from which the command was issued or to the port specified in the network manager form of the command.

When configuration tables are restored via the ReaD DefaultParameters command, the existing default parameter table in the server's memory is replaced by the table in the file identified by <filename>. Session parameters take effect at the onset of the next new session.

The specified filename can be an alphanumeric name or a number in the range 0 through 63. The system does not differentiate between upper- and lowercase in filenames. A number is a special kind of filename; each number corresponds to a port number. File number 0 contains the default configuration table for port 0, file number 1 contains the default configuration table for port 1, and so on. Regardless of whether the Communications Server boots from a local disk drive or from an NCS, each server has its own set of numbered default configuration files. A server that boots from an NCS, however, shares a set of named configuration files with all other servers supported by the same NCS.

The ReaD DefaultParameters command reads and automatically saves the default configuration table to diskette. For example, a user can read a numbered file containing the default configuration table for another port into the port 8 table: the configuration table for port 8 is then automatically saved on the diskette. Figure 4-1 illustrates the effects of the ReaD command with the DefaultParameters argument.

Example 1

```
read (!8) defaultparameters 10
```

In this example, the ReaD command creates a new default parameter table for port 8 by reading the parameters currently stored as a default table for port 10 into the default parameter table for port 8. To ensure that the in-memory and disk copies of the table are identical, the ReaD command automatically saves the new file to the system disk.

Example 2

```
rd (!6) dp vt100
```

This example first copies the alternate parameter table contained in the file "vt100" (a set of parameters appropriate for a particular terminal type) into the in-memory default parameter table for port 6, and then saves the in-memory default parameter table to the disk.

Normal Response

"Portid !<n> DefaultParameters loaded from configuration <filename>"

Error Messages

"Drive door open or diskette missing"

"File not found"

"Insufficient privilege"

"Invalid network manager syntax"

"Invalid Read syntax"

"Read error"

3.2.12 REMOTE Command

Syntax

REMOTE <address>

Default Privilege Level

Global Network Manager

Description

The REMOTE command gives the Global Network Manager access to a network management port on the specified NCS, CS/1-X.25, Gateway Server, Internetwork Bridge, or remote Communications Server.

While remote mode is in effect, the prompt is the string "remote:". To exit remote mode, press the break key or the character defined by the BReakChar parameter.

Because the network management port cannot be part of a virtual circuit connection, only a subset of the standard commands are available in remote mode. Specifically, commands used to create and manipulate sessions are restricted; the DEQueue, REMoteSET, REMoteSHOW, RESume, SWitch, and Transmit commands are unavailable and the Connect command can be used only to interconnect remote ports. On an NCS, no commands associated with establishing connections are available. Recursive macros cannot be used in remote mode. The help facility is available in remote mode; enter a question mark (?) in response to the remote system prompt to display a list of available commands.

The commands available during remote access vary depending on the server type. For example, the commands available in remote mode to an NCS differ from those available during remote access to a Communications Server. Each *NCS Installation and Operation Guide* describes the commands available on an NCS.

Remote access can be made to a Gateway Server on the local Ethernet or through a Gateway Server to a server on another Ethernet. However, a remote connection across a gateway is subject to some limitations. The output of some commands that cause long screen displays (such as "SHow (!<portid>) Parameters" and "SHow STATistics") is truncated.

Remote access cannot be made from an XNS server to a TCP server, or vice versa.

Example

```
remote cs.host1
connect (!2) !8
show allsessions
<BREAK>
```

In this example, the network manager requests remote mode access to the Communications Server whose clearinghouse name is "cs.host1", forms an interconnection between ports 2 and 8 on that Communications Server, requests a list of all sessions on that server, and then exits remote mode.

Normal Response

The prompt "remote:".

Error Messages

"Insufficient privilege"

"Invalid <physical-address> syntax"

"Querying Clearinghouse ... Clearinghouse name not found"

In addition, if a server accessed in remote mode is inoperative, all commands entered generate the message "Timeout failure".

3.2.13 REMoteSET Command

Syntax

REMoteSET <param-name> = <value> ...

Default Privilege Level

User

Description

The REMoteSET command sets a parameter on the port at the other end of the active session. The command enables users to change parameters on a destination port without accessing a higher privilege level. The command can affect only a port at the other end of an existing connection; otherwise, the REMoteSET command is identical to the SET command.

The parameters that can be set with the REMoteSET command are limited both by the privilege level of the port on which the command is issued and by the parameters supported by the server at the other end of the connection.

For example, the CS/1-HSM supports only a subset of the port configuration parameters available to a CS/1 with an asynchronous interface. If the user's connection is to a port on a CS/1-HSM, only the parameters supported by the CS/1-HSM can be specified with the REMoteSET command. The CS/1 supports higher baud rates than the CS/100. If a user at a CS/1 port requests a higher baud rate for a CS/100 port than is available, the baud rate is actually set to the highest possible rate for the CS/100 (19.2K baud).

This command is not valid on TCP servers.

Example

```
remset baud=1200
```

This example sets the baud rate of the remote device to 1200.

Normal Response

If the command is successful, the system responds with a new prompt.

Error Messages

```
"Ambiguous parameter name, try one of: <...>"
"Insufficient privilege"
"Invalid REMoteSET syntax"
"Missing equal after parameter <param-name>"
"Missing value after parameter <param-name>"
"Parameter <param-name> unknown"
"Parameter <param-name>: value '<value>' is illegal"
"Parameter <param-name>: value '<value>' is out of range"
```

3.2.14 REMoteSHow Command

Syntax

REMoteSHow <param-name>

Default Privilege Level

User

Description

The REMoteSHow command displays a parameter value for the port at the other end of the current session. It follows the same conventions as the SHow <param-name> command.

The REMoteSHow command is not valid on TCP servers.

Example

```
remsh baud
```

This example requests that the baud rate of the remote device be displayed.

Normal Response

The response depends on the display requested.

Error Messages

"Ambiguous parameter name, try one of: <...>"

"Insufficient privilege"

"Invalid REMoteSHow syntax"

"Parameter <param-name> unknown"

3.2.15 RESume Command

Syntax

```
RESume [<session number>]
```

Default Privilege Level

User

Description

The RESume command changes the local port from Command mode to Data Transfer mode, resuming communications for the specified session. If no session number is specified, the current session is resumed.

If the local port has just been notified that a queued connection is available, the RESume command completes the process of establishing the connection. The queued session has its own session number, which must be entered if a different session is active when the notification is received.

The RESume command is meaningful only if a completed or queued connection exists on a port.

Example 1

```
resume
```

This example resumes Data Transfer mode for the current session.

Example 2

```
res 2
```

This example resumes Data Transfer mode for session 2.

Normal Response

```
"Session <n> with <address> resumed"
```

```
"Queued session <n> connecting ... Access controlled Group <n> password:"
```

```
"Queued session <n> connecting ... Session <n> connected to <address>"
```

Error Messages

```
"Illegal request -- wrong state"
```

```
"Invalid RESume syntax"
```

```
"Invalid session number"
```

```
"No current session"
```

```
"No other sessions"
```

```
"Queued session <n> connecting ... No response"
```

```
"Queued session <n> connecting ... Remote is busy"
```

```
"Queued session <n> connecting ... Remote is disabled or nonexistent"
```

```
"Queued session <n> connecting ... Timeout failure"
```

3.2.16 ROTary Command

Syntax

```
ROtary !<rotary> = !<port> [- !<port>] [, !<port> ... ]
ROtary !<rotary> += !<port> [- !<port>] [, !<port> ... ]
ROtary !<rotary> -= !<port> [- !<port>] [, !<port> ... ]
```

Default Privilege Level

Local Network Manager

Description

The ROTary command is used to assign a rotary number to a single port number or a group of port numbers. The second form of the command adds ports to an existing rotary, and the third form of the command removes ports from an existing rotary.

The ROTary command creates a local rotary only; if a group of port numbers is specified, all ports in the group must be on the same server. Global rotaries are established via the Name command. Global rotaries do not apply to TCP servers. Local and global rotaries are described in Section 2.3.8.

Each server has its own rotary list regardless of its boot source. Eight rotary numbers are available for use on each server; rotary numbers range from 128 to 135.

The Connect command can use a rotary number as the destination, indicating that any of the ports assigned to that number is equally acceptable. The rotary number can also be assigned a clearinghouse or internet name, via the Name command, and thus can be specified in the Connect command by name.

A single rotary command can include a single port number, a series of nonconsecutive port numbers, a range of consecutive port numbers, or a combination of consecutive and nonconsecutive port numbers. If a series of nonconsecutive port numbers is specified, the port numbers must be separated by commas (,); if an inclusive range of consecutive port numbers is specified, the starting port number must be separated from the ending port number by a hyphen (-). See the examples below.

A single rotary number can be assigned to both physical and virtual ports.

A network manager can enter the SHow ROTaries command to display a list of all currently established rotaries and their assigned port numbers. On servers running the TCP/IP protocols, the resulting list shows only port numbers, not Internet addresses; the network manager can use the SHow InternetPorts command to display the mapping between port numbers and Internet addresses.

Example 1

```
rotary !128 = !4,!7,!13,!15
name host1 = !128
```

In this example, the ROTary command assigns rotary number 128 (!128) to ports 4, 7, 13, and 15 on the local server. Next, the Name command assigns the clearinghouse name "host1" to the addresses represented by rotary number 128. The user can then simply type the command "connect host1" to obtain a connection to any available port in the rotary.

Example 2

```
ro !129 = !20-!31
n host2 = !129
```

In this example, the ROTary command assigns rotary number 129 to ports 20 through 31 on the local server. The Name command then assigns the clearinghouse name "host2" to the rotary.

Example 3

```
ro !130 = !4,!7,!13,!15,!20-!31
n host3 = !130
```

This example represents a combination of examples 1 and 2. The ROTary command is used to assign rotary number 130 to ports 4, 7, 13, 15, and 20 through 31 of the local server. Then the Name command is used to assign the name "host3" to the combined rotary.

Example 4

```
ro !128 -= !7, !13
```

This example removes ports 7 and 13 from rotary 128. No other ports in the rotary are affected.

Example 5

```
ro !130 = !0-!6
setd (!130) ip = 192.0.0.5
name host1 = 192.0.0.5
```

In this TCP example, the ROTary command assigns rotary number 130 (!130) to ports 0 through 6 (!0 through !6) on the local server. Next, the SETD command assigns the Internet address 192.0.0.5 to rotary number 130. Finally, the name "host1" is assigned to the Internet address 192.0.0.5.

Normal Response

If the command is successful, the system responds only with a new prompt.

Error Messages

```
"Insufficient privilege"
"Invalid ROTary syntax"
"Missing equal sign after <rotary number>"
"Portid out of range"
"Rotary number out of range"
```

3.2.17 SAve Command

Syntax

SAve DefaultParameters <filename>
 SAve (!<portid>) DefaultParameters <filename>
 SAve Parameters <filename>
 SAve (!<portid>) Parameters <filename>

Default Privilege Level

Local Network Manager

Description

The SAve command writes a configuration table (a set of port parameters) to the diskette under the filename specified. Before entering the command, verify that the diskette is in place in the disk drive. A saved configuration table can be restored via the ReaD command. Tables saved in a numbered file are automatically restored at boot time.

If a question mark is substituted for an argument in the SAve command, the server displays a help screen describing all the valid forms of the command.

If the command line specifies DefaultParameters, the port's default configuration table is written onto the file specified by <filename>. If the command line specifies Parameters, the port's current configuration table is written onto the file specified by <filename>.

The filename can be alphanumeric or a number in the range 0 through 63 (0 through 13 on a CS/100). If an alphanumeric name is entered, the configuration information is stored on the diskette as an alternate configuration, not a default configuration. The Connection Service does not distinguish between upper- and lowercase in filenames. A number is a special kind of filename that is linked to port number. A configuration table saved with a number as filename becomes the new default configuration table for the port with that number.

** NOTE **

When a server is booted, the default configuration table for each port is read from the file whose name corresponds to the port number. This process overrides any previous attempt to save a default configuration table under any name other than a port number.

If the SAve command is used to write to a numbered file, it should be used in conjunction with the ReaD command, in order to maintain consistency between the default parameter values stored on the disk and the default parameter values stored in memory. Refer to example 2, below, for an illustration of the ReaD command used in conjunction with the SAve command.

If the specified file already exists, the new parameter table overwrites the old file.

A Communications Server that is to be booted from an NCS must be bound to the NCS before the SAve command is issued (each *NCS Installation and Operation Guide* provides more information).

Regardless of whether the server boots from a local disk drive or, for a Communications Server only, from an NCS, each server has an independent set of numbered default configuration files. A server that boots from an NCS, however, shares a set of named configuration files with all other servers supported by the same NCS.

Saving numbered configuration files requires only Local Network Manager privilege level on all servers. On a server that boots from an NCS, saving named configuration files requires Global Network Manager privilege level.

Example 1

```
save parameters port4.conf
```

This example writes the configuration table for the current session on the local device port to the file "port4.conf" on the diskette.

Example 2

```
rd (!5) dp 0  
sa (!5) dp 5
```

This example first reads the default parameter table for port 0 to the default parameter table for port 5, then saves port 5's new default parameter table to disk. Port 0's current and default configuration tables remain unchanged.

Normal Response

```
"Portid !<n> default parameters saved as configuration <filename>"  
"Session <n> parameters saved as configuration <filename>"
```

Error Messages

```
"Can't SAve"  
"Diskette write protected"  
"Drive door open or diskette missing"  
"Insufficient privilege"  
"Invalid network manager syntax"  
"Invalid SAve syntax"  
"Write error"
```

3.2.18 SET Command

Syntax

```
SET <param-name> = <value> ...
SET (<address>) DATE = yy/mm/dd hh:mm[:ss]
```

Default Privilege Level

User

Description

The SET command sets a configuration parameter value. The new value takes effect immediately, but remains in effect only for the current session. The SET command differs from the SETDefault command in that a parameter value specified with the SETDefault command takes effect only with the following session, then remains in effect until an explicit SETDefault or SET command overrides it.

The command "set ?" prints a list of all parameters that can be specified.

When multiple values are specified for a single parameter, the values must be separated by commas and enclosed in parentheses. If the parentheses are omitted, the server generates an error message, but the first of the multiple values is written to the active parameter table anyway.

The network manager form of the SET command can be used only to set the system clock. If any parameter other than DATE is specified in this form of the command, an error message is generated. In networks that include an NCS, the NCS automatically sets the system clock on each server in the network. However, SET DATE may be used on Communications Servers to set the date of all the servers on the network including the NCS, if necessary (i.e., in case of a time change, such as daylight savings). For networks that do not include an NCS, the date of the local server and all other servers in the network can be specified using the broadcast address (%ffffffff for XNS networks; 255.255.255.255 for TCP networks) in the SET DATE command. Section 3.1.5 defines the rules that govern the way parameter values are specified; Section 4.0 lists the parameters that can be specified with the SET and SETDefault commands.

On a server with internal disk drive, the network manager can change the privilege levels as required to execute commands. Do not establish a privilege level other than User for the SET command. Otherwise, no one will be able to access higher privilege levels, which is done only through the SET command.

Example 1

```
set breakaction = inband
set ecmchar = ^C
```

This example sets parameters appropriate for an application requiring the capability of transmitting in-band breaks. The second SET command provides a way to return to Command mode via an ECMChar (the character <CTRL-C>).

Example 2

```
set (%ffffffff) date = 86/06/26 10:15:00
```

This XNS example sets the system clocks on all Bridge servers on the network, including the local Communications Server, to 10:15 a.m. on June 6, 1986.

Example 3

```
set (255.255.255.255) date = 86/03/03 21:15:00
```

This TCP example sets the system clocks on all Bridge servers on the TCP network, including the local Communications Server, to 9:15 p.m. on March 03, 1986.

Normal Response

If the command is successful, the system responds only with a new prompt.

Error Messages

```
"Ambiguous parameter name, try one of: <...>"  
"Insufficient privilege"  
"Invalid SET DATE syntax"  
"Invalid SET syntax"  
"Missing equal sign after parameter <param-name>"  
"Missing value after parameter <param-name>"  
"Parameter <param-name> unknown"  
"Parameter <param-name>: value '<value>' is illegal"  
"Parameter <param-name>: value '<value>' is out of range"
```

3.2.19 SETDefault Command

Syntax

```
SETDefault [<param-name> = <value>] ...
SETDefault ( <address> ) [<param-name> = <value>] ...
SETDefault (!<port-id>) ip = <Internet address>
```

Default Privilege Level

Local Network Manager

Description

The SETDefault command is used to modify a port's default parameter table or the system's global parameters. The SETDefault command is also used to assign an Internet address to a port (TCP only).

A physical parameter specified with the SETDefault command takes effect after a Listen command has been issued to the port; a session parameter set with the SETDefault command goes into effect with the next new session. A parameter specified with the SET command takes effect immediately but remains in effect only during the current session.

If the SETDefault command is specified without parameters, the server prompts the user for all parameters, indicating the current default within angle brackets. To leave the default value unchanged, press the return key. To obtain a help screen listing legal values for the parameter being prompted for, enter a question mark (?). To cancel the remainder of the SETDefault, press the break or escape key. Any changes made prior to the time the break or escape key is pressed take effect.

When multiple values are specified for a single parameter, the values must be separated by commas and enclosed in parentheses. If the parentheses are omitted, the server generates an error message, but the first of the multiple values is written to the default parameter table anyway. The modified parameters are written to the diskette automatically after the SETDefault command is completed.

Each of the following types of parameter specifications is stored in a different disk file:

- Default port parameters and editing parameters listed in Sections 4.1.1 through 4.1.4 for asynchronous or 3270 ports and in Sections 4.2.1 through 4.2.4 for virtual ports on the GS/1.
- Passwords listed in Section 4.1.5 for asynchronous or 3270 servers and in Section 4.2.5 for the GS/1.
- Clearinghouse strings listed in Section 4.1.5 for asynchronous or 3270 servers and in Section 4.2.5 for the GS/1.
- All other global parameters listed in Section 4.1.5 for asynchronous or 3270 servers and in Section 4.2.5 for the GS/1.

Since a single SETDefault command can update only one disk file, the command line must not include specifications from more than one of the above categories.

A parameter table can also be written to the diskette with the SAve command, and a saved parameter table can be restored from the diskette with the ReaD command. There is no need to ReaD the parameter table after issuing the SETDefault command; the command alters both the default table on the disk and the default table in the server's memory.

On a Communications Server that boots from an NCS, the passwords described in Section 4.0 must be altered with the SETDefault command on the NCS which supports that server. All Communications Servers supported by a single NCS share the same GlobalPassWord and the same set of access control passwords. Access control does not apply to servers running the TCP protocols.

Section 3.1.5 lists the rules governing the way parameter values are specified; Section 4.0 describes all parameters that can be specified with the SET and SETDefault commands.

Example 1

```
setdefault prompt="cs_acctg> "
```

This example sets the prompt for terminal ports with User level privilege to the string "cs_acctg>".

Example 2

```
setd baud=300 databits=7 stopbits=2 parity=0
```

This example sets the local port's default baud rate, number of databits, number of stopbits, and parity.

Example 3

```
setd (!3) device = (term,paper)
```

In this example, the device attached to port 3 is configured as a hardcopy terminal.

Example 4

```
setd (!6) ip = 127.0.0.5
```

This TCP example assigns the Internet address 127.0.0.5 to port 6. This example is valid only on TCP servers.

Normal Response

The system either responds with a new prompt or displays the following message:

```
"Portid !<n> default parameters saved as configuration <n>"
```

Error Messages

```
"Ambiguous parameter name, try one of <...>"
```

```
"Insufficient privilege"
```

```
"Invalid SETDefault syntax"
```

```
"Missing equal sign after parameter <param-name>"
```

```
"Missing value after parameter <param-name>"
```

```
"Parameter <param-name> unknown"
```

```
"Parameter <param-name>: value '<value>' is illegal"
```

```
"Parameter <param-name>: value '<value>' is out of range"
```

3.2.20 SHow Command

Syntax

```
SHow <show-keyword> [ <parameter> ... ]
SHow (<address>) <show-keyword> [ <parameter> ... ]
```

Default Privilege Level

User

Description

The SHow command is used to display current parameter values and other system information.

Depending on customer requirements, some SHow keywords and some SHow parameters may be restricted to Local or Global Network Manager privilege. At the Global Network Manager privilege level, most of the SHow commands can take an Ethernet address before the keyword (see example 9, below). The displays generated by the SHow command are tailored to the privilege level of the requesting port.

The SHow keywords that are valid on an Internetwork Bridge or on an NCS in remote mode may differ from the keywords specified in the list below. Each *NCS Installation and Operation Guide* provides complete listings of SHow keywords for the NCSs.

The command "show ?" displays a list of the valid SHow keywords appropriate to the port's privilege level, indicating command format. When a keyword applies only to a particular server, the appropriate server is noted. Otherwise, the keywords listed are valid on both XNS and TCP servers.

```

SHow ADDRESS
SHow AllSessions [ p ]
* SHow AttachedNets
* SHow CHNames [ <name> [ @ <domain> [ @ <organ.> ] ] ]
SHow CONFigurations [ <filename> ]
SHow DATE
SHow [ ( <address> ) ] DefaultParameters [ <param-name> ... ]
SHow GLobalPARameters
* SHow GRoupPassWords
** SHow InternetPorts
** SHow InternetServers
*** SHow LineStatus
SHow MACros [ <macro-name> ]
** SHow NAMES [ <name> ]
SHow NetMap [ Short | Long ]
```

* Valid only on XNS servers.

** Valid only on TCP servers.

*** Available only in remote mode to a GS/3 or GS/300.

```

    SHow [ (<address> ) ] PARAMeters [ <param-name> ... ]
    SHow <param-name> ...
*   SHow RemoteNets [ <netid> ... ]
    SHow ROtaries
    SHow SECuritySTATistics
    SHow [ (<address> ) ] SESsions [P]
    SHow (<address>) STATistics
    SHow STATistics [ Sample | Minute | <hour> | Day ]
    SHow VERSion
    SHow VirtualPorts
**  SHow X25Addresses [ <netid> ]
**  SHow X25Connection [ <line number> ]

```

If the SHow command is entered with no keyword specified, the Connection Service assumes PARAMeters as the default keyword.

SHow ADDRESS on all XNS servers displays the Ethernet address of the local server, the port number of the local port, the bootstrap source of the local server, and the time and date it was last booted. On TCP servers, this command displays the port number and either the Internet address (if one is assigned) or the words "active only".

SHow AllSessions displays a list of all physical ports on the server and their statuses. The logical names of destination devices are shown for ports that are involved in a connection. With the p option, the physical addresses of the destination devices are shown instead of their logical names.

On TCP servers, the resulting list shows physical port numbers, not Internet addresses. Use the SHow InternetPorts command to display the mapping between physical ports and Internet addresses.

SHow AllSessions displays all physical ports; SHow VirtualPorts, described below, can be used to display all virtual ports.

SHow AttachedNets displays the network number of the local Ethernet network. If the command is executed remotely on the Gateway Server, the system displays the network numbers of all Ethernet networks attached to the gateway. This command is not available on TCP servers.

SHow CHNames displays a list of clearinghouse names. The clearinghouse names represent physical addresses or sets of physical addresses on the system. To display the physical address that the clearinghouse name maps into, use the command SHow CHNames <clearinghouse names>.

Ordinarily, the SHow CHNames command displays only the clearinghouse names in the local clearinghouse whose domain and organization strings match the default domain and

* Valid only on XNS servers.

** Valid only on the CS/1-X.25 or the GS/1.

organization strings for the local server. If some clearinghouse names have been established with unique domain and organization strings, the entire list can be displayed with this form of the command:

SHoW CHNames *0*0*

For a server supported by an NCS, clearinghouse names are stored on the NCS*. The **SHoW CHNames** command (without an argument) displays only those names with the same domain and organization strings as the server on which the command was entered. This command can be entered either locally or remotely on an NCS. If the servers have different default domain and organization strings, the resulting displays are different.

This command is available only on Communications Servers running the XNS protocols. The **SHoW NAmes** command provides a similar function on servers running TCP protocols. The **NAmes** keyword is described later in this section.

SHoW CONFIgurations displays a list of all configuration tables saved on the disk. The list of tables includes both default tables (those whose filenames consist of a port number) and alternate tables (those whose filenames consist of alphanumeric characters). **SHoW CONFIgurations <filename>** displays the contents of the parameter table contained in the specified file; both default and alternate tables can be displayed.

SHoW DATE displays the current date and time. If the server boots from internal disk drive, **DATE** is typically set after each system boot with the **SET** command (discussed in Section 3.2.18). If the server is supported by an NCS, **DATE** does not need to be reset.

SHoW DefaultParameters displays the default parameters for the specified port or, if no port is specified, for the port on which the command is typed. To display a few specific default parameters, type the command and keyword followed by the names of the parameters. To display a list of all default parameters, type the command and keyword only. During remote access to another server, the **SHoW DefaultParameters** command must include a port number; if none is specified, the system displays the remote server's global parameters instead.

SHoW GLoBalPARAmeters displays the global parameters discussed in Section 4.1.5 for asynchronous or 3270 ports and in Section 4.2.5 for virtual ports on the GS/1 (except for the access group passwords). The display is tailored to the privilege level of the requesting port.

SHoW GRoupPassWords displays a list of all 16 access groups and their passwords to the user with global network management privilege level. This command is available only on XNS servers.

SHoW InternetPorts displays the Internet address and Ethernet address of the local server, as well as the mapping of physical ports and rotary numbers to Internet addresses. This command is valid only on TCP servers.

SHoW InternetServers displays the Internet addresses of the Name Servers, the Default Gateway, the BootServer, and the **AUDitServers** on the TCP network. This command is valid only on TCP servers.

* If a non-client server is in the network, it can have its own name database.

SHoW LineStatus is valid only in remote mode to a GS/3, GS/3-IP, or GS/300. The command displays a list of each line leading from the Gateway Server, the line's baud rate, the line's state, and the network number of the network to which the line leads. The state may be one of the following:

Down	No remote Gateway Server can be detected on this line.
Faulty	The line has been disabled due to excessive line state transitions; the Gateway Server reinstates the line when it has stabilized.
Loopback	The line is not being used because the attached modem has gone into loopback mode.
Up	The line is in normal operation.
Wrong NetID	The line has been disabled because network numbers received over the network do not match those specified during system generation.

SHoW MACros without an argument displays a list of all macros defined for the local server (if the server boots locally) or a list of all shared macros (if the server boots from an NCS). **SHoW MACros <macro-name>** displays the contents of the specified macro.

SHoW NAmes displays a list of internet names. The names represent Internet addresses or sets of addresses on the TCP/IP system. To display the Internet address that the name maps into, use the command **SHoW NAmes <internet name>**. This command is valid only on TCP servers.

SHoW NetMap displays a list of the addresses of all Bridge servers on the network that run the same set of high-level protocols as the server on which the request is entered (e.g., from a TCP server, the list includes only TCP servers). The first address in the list is always the local server.

If the command includes the additional keyword "Long"*, the resulting list also indicates the software release number of any server on the network running SW/1-A/BSC/SDLC Release 20000 or higher or SW/100-A/BSC Release 15000 or higher.

On a Series/1 server, a maximum of 200 addresses are included in the display; on a CS/100, a maximum of 40 addresses are included. Any server that has been down for 5 minutes or longer is indicated in the list as inactive; after the server has been inactive for 72 hours, it is removed from the netmap list.

SHoW PARAMeters is like **SHoW DefaultParameters**, except that **SHoW PARAMeters** displays the parameters for the current session. If no connection has been established, the display includes only the port parameters, since no session parameter table exists for a port without sessions. The keyword **PARAMeters** can be omitted from a request for one or more specific parameters. That is, the command "**SHoW BAud**" is equivalent to the command "**SHoW PARAMeters BAud**". During remote access to another server, the **SHoW DefaultParameters** command must include a port number; if none is specified, the system displays the remote server's global parameters instead.

* Unavailable on CS/100.

SHoW RemoteNets displays a list of all networks available through gateways on the local network. If the keyword is followed by a network identification number, the system displays the Ethernet addresses of the Gateway Servers through which that network can be accessed. This command is not valid on TCP servers.

SHoW ROTaries displays a list of rotary numbers and the ports that have been assigned to them. For TCP servers, the list indicates physical port numbers, not Internet addresses. Use the SHoW InternetPorts command to display the mapping between port numbers and Internet addresses.

SHoW SECuritySTATistics is valid only on XNS servers. The command displays a summary of security-related activity (privilege level and access control) since the most recent system boot. The report is discussed in detail in the *Network Management Guide*.

SHoW SESsions displays a list of all current connections between the specified port and other destinations. On an asynchronous or 3270 server, if the final argument "P" is included, the resulting report shows the physical address of the circuit destination instead of its logical name.

SHoW STATistics can take either of two distinct forms. If it is used without a final argument, SHoW STATistics displays a summary of the statistics for the specified port or, if no port is specified, for the port on which the command is typed. If it is used with one of the four closing arguments (Sample, Min, <hour>, Day), the command displays one of the network management reports for the entire server. The *Network Management Guide* includes a complete discussion of statistics reports.

SHoW VERSion displays the software release number and date of the software currently running on the server, the firmware release numbers of all PROMs in the server, and the time, date, and source of the most recent bootstrap. Section 2.6 describes software and firmware release numbers.

SHoW VirtualPorts displays the connection status (passive or active) of the virtual ports, and the addresses of the ports to which the virtual ports are connected. Section 2.3.3 discusses virtual ports.

SHoW VirtualPorts displays all virtual ports; SHoW AllSessions, described above, can be used to display all physical ports.

SHoW X25Addresses is valid only when issued remotely or directly to a CS/1-X.25 or GS/1. The command displays the Ethernet number and X.25 address of each remote Ethernet accessible from the CS/1-X.25 or GS/1 on which the command is issued.

SHoW X25Connection is valid only when issued remotely or directly to a CS/1-X.25 or GS/1. The command displays a list of the currently active logical channel numbers, local X.25 addresses, and remote X.25 addresses associated with each line on the CS/1-X.25 or GS/1 on which the command is issued.

Example 1

```
show baud echodata
```

This example requests a display of the current values of the parameters BAud and ECHO-Data for the requesting port.

Example 2

```
sh conf 16
```

This example requests a display of the default configuration table for port 16 on the local server.

Example 3

```
sh date
```

This example requests a system clock display.

Example 4

```
sh chn host1*
```

This example requests a display of all clearinghouse names beginning with the letters "host1". This example is valid only on XNS servers.

Example 5

```
sh chn *@*@Bridge
```

This example requests a display of all clearinghouse names whose organization identifier is "Bridge". This example is valid only on XNS servers.

Example 6

```
sh na
```

This example requests a display of all TCP internet names defined on the local Communications Server running TCP protocols. This example is valid only on TCP servers.

Example 7

```
sh na host1
```

This example requests a display of the TCP Internet address represented by the internet name "host1". This example is valid only on TCP servers.

Example 8

```
sh (%080002001234) as
```

This Global Network Manager command requests a display of all sessions on the server whose Ethernet address is %080002001234.

Normal Response

Normal responses depend upon which SHow option is requested.

Error Messages

"Ambiguous parameter name, try one of: <...>"

"Insufficient privilege"

"Invalid network manager syntax"

"Invalid SHow clearinghouse name syntax"

"Invalid SHow STATistics syntax"

"Invalid SHow syntax"

"Parameter <param-name> unknown"

3.2.21 SWitch Command

Syntax

SWitch [`<session number>`]

Default Privilege Level

User

Description

The SWitch command is used to suspend the current session and switch the user device to another session on the port. A session is referred to by its session number. If no session number is specified, the most recently active session becomes active. The port remains in Command mode until the RESume command is entered.

Example

```
switch 2
```

This example requests that the current session be suspended and session 2 be activated.

Normal Response

```
"Switching ... to session <n>"
```

Error Messages

```
"Invalid session number"
```

```
"Invalid SWitch syntax"
```

```
"No other sessions"
```


3.2.22 Transmit Command

Syntax

Transmit <string> | InBandBreak | OutBandBreak

Default Privilege Level

User

Description

The Transmit command is used within a macro definition to instruct the server to transmit the specified string or break signal to the destination of the current session. If the destination of the transmission is an asynchronous or 3270 port whose EOM parameter is set to <CTRL-M>, a return is automatically appended to the string. Otherwise, the user must include a return at the end of the string.

One Transmit command can be used to send either a string or a break, but not both. Section 4.1.7 describes the difference between an in-band break and out-of-band break.

Macros can be defined only by a user with Local or a Global Network Manager privilege level.

The string text must be specified according to the syntax described in Section 3.1.5. The maximum permissible length of the string is 82 characters; if more are specified, an error message is generated and only the first 82 characters of the string are transmitted.

Example 1

```
transmit "myusername"
```

This example transmits the user's login string (myusername) to the destination of the session that is current at the time the macro containing the command is executed.

Example 2

```
t ibb
```

This example transmits an in-band break to the device at the other end of the current session.

Normal Response

Normal responses to the Transmit command depend on the remote device's response to the transmitted text.

Error Messages

```
"Invalid Transmit syntax"
```

```
"String truncated to 82 characters"
```

3.2.23 UNDefine Command

Syntax

UNDefine <macro-name>

Default Privilege Level

Local Network Manager

Description

The UNDefine command deletes a macro from the macro directory. The server does not distinguish between upper- and lowercase in macro names.

On a server that boots from an NCS, the UNDefine command requires Global Network Manager privilege level.

Example

```
undefine TEK
```

This example deletes the macro named "TEK".

Normal Response

If the command is successful, the system responds with a new prompt.

Error Messages

"File not found or in use"

"Insufficient privilege"

"Invalid network manager syntax"

"Invalid UNDefine syntax"

"Macro does not exist"

3.2.24 UNName Command

Syntax

UNName <clearinghouse name | internet name>

Default Privilege Level

Local Network Manager

Description

The UNName command deletes a clearinghouse or internet name assignment previously specified via the Name command. A Series/1 server that boots from an internal disk drive can be configured during system generation to either differentiate or not differentiate between upper- and lowercase in names. If the server does make the distinction, then the name must be entered exactly like the entry in the database, including case. The CS/100 and the NCSs do not differentiate between cases in clearinghouse names.

If a server boots from an NCS, the network manager must establish and delete all logical names on the NCS that supports the server. The NCS can be accessed either through the REMOTE command or from the NCS's console terminal.

Example

```
unname modem
```

This example deletes the clearinghouse entry associated with the name "modem".

Normal Response

If the command is successful, the system responds only with a new prompt.

Error Messages

```
"Clearinghouse name not found"  
"Insufficient privilege"  
"Invalid UNName syntax"  
"Name not found"
```

3.2.25 UNSave Command

Syntax

UNSave <filename>

Default Privilege Level

Local Network Manager

Description

The UNSave command deletes the specified configuration file from the directory on the diskette. On a server that boots from an NCS, the UNSave command requires Global Network Manager privilege level.

On a server that boots from an NCS, the UNSave command can be used to delete a named configuration file, but not to delete a default configuration file (i.e., one whose filename consists of a port number). If the network manager attempts to delete a default configuration file, the server does not generate an error message but does not delete the file.

On a server that boots from a local diskette, the UNSave command can be used to delete both named and numbered configuration files. However, if a numbered configuration file is deleted, the server will no longer have a default configuration file for the port with that number. The next time the system is booted, that port will revert to the original defaults described in Section 4.0.

Example

```
unsave port6.conf
```

This example deletes the saved configuration file named "port6.conf".

Normal Response

If the command is successful, the system responds with a new prompt.

Error Messages

"Drive door open or diskette missing"
"File not found or in use"
"Insufficient privilege"
"Invalid network manager syntax"
"Invalid UNSave syntax"

3.2.26 ZeroStats Command

Syntax

ZeroStats

Default Privilege Level

Local Network Manager

Description

The ZeroStats command sets the value of both the busiest minutes and the busiest sample statistics of the last 24-hour period to zero.

Using the ZeroStats command provides a starting point for analysis of the SHow STATistics performance statistics report. These statistics may be displayed using the SHow STATistics command.

Example:

```
zerostats
```

This example sets the busiest minutes and busiest sample statistics to zero.

Normal Response

A new prompt.

Error Messages

"Insufficient privilege"

4.0 PORT CONFIGURATION

This section describes port configuration parameters for Communications Server ports on asynchronous or 3270 interfaces and for virtual ports on the GS/1.

Each port on a Communications Server and each virtual port on a GS/1 has a set of default configuration parameters that determine how the port and the attached or remote device interact. Some of the parameters may have to be adjusted for the local installation.

The default parameter tables are stored in the server's memory and in files on the diskette. The tables on the diskette are stored with filenames consisting of numbers corresponding to the ports to which the files apply. Default parameters are divided into four categories:

- Port parameters depend on the needs of the device interacting with the port, and typically remain constant for a single port.
- Session parameters are more likely to vary when the device communicating with the port is interacting with different remote devices or running different applications.
- Editing parameters determine the functions of several special characters.
- Global parameters (e.g., passwords or welcome messages) apply to all ports on the server.

When a port becomes active, the system creates a working parameter table by copying the port's port and editing parameters and the global parameters from the default parameter table. When a session is established to a remote device, the server completes the active parameter table by copying the session parameters from the port's default parameter table. For each new session, the system creates a new active parameter table based on the default parameter table.

For asynchronous or 3270 ports and Gateway Server virtual ports, settings in both the active and default parameter tables can be altered. For character-synchronous and bit-synchronous ports, only default parameter tables can be altered. For virtual ports on the CS/1-HSM, CS/1-SNA, and IVECS, only default parameter tables can be altered, and only a limited number of parameters apply. The parameters for these servers are described in the *Network Management Guide*.

Active parameters can be changed only while an active parameter table exists. The SET command changes the active parameter table in the server's memory. The change remains in effect only as long as the active parameter table is in use (i.e., while the port remains in Data Transfer or Command mode or while a connection exists).

Default parameters can be changed at any time. The SETDefault command changes the default parameter table stored on the disk. The change takes effect the next time the system uses the default table to create a new active parameter table, which occurs when the port enters Command mode from Listen mode. Only the default parameters can be altered remotely by the network manager.

**** NOTE ****

A Global Network Manager can set default parameters remotely, but only if the destination server is running, not if it is powered off or running utilities from the monitor.

Some of the commands that affect parameter tables are `ReaD`, `SAve`, `SET`, and `SETDefault`:

- `ReaD` reads an entire table into memory and automatically saves the table onto the diskette.
- `SAve` writes an entire table from memory onto diskette.
- `SET` changes the setting of an active parameter.
- `SETDefault` changes the setting of a default parameter.

Figure 4-1 illustrates the effects of these commands. Section 3.2 describes these commands and the `SHow` command, which, depending on the option selected, displays the parameters in default or active parameter tables.

Many parameters can be specified with either the `SET` command or the `SETDefault` command. Other parameters can be specified only with the `SET` command or only with the `SETDefault` command. The parameter descriptions in the following sections indicate which command(s) can be used to specify each parameter.

In the detailed descriptions, values separated by vertical bars are mutually exclusive (i.e., only one can be specified). Where a list of mutually exclusive values is separated from another such list by a comma, one value can be specified from each list. Sets of nonexclusive values (i.e., more than one of which can be specified) are enclosed in parentheses and separated by commas.

When a connection is made to an X.25 destination, the session parameters may have to be changed to conform to the requirements of the host. When the connection is established, one or more of the default session parameters may be altered from the host side of the connection; these parameters are listed in Section 4.2. In this case, the parameters most likely to affect the user are `ECMChar` and `BReakAction`. For example, if the default parameter table has `ECMChar` set to `<CTRL-^>` and `BReakAction` set to `EscDTM`, when a connection is made either to a host connected to a CS/1-X.25 or to a host on a PDN accessed via a GS/1, the X.25 interface may reset `ECMChar` to `<CTRL-P>` and `BReakAction` to `OutofBand`. As a result, neither `<CTRL-^>` nor the break key can change the port from Data Transfer mode to Command mode.

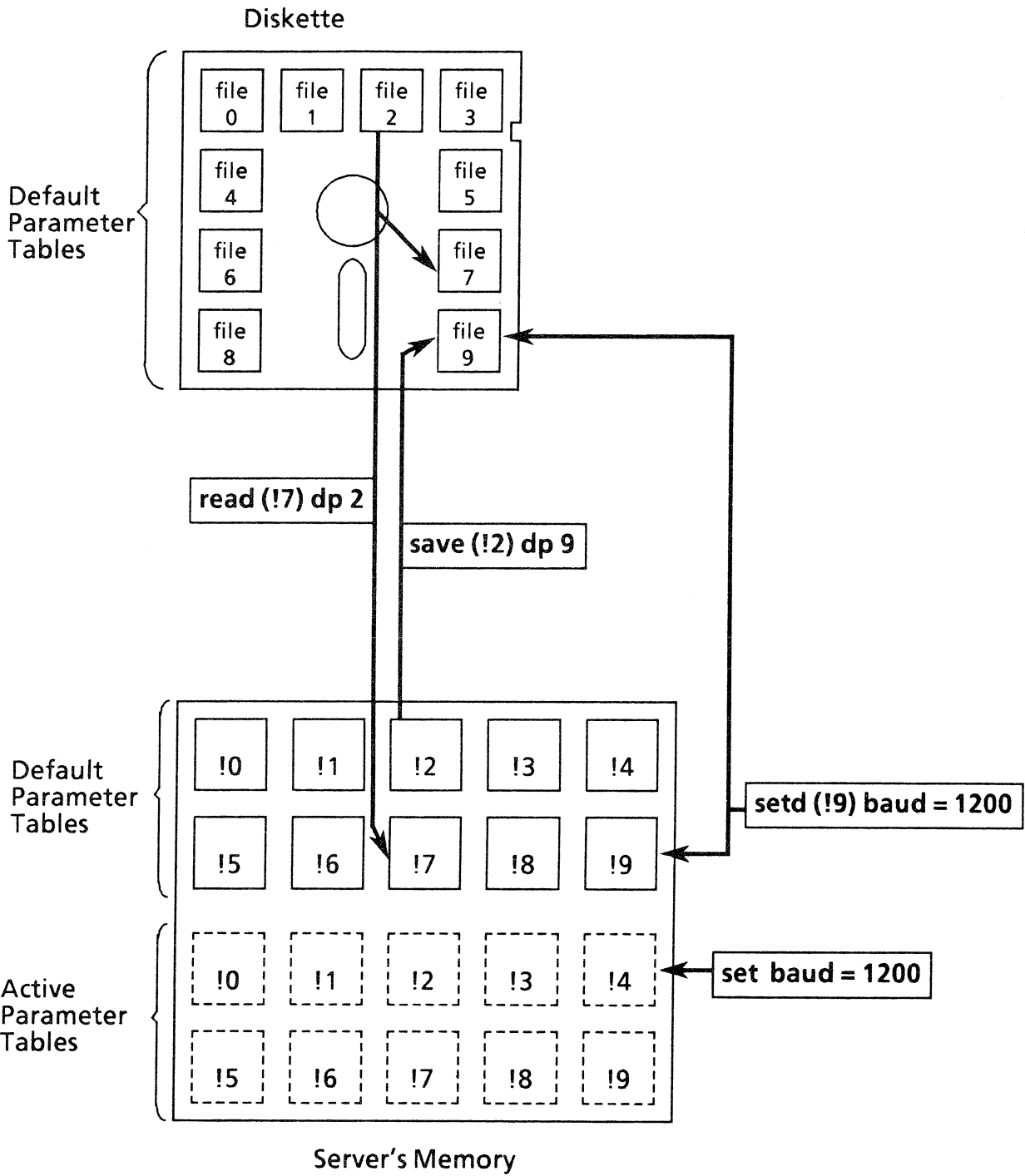


Figure 4-1 Effects of the ReaD, SAve, SET, and SETDefault Commands

4.1 Asynchronous and 3270 Server Configuration Parameters

Table 4-1 lists all asynchronous and 3270 port parameters alphabetically and gives the section number of each description. Uppercase characters represent the minimum unambiguous abbreviation of each parameter. This option is supported on all ports of a CS/1 with asynchronous or 3270 interface, CS/100 with asynchronous interface, and CS/200. For ports on TCP servers, all of the parameters apply except those indicated in Table 4-1.

**Table 4-1
Asynchronous and 3270 Configuration Parameter Summary**

<i>Parameter</i>	<i>Section</i>	<i>Parameter</i>	<i>Section</i>
AccessGroup *	4.1.1	GroupxPasswd *	4.1.5
AccessWord *	4.1.1	IdleTimer	4.1.3
AUDitServerAddr	4.1.5	InitMacro	4.1.1
AUToDisconnect	4.1.1	InterAction	4.1.1
AUtoLogoff	4.1.1	LFDelay **	4.1.2
BAud **	4.1.2	LFInsertion	4.1.3
BootServerAddr	4.1.5	LFPad **	4.1.2
BReakAction	4.1.3	LineERase	4.1.4
BReakChar	4.1.3	LinePRotocol **	4.1.2
BSDelay **	4.1.2	LocalEDiting	4.1.4
BSPad **	4.1.2	LocalPassWord	4.1.5
BufferSize	4.1.1	LogoffStr	4.1.5
CONNectAudit	4.1.5	LongBReakAction	4.1.3
CRDelay **	4.1.2	MaxSessions	4.1.1
CRPad **	4.1.2	MOde	4.1.3
DataBits **	4.1.2	NMPrompt	4.1.5
DataForward	4.1.3	Organization *	4.1.5
DATE	4.1.5	PARlty **	4.1.2
DefaultGateway ***	4.1.5	PermanentVC *	4.1.1
DeVice	4.1.1	PrimaryNS ***	4.1.5
DISconnectAction	4.1.3	PRlviIege	4.1.1
DOmain *	4.1.5	PROMPt	4.1.5
DUplex **	4.1.2	ReprintLine	4.1.4
ECHOData	4.1.3	SecondaryNS ***	4.1.5
ECHOMask	4.1.3	StopBits **	4.1.2
ECMChar	4.1.3	TabDelay **	4.1.2
EOM	4.1.3	TabPad **	4.1.2
ERase	4.1.4	UseDCDout **	4.1.2
ERRorAudit	4.1.5	UseDTRin **	4.1.2
FFDelay **	4.1.2	VERBatim	4.1.4
FFPad **	4.1.2	WelcomeString	4.1.5
FlowControlFrom **	4.1.3	WordERase	4.1.4
FlowControlTo **	4.1.3	XOFF	4.1.3
FlushVC	4.1.3	XON **	4.1.3
GlobalPassWord	4.1.5		

* Not applicable to TCP servers.
 ** Not applicable to an SIO-3270 interface.
 *** Applies to TCP servers only.

4.1.1 Asynchronous and 3270 Port Transmission Parameters

This section describes the asynchronous and 3270 port transmission parameters, usually set by the network manager for each port. The parameters and their permitted values are listed in Table 4-2.

Descriptions of all parameters and parameter values follow the table. If the indicated default value is the value desired, the parameter need not be set.

Table 4-2 Asynchronous and 3270 Port Transmission Parameters	
<i>Parameter</i>	<i>Permitted Values</i>
AccessGroup *	NoGroup AllGroups (1 , 2 , 3 , 4 , 5 , 6 , 7 , 8 , 9 , 10 , 11 , 12 , 13 , 14 , 15 , 16)
AccessWord *	NoGroup AllGroups (1 , 2 , 3 , 4 , 5 , 6 , 7 , 8 , 9 , 10 , 11 , 12 , 13 , 14 , 15 , 16)
AUToDisconnect	Disabled <number> (1-16000 minutes)
AUtoLogoff	[OFF ON]
BUffersize	<number> (1-512 bytes)
DeVice	(Host Terminal , Paper Glass)
InitMacro **	<string> (macro name)
InterAction	(Brief Verbose , Echo NoEcho , MacroEcho NoMacroEcho , BroadcastON BroadcastOFF , LFinsert NoLFinsert MacroBreak * NoMacroBreak *)
MaxSessions	<number> (1-8 sessions)
PermanentVC *	"" "<address>"
PRiVilege ***	User LocalNM GlobalNM
	* Not available on TCP servers.
	** Can be set only with SETDefault, not SET.
	*** Can be set only with SET, not SETDefault.

The **AccessGroup** and **AccessWord** parameters together determine which ports can make connections to which ports, as described in Section 2.3.9. When a connection is requested, the system compares the **AccessWord** of the requesting port with the **AccessGroup** of the destination port. If at least one common number appears in both sets, the connection is established.

If no common group numbers appear, the system prompts the user for a password associated with the **AccessGroup** parameter for the destination port (see Section 4.1.5). If the **AccessGroup** has more than one value, the password for any one of the values is accepted. Each of the two parameters can have the value **NoGroup**, **AllGroups**, or one or more numbers from 1 to 16. The default value for both parameters is 1.

Bridge recommends setting **AccessWord** to **NoGroup** for any port to which a dial-in modem is attached. This requires entry of the appropriate password before the user calling in can establish a connection through that modem.

The **AccessGroup** and **AccessWord** parameters are not available on TCP servers.

The **AUTOdisconnect** parameter specifies an interval after which the current session is disconnected if no activity occurs. The **AUTOdisconnect** interval can be set to disabled or to a number in the range 1 to 16000 (in minutes). Setting a value other than **Disabled** is appropriate only for host ports. The default value is 60 minutes for host ports and **Disabled** for terminal ports.

The **AUTOlogoff** parameter determines whether or not the string defined by the **LogoffStr** parameter is transmitted to the destination of a connection when the connection is broken by the **DisConnect** command or by the expiration of the **AUTOdisconnect** interval. The string is not transmitted if the disconnection is the result of a **Listen** command or if traffic to the destination port is flow controlled and the logoff string cannot be transmitted within six seconds. Setting this parameter to **ON** is appropriate only for host ports, because the logoff string usually consists of a logoff command, which causes the host to close the port in an efficient manner. The **LogoffStr** parameter is described in Section 4.1.5.

The **BUffersize** parameter specifies the size of the data buffer in bytes. It can be set to a value in the range 1 to 512. The data buffer accumulates data until the buffer becomes full, or until the interval specified by the **IdleTimer** parameter elapses; then the data is packetized and forwarded. Depending on the value of the **DataForward** parameter, data may also be forwarded when a data-forwarding character is entered. The default buffer size is 82, unless it has been modified during the system generation procedure. Normally, a CS/1 with an asynchronous or 3270 interface can have up to four ports whose **BUffersize** is set to 512; the **BUffersize** for the remaining ports must not exceed 82 for each port. A CS/100 with an asynchronous interface can have up to two ports whose **BUffersize** is set to 512; the **BUffersize** for the remaining ports must not exceed 82 for each port. A CS/200 can have up to 10 ports whose **BUffersize** is set to 512. Setting this parameter to a smaller value than the server's buffer size may be useful for PC-to-host file transfer applications.

The **DeVice** parameter specifies the local device type. One of two primary values can be specified:

Host | Terminal

Specifies whether the device is a host or a terminal.

Setting **DeVice** to **Host** automatically resets the following parameters: **BReakAction** is set to **Ignore**, **AUToDisconnect** is set to **60**, and **ECMChar** and **BReakChar** are disabled. The **InterAction** parameter is set to **Verbose** and **Echo**; **BufferSize** is set to the buffer size specified at the time of system generation.

Setting **DeVice** to **Terminal** automatically resets the following parameters: **BReakAction** is set to **EscDTM** and **InterAction** is set to **Verbose** and **Echo**. **BufferSize** is set to the buffer size specified at the time of system generation.

On a **CS/1** with an asynchronous, **3270**, bisynchronous, or bit-synchronous interface, the default **DeVice** parameter values are **Host** for ports 0 through 3 of each SIO board and **Terminal** and **Glass** for ports 4 through 7 of each SIO board. On the **CS/100** with an asynchronous or bisynchronous interface, the default values are **Terminal** and **Glass** for ports 0 through 7, and **Host** for ports 8 through 13. On the **CS/200**, the default values are **Terminal** and **Glass** for odd-numbered ports, and **Host** for even-numbered ports.

If **DeVice** is set to **Terminal**, one of the following secondary characteristics can also be specified:

Paper | Glass

Determines whether the terminal is a video display unit (**Glass**, the default) or a hard-copy printer (**Paper**). The setting affects how backspacing is handled during local editing, for instance, when the user erases a character or a word using the backspace key or the local editing characters. If **DeVice** is set to **Glass**, the server moves the terminal cursor to the left one column for each character erased. If **DeVice** is set to **Paper**, the server prints a crosshatch symbol (#) for each character erased instead of attempting to move the print mechanism.

The **InitMacro** parameter specifies the name of a port initialization macro to be executed automatically each time the device makes a transition from **Listening** mode to **Command** mode. The macro itself is defined with the **DEFine** command. Port modes are described in Section 2.3.7; the **DEFine** command is described in Section 3.2.

**** NOTE ****

This parameter cannot be used to establish a system initialization macro; a system initialization macro can be established only by defining a macro whose name begins with the letters "init" (refer to Section 3.2).

The **InterAction** parameter describes the interaction between the local device and the server. This parameter has no effect on a host port. The possible values are:

Verbose | Brief

Determines whether responses or error messages from the server to the local device are sent in their short form (Brief) or full-length form (Verbose, the default). Brief responses are "OK" if the requested action is successful, and "Err <n>" if an error is encountered. Appendix A lists all error messages and their corresponding error numbers. This pair of values also determine whether broadcast messages are preceded by a header indicating the port number of the sender of the message. The value Brief is appropriate for a host or a terminal emulator program; Verbose is appropriate for a terminal.

Echo | NoEcho

Determines whether input from the local device, while the device is in Command mode, is echoed back to the device. The default is Echo.

MacroEcho | NoMacroEcho

Determines whether or not macros are echoed on the screen as they are executed. The default is MacroEcho.

BroadcastON | BroadcastOFF

Determines whether or not the port receives messages sent with the Broadcast command when the port is in Command or Data Transfer modes. The default is BroadcastON.

LFinsert | NoLFinsert

Determines whether or not the server echoes a return and a linefeed when the user enters a command. This option is useful for terminals that perform local echo but do not generate a linefeed echo when a return is entered. The default is NoLFinsert.

MacroBreak | NoMacroBreak

Determines whether the <BREAK> key can be used to stop execution of a macro. In macros that raise the privilege level to Local or Global Network Manager, setting NoMacroBreak prevents the user from breaking out of the macro and, as a result, being left in network manager privilege level. The default is MacroBreak. The MacroBreak/NoMacroBreak option is not available on TCP servers.

The **MaxSessions** parameter specifies the maximum number of open sessions permitted on a single port. The parameter can be set to a number in the range 1 to 8. The default value is 2.

The **PermanentVC** parameter specifies a permanent virtual circuit from the current or specified port to the specified address or clearinghouse name. The default is the null string, which indicates no permanent virtual circuit. This parameter is available on host ports only; however, the destination end of the circuit may be a terminal or host port. PermanentVC may be defined on both ends of the circuit.

To disable an existing permanent virtual circuit, set the parameter equal to the null string. This removes the definition, but does not disconnect any existing connection.

The PermanentVC parameter is not available on TCP servers.

The **PRivilege** parameter specifies the privilege level of the local device. This parameter affects all sessions, not just the current or next session. Privilege is not affected if a new configuration table obtained via the **ReaD** command contains a different privilege level (Section 3.2 describes the **ReaD** command). The default value is **User**. The **PRivilege** parameter is the only parameter whose default value cannot be changed with the **SETDefault** command.

Three privilege levels are available:

User

Specifies User privilege level. User privilege permits the user to display or set characteristics for the local device port.

LocalNM

Specifies Local Network Manager privilege level. This level permits the user to set characteristics and control the status of any port on the local server and to define the setup of the local server.

GlobalNM

Represents Global Network Manager privilege level. This privilege level permits the user to set characteristics and control the status of any port on the network and to define the setup of either the local or a remote server.

4.1.2 Asynchronous Port Physical Parameters

This section describes the asynchronous port physical parameters, which are usually set by the network manager for all ports. The parameters and their possible values are summarized in Table 4-3.

Physical parameters do not apply to Communications Server ports on an SIO-3270 interface.

Table 4-3 Asynchronous Port Physical Parameters	
<i>Parameter</i>	<i>Permitted Values</i>
BAud	AutoBaud Low_AutoBaud Hi_AutoBaud 50 75 110 134.5 150 200 300 600 1200 1800 2400 3600 4800 7200 9600 19.2K 38.4K *
BSDelay/ CRDelay/ FFDelay/ LFDelay/ TabDelay	None <number> (1-127 sixtieths of a second)
BSPad/ CRPad FFPad/ LFPad/ TabPad	None <number> (1-127 nulls of padding)
DataBits	5 6 7 8
DUPlex	Half Full
LinePRotocol **	ASynchronous BYTESynchronous BITSynchronous
PARlty	None Odd Even 1 0 AutoParity
StopBits	1 1.5 2
UseDCDout **	(AlwaysAssert OnConnection , ToggleonDisc NoToggle)
UseDTRin **	Ignore AsDTR AsDCD
	* AutoBaud is available on CS/200 only. Hi_AutoBaud and Low_AutoBaud are available on CS/1 and CS/100 only. The value 38.4K is unavailable on CS/100.
	** Can be set only with SETDefault, not SET.

The **BAud** parameter specifies the local device baud rate. The default for all ports is 9600. The availability and effect of **AutoBaud**, **Low_AutoBaud**, or **Hi_AutoBaud** depends on the type of server:

- On a CS/1 port on an SIO-16 interface: When the **BAud** parameter is set to **Low_AutoBaud** or **Hi_AutoBaud**, the SIO-16 automatically selects the appropriate device baud rate from one of the numeric values listed in Table 4-3.

If the SIO-16 sets the baud rate to 300 or higher, a <RETURN> must be entered immediately after the device is powered on or reset. If it sets the baud rate to 200 or lower, the first sequence typed after the device is powered on or reset must be <RETURN><RETURN>, with no delay between the keystrokes.

- On the CS/1 (with all other interface types) and CS/100: When the **BAud** parameter is set to **Hi_AutoBaud**, the server automatically selects the appropriate device baud rate of 2400, 4800, or 9600. If the **BAud** parameter is set to **Low_AutoBaud**, the server automatically selects the appropriate device baud rate of 300 or 1200.

If either **Hi_AutoBaud** or **Low_AutoBaud** is selected, a <RETURN> must be the first character entered after the device is powered on or reset.

- On the CS/200: When the **BAud** parameter is set to **AutoBaud**, the server automatically selects the appropriate device baud rate from one of the numeric values listed in Table 4-3.

If **AutoBaud** sets the server's baud rate to 300 or higher, a <RETURN> must be entered immediately after the device is powered on or reset. If **AutoBaud** sets the server's baud rate to 200 or lower, the first sequence typed after the device is powered on or reset must be <RETURN><RETURN>, with no delay between the keystrokes.

The **xxDelay** parameters specify the length of the delay (in sixtieths of a second) following the echo or transmission of the specified character before the server echoes or transmits another character. The default value is None (i.e., no delay). This parameter is designed for use with terminals with a moving print-head mechanism. The delay allows the mechanism to complete its motion before subsequent characters are received.

The **xxPad** parameters specify the number of nulls the server inserts between the specified character and the next character. The default value is None (i.e., no nulls inserted). These parameters are alternate forms of the **xxDelay** parameters.

The **DataBits** parameter specifies the number of databits per byte. The value can be set to 5, 6, 7, or 8. The default is 8 for all host ports, for one of the terminal ports on the CS/100, and for one of the terminal ports on each CS/1 SIO board. With **DataBits** set to 8, **PARItY** should be set to None, Odd, or Even; 0 and 1 are meaningless. The default for most terminal ports is 7.

The **DUPlex** parameter specifies whether the local device transmits and receives in half-duplex mode or full-duplex mode. The default value is Full; half-duplex mode is not currently implemented.

The **LineProtocol** parameter specifies the type of line protocol used by the port. For ports attached to the asynchronous interface of a CS/1 or CS/100, any value other than **ASynchronous** is illegal. The server automatically sets the value based on the SIO firmware present on the board.

The **PARity** parameter specifies the local device parity. The possible values are None, Odd, Even, 1 (mark), 0 (space), or AutoParity.

- On the CS/1 and CS/100, the default value is None for host ports (ports 0 through 3 on each asynchronous CS/1 SIO board and ports 8 and 9 on the CS/100 with an asynchronous interface).

The default value varies for each terminal port.

The value AutoParity is valid only if the BAud parameter is set to Lo_AutoBaud or Hi_AutoBaud. If AutoParity is in effect, the first sequence entered after the device is powered on or reset must be <RETURN>.<RETURN>.

- On the CS/200, the default value is Even for ports 0 and 1, mark for ports 4 and 5, Odd for ports 6 and 7, and None for ports 2, 3, 8, and 9. (Ports 0, 2, 4, 6, and 8 are host ports; ports 1, 3, 5, 7, and 9 are terminal ports.)

The value AutoParity is valid only if the BAud parameter is set to AutoBaud. If the baud rate is set to 300 or higher, the first sequence entered after the device is powered on or reset must be <RETURN>.<RETURN>. If the baud rate is set to 200 or lower, the first sequence entered after the device is powered on or reset must be <RETURN><RETURN>.<RETURN>, with no delay between the first two keystrokes.

The **StopBits** parameter specifies the number of stopbits per byte. The value can be set to 1, 1.5, or 2. The default is 1.

The **UseDCDout** parameter specifies how the server supplies the Data Carrier Detect (DCD) signal to the attached device. This option is supported on all ports of a CS/1 with asynchronous interface, CS/100 with asynchronous interface, CS/200, and IVECS. Only some ports on other Communications Server types support this option. Refer to the appropriate *Installation Guide* for mapping between DCD, DTR, and the EIA connector pins. One each of two sets of parameter values can be specified:

AlwaysAssert | OnConnection

Determines when the DCD output signal is asserted.

AlwaysAssert causes the DCD output signal to be asserted at all times.

OnConnection causes the DCD output signal to be deasserted at all times as long as no connection is established to the device and asserted when a connection is made.

ToggleonDisc | NoToggle

Determines whether or not the DCD output signal toggles when a connection is broken.

ToggleonDisc causes the DCD output signal to be deasserted for at least 65 milliseconds within 150 microseconds after disconnection. Depending on the other UseDCDout parameter setting, the signal then either remains deasserted or returns to asserted. This value is used when the server is connected to certain data switch devices.

NoToggle suppresses the toggle upon disconnection. The signal either stays asserted or changes cleanly to deasserted, depending on the other UseDCDout parameter setting.

The default value of UseDCDout is AlwaysAssert, NoToggle for all terminal ports and OnConnection, NoToggle for all host ports. The interaction between these sets of values is illustrated in Figure 4-2; Table 4-7 lists recommended settings of the UseDCDout parameter for use with various devices (both figure and table are in Section 4.1.8).

The **UseDTRin** parameter specifies the server's response to the value of the Data Terminal Ready (DTR) input signal received from the attached device. This option is supported on all ports of a CS/1 with asynchronous interface, CS/100 with asynchronous interface, CS/200, and IVECS. Only some ports on other CS/1 types support this option; refer to the appropriate *Installation Guide* for mapping between DCD, DTR, and the EIA connector pins. One of three parameter values can be specified:

Ignore

Specifies that the server does not check the state of the DTR or DSR input signal when a connection is made and takes no action when the signal changes value.

This value should never be specified if the FlowControlTo and FlowControlFrom parameters are set to CTS_RTS (refer to Section 4.1.3).

When the FlowControlFrom/To parameters are set to CTS_RTS, the SIO firmware uses DTR to enable and disable the SIO receiver; the UseDTRin parameter must not be set to Ignore or the SIO receiver is never enabled, and the port appears to hang. If the application requires that the DTR signal be ignored, the customer must build a special cable that holds the DTR signal high.

This value is the default for terminal ports.

AsDTR

Specifies that the server checks the state of the DTR input signal before establishing a connection to a port. If the DTR input is deasserted, the server rejects any connection requests to the port. If the DTR input changes from asserted to deasserted, all connections to the port are terminated and the port enters Listening mode. If the device is a terminal and the input signal changes from deasserted to asserted, a Connection Service process is started for the port (i.e., the WelcomeString is transmitted to the terminal and the InitMacro, if any, is executed).

This value is the default for host ports.

AsDCD

Specifies that the Communications Server does not reject a connection request to the port based on the value of the DTR input. However, if the DTR input changes from asserted to deasserted, all connections to the port are terminated and the port enters Listening mode. If the device is a terminal and the input signal is changed from deasserted to asserted, a Connection Service process is started for the port.

4.1.3 Asynchronous and 3270 Session Transmission Parameters

Table 4-4 lists the session transmission parameters. A description of each parameter, an explanation of each possible value, and an indication of the default follows the table. If the default is acceptable, the parameter does not have to be set.

These parameters can be set with either SET or SETDefault unless otherwise indicated in the table.

Table 4-4 Asynchronous and 3270 Session Transmission Parameters	
<i>Parameter</i>	<i>Permitted Values</i>
BReakAction	IGnore (OutofBand , FlushVC , InBand , EscDTM)
BReakChar	Disabled <char>
DataForward	None (AlphaNum , CR , ESC , EDiting , Term , FormEf , COnTrol , Punct)
DisconnectAction	None SendLongBreak
ECHOData	OFF ON
ECHOMask	None (AlphaNum , CR , ESC , EDiting , Term , FormEf , COnTrol , Punct)
ECMChar	Disabled <char>
EOM	Disabled <char>
* FlowControlFrom/ * FlowControlTo	None CTS_RTS XON_XOFF ENQ_ACK
** FlushVC	OFF ON
IdleTimer	Disabled <number> (1-255 sixtieths of a second)
LFInsertion	None (OutputCrlf , EchoCrlf)
LongBReakAction	IGnore (Listen , OutofBand , InBand)
MOde	Transparent Scroll
* XOFF	Disabled <char>
* XON	Disabled <char>
	* Not applicable to servers with an SIO-3270 interface.
	** Can be set only with SET, not SETDefault.

The **BReakAction** parameter specifies the action taken by the server when a break (or the alternative character specified by the **BReakChar** parameter) is detected. The value **IGnore** is mutually exclusive with any other value; more than one of the remaining values can be specified. The default value is **InBand** for terminal ports and **IGnore** for host ports. There are five possible values:

IGnore

Specifies no action.

OutofBand

Specifies that an out-of-band break is transmitted to the remote device.

FlushVC

Specifies that all packets for this session currently in the circuit are flushed when a break is detected.

For servers running XNS protocols, this value implements X.3 parameter 7 and operates in conjunction with the **FlushVC** parameter (X.3 parameter 8). This value must not be specified unless the destination host supports X.3 parameters 7 and 8 or equivalent functions.

For servers running TCP protocols, this parameter uses the Telnet **DO TIMING** option. This value must not be specified if the remote host does not respond to a **DO TIMING** command. Either a negative or a positive response is acceptable, but no response at all makes the port appear to hang.

Refer to the **FlushVC** parameter in this section for a description of how this **BReakAction** value operates, and to Section 4.2.6 for a discussion of the X.3 parameters.

InBand

Specifies that an in-band break is transmitted to the remote device (default).

EscDTM

Specifies that the user port will change from Data Transfer mode to Command mode.

The **BReakChar** parameter specifies the character that is interpreted by the server as a break signal. This parameter is useful for terminals that do not have a break key. Since most terminals have a break key, the default is **Disabled**.

The **DataForward** parameter specifies the events that cause data to be packetized and forwarded in Data Transfer mode. Some events are predetermined **DataForward** conditions; these include the elapsing of the **IdleTimer** (if enabled), the End of Message (EOM) signal, and the **ATTN** or break signal. One or more of the events listed below can also be specified. The default **DataForward** value is **None**, which is mutually exclusive with any other value.

None

Specifies that data is forwarded if the data buffer (size specified by the **BufferSize** parameter) becomes full or the **IdleTimer** elapses (if set). This is the default value.

AlphaNum

Specifies that a packet is created and forwarded as soon as any upper- or lowercase alphabetic character or numeric character is detected.

CR

Specifies that a packet is created and forwarded as soon as a return is detected.

ESC

Specifies that a packet is created and forwarded as soon as an escape (ESC, BEL, ENQ, or ACK) signal is detected.

EDiting

Specifies that a packet is created and forwarded as soon as any editing character is detected. Alternative editing characters can be specified; Section 4.1.4 lists the characters and their default values.

Term

Specifies that a packet is created and forwarded as soon as any terminator (ETX or EOT signal) is detected.

FormEf

Specifies that a packet is created and forwarded as soon as any "Form Effector" character is detected. Form Effectors are the linefeed, tab, and formfeed characters.

COntrol

Specifies that a packet is created and forwarded as soon as any control character is detected.

Punct

Specifies that a packet is created and forwarded as soon as any "punctuation" character is detected (includes all the nonalphanumeric "graphics" characters, i.e., ! @ # \$ % ^ & * () _ - + = ~ ' | \ [] { } : ; " ' < > , . ? / and space).

The **DisconnectAction** parameter specifies the action taken by the server when a session is disconnected. This parameter applies only to host ports, and only to hosts that distinguish between the break signal (approximately 150 milliseconds) and the long break signal (approximately 3 seconds). There are two possible values:

None

Specifies that no long break is sent on disconnection (default).

SendLongBreak

Specifies that the server sends a long break to the host when a session is disconnected.

The **ECHOData** parameter specifies whether or not the server will echo input data back to the device while the device is in Data Transfer mode. The default value is OFF.

The **ECHOMask** parameter specifies which characters are echoed if ECHOData is enabled. The character classes are the same as those listed for the DataForward parameter. If ECHOData is enabled, then all characters that fit the ECHOMask descriptions are echoed when typed. The default ECHOMask values are AlphaNum, CR, Term, and Punct.

The **ECMChar** parameter specifies a character that is interpreted by the server as a request to change from Data Transfer mode to Command mode. The default value is "^" (representing the character <CTRL-caret>). The defined character cannot be transmitted as data. This parameter is used only if the application requires that a break signal be transmitted as data (i.e., the **BreakAction** parameter is set to **InBand** or **OutofBand**).

**** NOTE ****

The **ECMChar** does not change from Data Transfer mode to Command mode if the **IdleTimer** parameter is set to **Disabled** and the **DataForward** parameter is set to **None**.

The **EOM** parameter specifies a character to represent the local End of Message (EOM) signal. When the parameter is set to **Disabled** (the default), every packet that is transmitted is terminated with an EOM signal; in this case, the **EOM** parameter for the destination port should be set to the same value.

The **FlowControlFrom** and **FlowControlTo** parameters specify the flow control mechanism from the server to the local device (i.e., the server can turn transmission from the local device on or off) and from the local device to the server (i.e., the local device can turn transmission from the server on or off), respectively. For all ports, the default value of both **FlowControlFrom** and **FlowControlTo** is **XON_XOFF**.

These parameters govern local flow control (i.e., between the local device and the local server). The remote device can use different flow control than the local device, since flow control across the network is handled by the servers at either end of the circuit independently of local flow control. Permitted values are:

None

Specifies that no flow control is used.

CTS_RTS

Specifies that the hardware control lines CTS and RTS are used. Refer to the appropriate *Installation Guide* for the mapping between these lines and EIA connector pins, and to Section 4.1.2 for a description of the **UseDTRin** parameter. This value must not be selected if **UseDTRin** is set to **Ignore**. This value is not valid on an SIO-16.

When the **FlowControlFrom/To** parameters are set to **CTS_RTS**, the SIO firmware uses DTR to enable and disable the SIO receiver; the **UseDTRin** parameter must not be set to **Ignore** or the SIO receiver is never enabled, and the port appears to hang. If the application requires that the DTR signal be ignored, the customer must build a special cable that holds the DTR signal high.

XON_XOFF

Specifies that the characters defined by the **XON** (transmit on) and **XOFF** (transmit off) parameters are used.

ENQ_ACK

Specifies that the **ENQ/ACK** flow control protocol is used. If this value is set, the server sends the device an **ENQ** message before sending a block of data, and sends the data only if the device responds with an **ACK** message indicating it is ready to receive data.

The `FlowControlFrom` and `FlowControlTo` parameters do not apply to Communications Server ports on an SIO-3270 interface.

The **FlushVC** parameter applies only if the `BReakAction` parameter is set to `FlushVC`, and specifies whether packets for a session are being flushed (discarded) or transmitted.

This parameter is not used by TCP servers.

There are two possible values:

OFF

Specifies that packet flushing is disabled (default).

ON

Specifies that packet flushing is enabled. If the `BReakAction` parameter is set to `FlushVC` and a break is detected, the local server forwards the break signal to the remote server and enables packet flushing. The remote server then forwards the break to the host. If the host supports X.3 parameters 7 and 8 (or a comparable function) the host sends a request to the local server to reset the `FlushVC` parameter to `OFF`. If the host does not support X.3 parameters 7 and 8, the user must not set the `BReakAction` parameter to `FlushVC`, because the host will be unable to disable packet flushing and no packets will be transmitted in either direction following a break signal.

The **IdleTimer** parameter specifies the interval after which, if no further characters are input from the local device, all accumulated characters are packetized and forwarded. In Data Transfer mode, characters are accumulated in a data buffer until an event specified by the `DataForward` parameter occurs, the buffer fills, or the `IdleTimer` interval elapses. `IdleTimer` can be set to `Disabled` or to a number in the range 1 to 255 (sixtieths of a second).

The default value for host ports is 1, which is appropriate for line speeds of 9600 baud or greater. The default value for terminal ports is 2. Since characters take longer to be transmitted from the device to the server at lower line speeds, the `IdleTimer` parameter should be adjusted to an interval greater than or equal to the time needed for a single character to be transmitted (e.g., set `IdleTimer` to 2 for 4800 baud lines, and to 4 for 1200 baud lines). This reduces packet overhead and improves system performance.

The **LFInsertion** parameter specifies whether linefeeds are transmitted (or echoed) following a return (or an EOM signal if `EOM` is set to `CR`). The default value is `None`. The parameter accepts three values:

None

Specifies that no linefeed is echoed or transmitted with the return after an EOM signal. This value is mutually exclusive with the other values.

OutputCrlf

Specifies that if an EOM signal is received from the remote device, a return and a linefeed are sent to the device.

EchoCrlf

Specifies that if a return is received from the local device, a return and a linefeed are echoed to the device.

The **LongBreakAction** parameter specifies the action taken by the server when a long break is detected. This parameter applies only to terminal ports. For servers running the TCP protocols, LongBreakAction operates only if the source and destination are on the same server; for connections across the network, LongBreakAction has essentially the same effect as BReakAction. The value Ignore is mutually exclusive with any other value; more than one of the remaining values can be specified. The default value is Ignore for both terminal and host ports. There are four possible values:

Ignore

Specifies no action (default).

Listen

Specifies that the port is placed in Listening mode and all sessions for the port are disconnected.

OutofBand

Specifies that the long break signal is transmitted out-of-band to the remote device.

InBand

Specifies that the long break signal is transmitted in-band to the remote device.

The **MOde** parameter specifies one of two Data Transfer modes:

Transparent

Specifies that the local device is a screen-oriented intelligent terminal whose display format is controlled by an application. Local editing and local echo are disabled. Except for the characters defined by the ECMChar and BReakChar parameters, all input from the terminal in Data Transfer mode is transmitted exactly as is; no translation is provided. This is the default value.

Setting MOde to Transparent automatically resets the following parameters: ECHOData is set to OFF, LFInsertion is set to None, DataForward is set to None, IdleTimer is set to 1, and BReakAction is set to InBand.

Scroll

Specifies that the local device is a line-oriented TTY-type terminal or application. Local editing and local echo are enabled.

Setting MOde to Scroll automatically resets the following parameters: ECHOData is set to ON; LFInsertion is set to EchoCrLf and OutputCrLf; DataForward is set to CR, ESC, EDiting, and COntrl; and IdleTimer is set to Disabled.

The **XOFF** and **XON** parameters specify characters that are recognized by the server as XOFF/XON flow control characters. The default XOFF character is <CTRL-S>; the default XON character is <CTRL-Q>.

For ports on an SIO-3270 interface, the XON parameter does not apply and the XOFF parameter has a non-standard meaning. Setting XOFF to the value ^S specifies that the port is in the default terminal emulation mode; the value d specifies VT100 emulation mode; the value i specifies extended VT100 emulation mode.

4.1.4 Session Editing Parameters

Table 4-5 summarizes the editing parameters, which can be used in Command mode and during sessions in which the MODE parameter is set to Scroll. A description of each parameter, an explanation of the possible values, and an indication of the default follows the table. If the default value is acceptable, the parameter does not have to be set.

These parameters can be set either with SET or SETDefault.

Table 4-5 Editing Parameters	
<i>Parameter</i>	<i>Permitted Values</i>
ERase	Disabled <char>
LineERase	Disabled <char>
LocalEDiting	(NoDataEditing DataEditing , NoCmdEditing CmdEditing)
ReprintLine	Disabled <char>
VERBatim	Disabled <char>
WordERase	Disabled <char>

The **ERase** parameter specifies the character (default <CTRL-H>) that the server interprets as an ERase character. Entered before the current line is terminated by the return key, the ERase character deletes the most recently typed character. On most terminals, the backspace key also performs the ERase function.

The **LineERase** parameter specifies the character (default <CTRL-U>) that the server interprets as a LineERase character. Entered before the current line is terminated by the return key, the LineERase character deletes the entire line.

The **LocalEDiting** parameter specifies whether local editing is permitted. The default value enables local editing in Command mode but not in Data Transfer mode. One each of two pairs of values can be specified:

NoDataEditing | DataEditing

Disables (the default) or enables local editing in Data Transfer mode during a session in which the MODE parameter is set to Scroll.

NoCmdEditing | CmdEditing

Disables or enables (the default) local editing in Command mode.

The **ReprintLine** parameter specifies the character (default <CTRL-R>) that the server interprets as a ReprintLine character. This character is used to reprint all pending input on the current line before the line is terminated by the return key.

The **VERBatim** parameter specifies the character (default <CTRL-V>) that the server interprets as a VERBatim character. The VERBatim character causes the next character entered to be used verbatim rather than interpreted by the server as a special character. The VERBatim character has no effect if the next character entered is a return or the VERBatim character itself.

The **WordERase** parameter specifies the character (default <CTRL-W>) that the server interprets as a WordERase character. Entered before the current line is terminated by the return key, the WordERase character deletes the most recent word typed.

4.1.5 Global Parameters

Table 4-6 lists the configuration parameters that determine the welcome message, date, prompts, passwords, and NCS audit trail functions. For TCP servers, these parameters also determine the addresses of the Name Servers and Default Gateway. Each of these parameters affects the entire server, not just the current port or session. All of the global parameters except DATE and BootServerAddr must be specified with the SETDefault command, not the SET command.

Table 4-6 Global Parameters	
<i>Parameter</i>	<i>Permitted Values</i>
AuditServerAddr	<address>
BootServerAddr *	<address>
CONNECTAudit	OFF ON
DATE	<yy/mm/dd hh:mm[:ss]> <mm/dd/yy hh:mm[:ss]>
DefaultGateway **	<physical-address>
Domain ***	<string>
ERRorAudit	OFF ON
GlobalPassWord	<string>
GroupxPasswd ****	<string>
LocalPassWord	<string>
LogoffStr ****	<string>
NMPrompt	<string>
Organization ***	<string>
PrimaryNS **	<physical-address>
PROMPt	<string>
SecondaryNS **	<physical-address>
WelcomeString	<string>
*	Can be set with SET only, not SETDefault.
**	Applies to TCP servers only.
***	Not applicable to TCP servers; on a diskless server, can be set with SET only.
****	Not applicable to TCP servers.

The **AUDITServerAddr** parameter specifies the address of the NCS to which the local server sends audit trail data. This parameter is used only to send the local server's audit trail to an NCS other than the one to which the server is bound or to send an unbound server's audit trail to an NCS. Each *NCS Installation and Operation Guide* describes the NCS audit trail.

The **BOOTServerAddr** parameter, valid only on servers booted from an NCS, specifies the address of the NCS from which the local server boots. This parameter is used only to override the NCS to which the server is bound (e.g., if the server's primary and secondary NCSs are down, and another NCS can enable the server to function on a temporary basis). Each *NCS Installation and Operation Guide* describes this facility.

The **CONNECTAudit** parameter, valid only on servers bound to an NCS, disables (OFF) or enables (ON) generation of connection-related audit trail statistics by the server. If this parameter is set to ON, the audit trail data is sent to the NCS to which the server is bound or to the NCS specified by the **AUDITServerAddr** parameter (if any is specified). Each *NCS Installation and Operation Guide* describes the NCS audit trail.

The **DATE** parameter is used to set the system clock. The value can be entered in either of the two formats shown in Table 4-6. Times are entered in 24-hour-clock time. The clock is used by the network management reports and should be set after each system boot, unless there is an NCS in the network. Unusually frequent disk activity may cause the clock to drift by a few seconds per year.

The **DefaultGateway** parameter applies to TCP servers only. When a server must communicate with a destination server that has a different network number, the source server looks up which Gateway Server provides access to the other network. If the source server has no record of a Gateway Server that can provide access to the other network, it sends its request to the default Gateway Server. This parameter specifies the address of the default Gateway Server.

The **DefaultGateway** parameter is 0, which specifies use of ARP-based routing for internet-work traffic.

The **DOMAIN** and **Organization** parameters specify the default domain and organization fields for all clearinghouse names entered on the server. These defaults are automatically appended to the local name unless overridden when the name is entered. The default value of these parameters is the null string ("").

An NCS and the servers that it supports normally have the same default domain and organization strings. The network manager can use the SET command on a diskless server to override the defaults, but the new values remain in effect only until the next boot, at which time the server reverts to the defaults established for the NCS. These parameters are not valid on TCP servers.

The **ERRORAudit** parameter disables (OFF) or enables (ON) generation of error-related audit trail data by the server. If this parameter is set to ON, the error statistics are sent to the NCS to which the server is bound or to the NCS specified by the **AUDITServerAddr** parameter (if any is specified). Each *NCS Installation and Operation Guide* describes the NCS audit trail.

The **GlobalPassword** parameter specifies the password (maximum 14 characters) that the user must type when setting the privilege level to Global Network Manager. The default value is null (""). On a server supported by an NCS, the password must be established remotely on the NCS.

The **GroupxPasswd** parameter specifies the password (maximum 14 characters) that a user must enter in order to establish a connection with any device on the local Communications Server when the user's AccessWord values do not match any of the device's AccessGroup values. Each AccessGroup can have its own password. This system is designed to limit access within the network for security purposes, as described in Section 2.3.10. Only a Global Network Manager can set or change AccessGroups, AccessWords, or GroupxPasswds. The default password for all AccessGroups is null (""). On a server supported by an NCS, the passwords must be established remotely on the NCS. The GroupxPasswd parameters are not valid on TCP servers.

The **LocalPassWord** parameter specifies the password (maximum 14 characters) that the user must type when setting the privilege level to Local Network Manager. The default value is null ("").

The **LogoffStr** parameter specifies the string to be transmitted to the host when a connection is broken by the DisConnect command or by the expiration of the AUtoDisconnect interval. The string is transmitted to the host port before the port closes the circuit. The string usually consists of a logoff command, which causes the host to close the port in an efficient manner. The string may be no more than 24 characters long. The AUtoLogoff parameter, described in Section 4.1.1, must be set ON for this string to be transmitted. The LogoffStr parameter is not available on TCP servers.

The **NMPrompt** parameter specifies the string (maximum 14 characters) that the server prints on the local device (starting in column 1) to indicate Command mode if the port has Local or Global Network Manager privilege. The default prompt for all servers consists of the server model in lowercase followed by a crosshatch symbol (#) and a space. For example, on the CS/1, the default prompt is "cs/1# ".

The **PrimaryNS** parameter, which applies to TCP servers only, specifies the address of the server's primary Name Server. All internet name requests are sent first to the server specified by this parameter.

The **PROMPT** parameter specifies the string (maximum 14 characters) that the server prints on the local device (starting in column 1) to indicate Command mode if the port has User privilege. The default prompt for all servers consists of the server model followed by a right angle bracket (>) and a space. For example, on the CS/1, the default prompt is "CS/1> ".

The **SecondaryNS** parameter, which applies to TCP servers only, specifies the address of the server's primary Name Server. The server sends all internet name requests to the server specified by this parameter if it gets no response from the primary Name Server.

The **WelcomeString** parameter specifies the string printed on the local device by the Communications Server when the device or the server is powered on or reset. The maximum length of the string is 80 characters. For Communications Servers, the default string is "^M^J Welcome to your Communications Server ^M^J".

Section 3.1.5 describes the conventions for entering string text.

4.1.6 Asynchronous Host Configuration

This section describes the procedure for configuring an asynchronous port as a host port.

**** NOTE ****

This information does not apply to the virtual ports on a CS/1-HSM, CS/1-SNA, or CS/1-X.25, or IVECS. Refer to the *Network Management Guide* for information on configuring the virtual ports on these systems.

On a new unit, some ports are configured for terminal device connections; the following parameters are in effect:

```
device=terminal
mode=transparent
```

The default configuration specifies ports 0 through 3 on each asynchronous CS/1 SIO board, ports 8 and 9 on the asynchronous CS/100, and ports 0, 2, 4, 6, and 8 on the CS/200 as host ports. The network manager can configure additional ports as host interface ports by respecifying the DeVice parameter. For example, to convert port 7 into a host port, the network manager types the following command from any terminal port other than port 7:

```
setdefault (!7) device=host
```

Section 3.2 describes the SETDefault command. Sections 4.1.1 and 4.2.1 describe the DeVice parameter.

Setting DeVice equal to Host disables ECMChar and BReakChar; sets InterAction to Brief, NoEcho, NoMacroEcho, and BroadcastOFF; sets BReakAction to Ignore; sets AUToDisconnect to 60 minutes; and sets BUffersize to the default small buffer size (typically 82 bytes).

4.1.7 Asynchronous Terminal Configuration

The specific configuration appropriate for an asynchronous terminal device depends on the type of device and on the application being run. This section describes some of the configuration parameters and commands that frequently cause confusion.

- Port physical parameters specified with the SETDefault command do not take effect until a Listen command is issued to the port. Existing sessions are not affected. Session parameters go into effect with the next new session. The parameters then remain in effect until overridden explicitly via another SETDefault or SET command or implicitly via the setting of another configuration parameter.
- The SETDefault command performs an automatic save on the diskette, thus changing the configuration table that is read from the diskette when the system is booted.
- Parameters specified with the SET command take effect immediately and remain in effect until overridden explicitly via another SET command or until the session is terminated. When an additional session is opened while the first connection is still intact, the server copies a new session parameter table from the default configuration table, not from the current session table.

After multiple sessions are opened, the session parameters for each session can be altered without affecting the parameters of the other sessions.

- The `AccessGroup`, `AccessWord`, `BReakAction`, `ECHOMask`, `LFInsertion`, and `DataForward` parameters accept one or more of a set of values. When new values are set, they are added to the existing list, but values already in the list are not deleted. To remove a value from the list, first set the parameter equal to `NoGroup` (for `AccessGroup` and `AccessWord`), `IGnore` (for `BReakAction`), or `None` (for `ECHOMask`, `LFInsertion`, and `DataForward`). Then set any desired values.
- The `BReakAction` parameter values `OutofBand` and `InBand` are often confused. The difference between the two values is whether or not the break affects the characters that were transmitted just ahead of it and have not yet reached the other end of the circuit. An `OutofBand` break causes the characters ahead of it in the circuit to be garbled and discarded. An `InBand` break, however, remains in the queue of characters in the circuit, and characters ahead of the break reach the other end of the circuit before the break.
- Setting `BReakAction` to both `InBand` and `EscDTM` has one side effect. If the user has established a connection to a host and then presses the break key or enters the `BReakChar` (if one is set), the break is sent in-band to the host and is also intercepted by the server as a request to change to Command mode.

The Connection Service sends a server prompt to the terminal, and the host sends a host prompt to the terminal. The host prompt, however, is not displayed on the terminal until the user enters a `RESume` command and returns to Data Transfer mode. This can be avoided by changing `BReakAction` to `EscDTM` only. The parameter must be set first to `IGnore`, then to `EscDTM`. For example:

```
set mode=transparent breakact=ignore breakact=escdtm
```

- If a port is in Command mode, and a `Connect`, `DEFine`, `DO`, `Pause`, or `SHow` request is in progress, the request can be aborted with the break key or `BReakChar`. This terminates the request even if the `BReakAction` parameter is set to `IGnore`.
- A connection from one device to another cannot be established unless the destination device port is in Listening mode. If the destination port is in Command mode or Data Transfer mode, either a user at the terminal or a network manager at a remote terminal can convert the port to Listening mode with the `Listen` command. Section 2.3.4 describes the modes of operation. Section 3.2.8 describes the `Listen` command.
- Setting the `MOde` parameter to `Transparent` is desirable for many applications (e.g., screen editors) but has some side effects. Setting `MOde` to `Transparent` automatically sets `BReakAction` to `InBand` only, `IdleTimer` to 1, `ECHOData` to `OFF`, `LFInsertion` to `None`, and `DataForward` to `None`. With `BReakAction` set to `InBand` only, the user cannot return from Data Transfer mode to Command mode using the break key or the `BReakChar` (if one is set), since neither break signal is intercepted by the server. Therefore, when setting `MOde` to `Transparent`, either set `BReakAction` to `EscDTM` before going into Data Transfer mode or ensure that an `ECMChar` is set. The default `ECMChar` is `<CTRL-^>`.
- The `LinePProtocol` parameter can be displayed but not set for asynchronous terminal ports. This parameter is settable only on character-synchronous and bit-synchronous ports; it determines which of these protocols the port uses.

- If the network manager specifies values for the PARity and DataBits parameters that are inappropriate for the device (e.g., setting DataBits to 8 and PARity to 0 or 1), the port may appear to hang. To recover from this condition, the network manager must use the SETDefault command remotely to establish appropriate values and then use the Listen command remotely to reinitialize the port.
- The LongBReakAction parameter takes advantage of some terminals' ability to generate both a normal break signal (approximately 150 milliseconds) and a long break signal (at least 3 seconds). Long breaks are usually generated by pressing both shift and break keys simultaneously. For terminals that can generate a long break signal but cannot toggle the DTR signal, setting the LongBReakAction parameter to Listen permits long breaks to simulate the toggling of DTR (thus placing the port in Listening mode).

4.1.8 Asynchronous Modem Control Lines

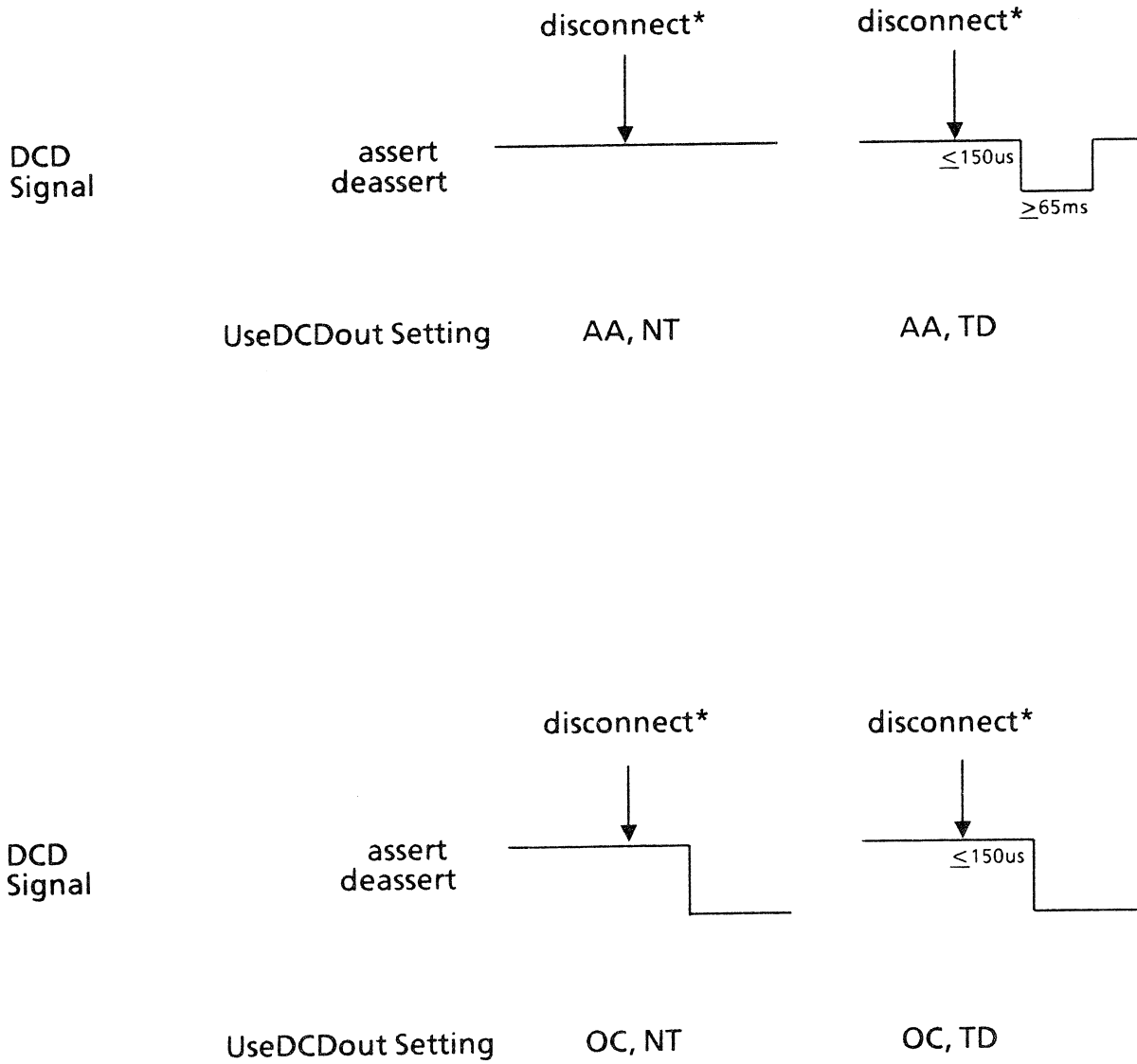
Table 4-7 describes the interaction between the hardware modem control lines DTR and DCD and the software configuration parameters UseDTRin and UseDCDout. The information covers terminal ports, host ports, and modem ports, since these lines can be used by devices other than modems. Section 4.1.2 describes the UseDTRin and UseDCDout parameters.

Some modems expect a toggle in the DCD signal at disconnect. Figure 4-2 illustrates the effect of different UseDCDout parameter settings on the DCD signal at disconnect. Table 4-7 includes separate entries for modems that expect the toggle and modems that do not expect the toggle.

The support of modem control lines can also be affected by the cable used to connect the device to the server. Refer to the appropriate *Installation Guide* for cable information.

The parameter UseDCDout controls the Data Carrier Detect signal to the modem from the server. The signal from the modem is usually called DTR. Most originate modems will not go offhook (unless this signal is deasserted) and most answer modems will not answer a ringing line unless this signal is asserted.

The parameter UseDTRin refers to the Data Terminal Ready signal from the modem to the server. This signal from the modem is usually labeled DSR.



* The disconnect can come from either end of the session; it can be the dropping of DTR if the UseDTRin parameter is set to anything other than Ignore.

Figure 4-2 Effect of UseDCDout Parameter Settings

Table 4-7 Recommended Settings of UseDCDout and UseDTRin		
<i>Device Type</i>	<i>UseDCDout Setting</i>	<i>UseDTRin Setting</i>
Terminal without DTR and DCD lines	Don't care	Ignore
Terminal with DTR and DCD lines	AlwaysAssert NoToggle	AsDTR
Host without DTR and DCD lines	Don't care	Ignore
Host with DTR and DCD lines	OnConnection NoToggle	AsDTR
Dial-in modem without unattended disconnect	AlwaysAssert NoToggle	AsDTR
Dial-out modem without unattended disconnect	OnConnection NoToggle	AsDCD
Dial-in modem with unattended disconnect	AlwaysAssert ToggleonDisc	AsDTR
Dial-out modem with unattended disconnect	OnConnection ToggleonDisc	AsDCD

4.2 GS/1 Virtual Port Configuration Parameters

This section describes the configuration parameters that apply to GS/1 virtual ports and to the server as a whole.

Table 4-8 lists all virtual port parameters for the GS/1 alphabetically and gives the section number of each parameter description. Uppercase characters represent the minimum unambiguous abbreviation of each parameter. The possible values of each parameter, and the effects of the possible values, are described in the following subsections.

Table 4-8 GS/1 Configuration Parameter Summary			
<i>Parameter</i>	<i>Section</i>	<i>Parameter</i>	<i>Section</i>
AccessGroup	4.2.1	GroupxPasswd	4.2.5
AccessWord	4.2.1	IdleTimer	4.2.3
AUtoDisconnect	4.2.1	InitMacro	4.2.1
BReakAction	4.2.3	InterAction	4.2.1
BReakChar	4.2.3	LFInsertion	4.2.3
CRPad	4.2.2	LineERase	4.2.4
DataBits	4.2.2	LocalEDiting	4.2.4
DataForward	4.2.3	LocalPassWord	4.2.5
DATE	4.2.5	MaxSessions	4.2.1
DeVice	4.2.1	MOde	4.2.3
DOmain	4.2.5	NMPrompt	4.2.5
ECHOData	4.2.3	Organization	4.2.5
ECMChar	4.2.3	PRiilege	4.2.1
EOM	4.2.3	PROMPt	4.2.5
ERase	4.2.4	ReprintLine	4.2.4
FlowControlFrom	4.2.3	VERBatim	4.2.4
FlowControlTo	4.2.3	WelcomeString	4.2.5
GlobalPassWord	4.2.5	WordERase	4.2.4

4.2.1 GS/1 Port Transmission Parameters

This section describes the GS/1 port transmission parameters usually set by the Network Manager for each port. The parameters and their permitted values are listed in Table 4-9.

Definitions of the parameters, explanations of each possible value, and an indication of the default follow the table. If the default is acceptable, the parameter need not be set.

Table 4-9 GS/1 Port Transmission Parameters	
<i>Parameter</i>	<i>Permitted Values</i>
AccessGroup	NoGroup AllGroups (1 , 2 , 3 , 4 , 5 , 6 , 7 , 8 , 9 , 10 , 11 , 12 , 13 , 14 , 15 , 16)
AccessWord	NoGroup AllGroups (1 , 2 , 3 , 4 , 5 , 6 , 7 , 8 , 9 , 10 , 11 , 12 , 13 , 14 , 15 , 16)
Autodisconnect	Disabled <number> (1-16000 minutes)
DeVice	(Host Terminal , Paper Glass)
InitMacro *	<macro-name>
InterAction	(Verbose Brief , Echo NoEcho , MacroEcho NoMacroEcho , BroadcastON BroadcastOFF , LFinsert NoLFinsert) MacroBreak NoMacroBreak)
MaxSessions	<number> (1-8 sessions)
PRiVilege **	User LocalNM GlobalNM
	* Can be set only with SETDefault, not with SET.
	** Can be set only with SET, not with SETDefault.

The **AccessGroup** and **AccessWord** parameters together determine which ports can make connections to which ports, as described in Section 2.3.9. When a connection is requested, the system compares the AccessWord of the requesting port with the AccessGroup of the destination port. If at least one common group number appears in both sets, the connection is established.

If no common group numbers appear, the system prompts the user for a password associated with the `AccessGroup` parameter for the destination port (Section 4.2.5 describes group passwords). If the `AccessGroup` has more than one value, the password for any one of the values is accepted. Each of the two parameters can have the value `NoGroup`, `AllGroups`, or one or more numbers from 1 to 16. The default value for both parameters is 1.

Bridge recommends setting `AccessWord` to `NoGroup` for any port to which a dial-in modem is attached. This requires entry of the appropriate password before the user calling in can establish a connection through that modem.

The **AUTOdisconnect** parameter specifies the interval after which the current session will be disconnected if no activity occurs. The `AUtodisconnect` interval can be set to `Disabled` or to a number in the range 1 to 16000 (in minutes). A value other than `Disabled` is only appropriate for host ports. The default value is 60 minutes for host ports, and `Disabled` for terminal ports.

The **DeVice** parameter specifies a device type for the virtual port. One of two mutually exclusive primary values can be specified:

Host | Terminal

These values specify whether the device is a host or a terminal.

**** NOTE ****

The `DeVice` parameter value `Host` is not appropriate for any virtual port in the GS/1 Connection Service.

Setting `DeVice` to `Host` automatically resets the following other parameters: `BReakAction` is set to `Ignore`, `AUtodisconnect` is set to 60, and `ECMChar` and `BReakChar` are disabled. The `BufferSize` parameter is set to the buffer size specified at the time of system generation.

Setting `DeVice` to `Terminal` automatically resets the following other parameters: `BReakAction` is set to `EscDTM`, and `InterAction` is set to `Verbose` and `Echo`.

The default `DeVice` parameter value is `Terminal` for all virtual ports in the GS/1 Connection Service.

If `DeVice` is set to `Terminal`, one of the following mutually exclusive, secondary characteristics can also be specified:

Paper | Glass

These values determine whether the terminal is a video display unit (`Glass`, the default) or a hardcopy printer (`Paper`). The setting affects how backspacing is handled during local editing when the user erases a character or a word using `<BS>` or the local editing characters. If `DeVice` is set to `Glass`, the Connection Service causes the terminal cursor to move to the left one column for each character erased. If `DeVice` is set to `Paper`, the server prints a crosshatch symbol (#) for each character erased instead of attempting to move the print mechanism.

The **InitMacro** parameter specifies the name of a port initialization macro to be executed automatically each time the device makes a transition from Listening mode to Command mode. The macro itself is defined with the **DEFine** command. Section 2.3.4 describes modes of operation. Section 3.2.3 describes the **DEFine** command.

**** NOTE ****

This parameter cannot be used to establish a system initialization macro. To set up a macro that is to be executed automatically every time the server is booted, define a macro that begins with the letters "init".

The **InterAction** parameter describes the interaction between the local device and the GS/1. This parameter has no effect on a host port. The possible values are:

Verbose | Brief

Determines whether responses or error messages from the GS/1 Connection Service to the local device will be sent in their short form (Brief) or full length form (Verbose, the default). Brief responses are "OK" if the requested action is successful, and "Err <n>" if an error is encountered. Appendix A lists all error messages and their corresponding error numbers. The value Brief is appropriate for a port on which a host is emulating a terminal; Verbose is appropriate for a terminal.

Echo | NoEcho

Determines whether input from the local device is echoed back to the device while the device is in Command mode. The default is Echo.

MacroEcho | NoMacroEcho

Determines whether or not macros are echoed on the screen as they are executed. The default is MacroEcho.

BroadcastON | BroadcastOFF

Determines whether or not the port receives broadcast messages. The default is BroadcastON.

LFinsert | NoLFinsert

Determines whether or not the Connection Service echoes a return and a linefeed when the user enters a command. This option is useful for terminals that perform local echo but do not generate a linefeed echo when a return is entered. The default is NoLFinsert.

MacroBreak | NoMacroBreak

Determines whether the <BREAK> key can be used to stop execution of a macro. In macros that raise the privilege level to Local or Global Network Manager, setting NoMacroBreak prevents the user from breaking out of the macro and, as a result, being left in network manager privilege level. The default is MacroBreak.

The **MaxSessions** parameter specifies the maximum number of open sessions permitted on a single port. The parameter can be set to a number in the range 1 to 8. The default value is 2.

The **PRiVilege** parameter specifies the privilege level of the local device. This parameter affects all sessions, not just the current or next session. Privilege is not affected if a new configuration table obtained via the **ReaD** command contains a different privilege level (Section 3.2.11 describes the **ReaD** command). The default value is **User**. The **PRiVilege** parameter is the only parameter whose default value cannot be changed with the **SETDefault** command. Three privilege levels are available:

User

Specifies user privilege level. This level permits the user to display or set characteristics for the local device port.

LocalNM

Specifies Local Network Manager privilege level. This level permits the user to set characteristics and control the status of any port on the local GS/1 and to define the setup of the local server.

GlobalNM

Represents Global Network Manager level. This privilege level permits the user to set characteristics and control the status of any port on the network and to define the setup of either the local or a remote server.

4.2.2 GS/1 Port Physical Parameters

This section describes the port physical parameters, which are usually set for all ports by the network manager.

Because most of the physical characteristics of a GS/1's virtual ports are determined by the lines connecting the GS/1 with the X.25 network, the port physical parameters available on a Gateway Server are limited to a few data-transmission characteristics. The parameters and their possible values are summarized in Table 4-10.

Definitions of the parameters, explanations of each possible value, and an indication of the default follow the table. If the default value is acceptable, the parameter need not be set.

Table 4-10 GS/1 Port Physical Parameters	
<i>Parameter</i>	<i>Permitted Values</i>
CRPad	None <number> (1-127 nulls of padding)
DataBits *	7 8
* Can be set only with SETDefault, not with SET.	

The **CRPad** parameter specifies the number of nulls the server will insert following a carriage return before echoing or transmitting the next character. The default value is None (i.e., no nulls inserted).

The **DataBits** parameter specifies the number of data bits per byte. The value can be set to 7 or 8. The default is 8 for all virtual ports.

4.2.3 GS/1 Session Transmission Parameters

Table 4-11 lists the session transmission parameters. These values can all be set for the current session by the user. Definitions of the parameters, explanations of each possible value, and an indication of the default follow the table. If the default is acceptable, the parameter does not have to be set.

Table 4-11 GS/1 Session Transmission Parameters	
<i>Parameter</i>	<i>Permitted Values</i>
BReakAction	IGnore (OutofBand , FlushVC, InBand , EscDTM)
BReakChar	Disabled <char>
DataForward	None (AlphaNum , CR , ESC , EDiting , Term , FormEF , COntrol , Punct)
ECHOData	OFF ON
ECMChar	Disabled <char>
EOM	Disabled <char>
FlowControlFrom/ FlowControlTo	None XON _XOFF
IdleTimer	Disabled <number> (1-255 sixtieths of a second)
LFInsertion	None (OutputCrlf , EchoCrlf)
MOde	Transparent Scroll

The **BReakAction** parameter specifies the action taken by the server when a break signal (or the alternative character specified by the BReakChar parameter) is detected. The value IGnore is mutually exclusive with any other value: more than one of the remaining values can be specified. The default value is InBand for terminal ports and IGnore for host ports. The possible values are:

IGnore

Specifies no action.

OutofBand

Specifies that an out-of-band break will be transmitted to the remote device.

FlushVC

Specifies that all packets for this session currently in the circuit are flushed when a break is detected.

InBand

Specifies that an in-band break will be transmitted to the remote device (default).

EscDTM

Specifies that the user port will change from Data Transfer mode to Command mode.

The **BR**eakChar parameter specifies a character other than the break key that will be interpreted by the Connection Service as a break signal. This is useful for terminals that do not have a break key. The default value is Disabled.

The **DataForward** parameter specifies the events that cause data to be packetized and forwarded in Data Transfer mode. Some events are predetermined DataForward conditions; these include the elapsing of the IdleTimer (if enabled), the End of Message (EOM) signal, and the ATTN or break signal. One or more of the events listed below can also be specified. The default DataForward value is None, which is mutually exclusive with any other value.

None

Specifies that data will be forwarded only if the data buffer becomes full, or the IdleTimer elapses (if set). This is the default value.

AlphaNum

Specifies that a packet is created and forwarded as soon as any upper- or lowercase alphabetic character or numeric character is detected.

CR

Specifies that a packet is created and forwarded as soon as a return is detected.

ESC

Specifies that a packet is created and forwarded as soon as an escape (ESC, BEL, ENQ, or ACK) signal is detected.

EDiting

Specifies that a packet is created and forwarded as soon as any editing character is detected. Alternative editing characters can be specified; Section 4.2.4 lists the characters and their default values.

Term

Specifies that a packet is created and forwarded as soon as any terminator (ETX or EOT signal) is detected.

FormEF

Specifies that a packet is created and forwarded as soon as any "Form Effector" character is detected. Form Effectors are the linefeed, tab, and formfeed characters.

Control

Specifies that a packet will be created and forwarded as soon as any control character is detected.

Punct

Specifies that a packet is created and forwarded as soon as any "punctuation" character is detected (includes all the nonalphanumeric "graphics" characters, i.e., ! @ # \$ % ^ & * () _ - + = ~ ' | \ [] { } : ; " ' < > , . ? / and space).

The **ECHOData** parameter specifies whether the server will echo input data back to the device while the device is in Data Transfer mode. The default is OFF.

The **ECMChar** parameter specifies a character which will be interpreted by the Connection Service as a request to change from Data Transfer mode to Command mode. The default value is "^" (representing the character <CTRL-caret>). The defined character cannot be transmitted as data. This parameter is used only if the application requires that a break signal be transmitted as data (i.e., the BReakAction parameter is set to InBand or OutofBand).

The **EOM** parameter specifies a character to represent the local value of the End of Message (EOM) signal. The default value is <CTRL-M>.

The **FlowControlFrom** and **FlowControlTo** parameters specify the flow control mechanism from the GS/1 to the local device (i.e., the server can turn transmission from the local device on or off) and from the local device to the GS/1 (i.e., the local device can turn transmission from the server on or off), respectively. For all ports, the default value of both FlowControlFrom and FlowControlTo is XON_XOFF. One of the following mutually exclusive values can be specified:

None

Specifies that no flow control will be used. This is the default value.

XON_XOFF

Specifies that the XON character <CTRL-S> and the XOFF character <CTRL-Q> will be used.

The **IdleTimer** parameter specifies the interval after which, if no further characters are input from the local device, all accumulated characters are packetized and forwarded. In Data Transfer mode, characters are accumulated in a data buffer until an event specified by the DataForward parameter occurs, the buffer fills, or the IdleTimer interval elapses. IdleTimer can be set to Disabled or to a number in the range 1 to 255 (sixtieths of a second). The default value is 1.

The **LFInsertion** parameter specifies whether linefeeds will be transmitted (or echoed) following a return. This parameter is applicable only if the character specified by the EOM is a return and if the other side of the connection is in scroll mode. The default value is None; values permitted are:

None

Specifies that no linefeed will be echoed or transmitted with the return after an EOM signal. This is the default value.

OutputCrlf

Specifies that if an EOM signal is received from the remote device, a return and a linefeed will be sent to the device.

EchoCrlf

Specifies that if a return is received from the local device, a return and a linefeed will be echoed to the device.

The **MOde** parameter specifies one of two mutually exclusive Data Transfer modes:

Transparent

Specifies that the local device is a screen-oriented intelligent terminal whose display format is controlled by an application. Local editing and local echo are disabled. Except for the characters defined by the **ECMChar** and **BreakChar** parameters, all input from the terminal in Data Transfer mode is transmitted exactly as typed; no translation is provided. This is the default value.

Setting **MOde** to **Transparent** automatically resets the following parameters: **ECHOData** is set to **OFF**, **LFInsertion** is set to **None**, **DataForward** is set to **None**, **IdleTimer** is set to **1**, and **BReakAction** is set to **InBand**.

Scroll

Specifies that the local device is a line-oriented TTY-type terminal or application. Local editing and local echo are enabled.

Setting **MOde** to **Scroll** automatically resets the following parameters: **ECHOData** is set to **ON**, **LFInsertion** is set to **EchoCrlf** and **OutputCrlf**, **DataForward** is set to **CR**, and **IdleTimer** is set to **Disabled**.

4.2.4 GS/1 Session Editing Parameters

Table 4-12 summarizes the session editing parameters, which can be used in Command mode and in Data Transfer mode during sessions in which the M_{ODE} parameter is set to Scroll. Definitions of the parameters, explanations of each possible value, and an indication of the default follow the table. If the default is acceptable, the parameter does not have to be set.

Table 4-12 GS/1 Session Editing Parameters	
<i>Parameter</i>	<i>Permitted Values</i>
ERase	Disabled <char>
LineERase	Disabled <char>
LocalEDiting	(CmdEditing NoCmdEditing , DataEditing NoDataEditing)
ReprintLine	Disabled <char>
VERBatim	Disabled <char>
WordERase	Disabled <char>

The **ERase** parameter specifies the character (default <CTRL-H>) that the Connection Service interprets as an ERase character. If entered before the current line is terminated with a return, the ERase character deletes the most recently typed character. On most terminals, the backspace key also performs the ERase function.

The **LineERase** parameter specifies the character (default <CTRL-U>) that the Connection Service interprets as a LineERase character. If entered before the current line is terminated with a return, the LineERase character deletes the entire line.

The **LocalEDiting** parameter specifies whether local editing is permitted. The default value enables local editing in Command mode but not in Data Transfer mode. One value from each of two pairs of values can be specified:

CmdEditing | NoCmdEditing

Enables (the default) or disables local editing in Command mode.

DataEditing | NoDataEditing

Enables or disables (default) local editing in Data Transfer mode during a session in which the M_{ODE} parameter is set to Scroll.

The **ReprintLine** parameter specifies the character (default <CTRL-R>) that the GS/1 interprets as a ReprintLine character. This character is used to reprint all pending input on the current line before the line is terminated with a return.

The **VERBatim** parameter specifies the character (default <CTRL-V>) that the Connection Service interprets as a Verbatim character. The Verbatim character causes the editing character or other special character immediately following to be transmitted verbatim rather than interpreted by the server as a special character. The VERBatim character has no effect if the next character entered is a return or the VERBatim character itself.

The **WordERase** parameter specifies the character (default <CTRL-W>) that the server interprets as a WordERase character. If entered before the current line is terminated with a return, the WordERase character deletes the most recent word typed.

4.2.5 GS/1 Global Parameters

Table 4-13 lists the configuration parameters that determine the server's welcome message, prompts, passwords, and date. Each of these parameters affects the entire server, not just the current port or session. All of these parameters except the date must be specified with the SETDefault command, not with SET.

Table 4-13 GS/1 Global Parameters	
<i>Parameter</i>	<i>Permitted Values</i>
DATE	<yy/mm/dd hh:mm[:ss]> <mm/dd/yy hh:mm[:ss]>
DOmain *	<string>
GlobalPassWord *	<string>
GroupxPasswd *	<string>
LocalPassWord *	<string>
NMPrompt *	<string>
Organization *	<string>
PROMPt *	<string>
WelcomeString *	<string>
* Can be set with SETDefault only, not with SET.	

The **DATE** parameter is used to set the system clock. The value can be entered in either of the two formats shown in Table 4-13. Times are entered in 24-hour clock time. The clock is used for the network management reports and should be set after each system boot, unless there is an NCS on the network. Unusually frequent disk activity may cause the clock to drift by a few seconds per year.

The **DOmain** and **Organization** strings specify the default domain and organization fields for all clearinghouse names entered on the server. These defaults are automatically appended to the local name unless overridden when the name is entered. The default value of these parameters is the null string ("").

The **GlobalPassWord** parameter specifies the password (maximum 14 characters) that the user must type when setting the privilege level to Global Network Manager. The default password is the null string ("").

The **GroupxPasswd** parameter specifies the password (maximum 14 characters) that a user must enter in order to establish a connection with a device when the user's AccessWord values do not match any of the device's AccessGroup values. Each AccessGroup can have its own password. This system is designed to limit access within the network for security purposes, as described in Section 2.3.9. Only a Global Network Manager can set or change AccessGroups, AccessWords, or GroupxPasswds. The default password for each group is the null string ("").

The **LocalPassWord** parameter specifies the password (maximum 14 characters) that the user must type when setting the privilege level to Local Network Manager. The default password is the null string ("").

The **NMPrompt** parameter specifies the string (maximum 14 characters) that the server will print on the local device (starting in column 1) to indicate Command mode if the port has Local or Global Network Manager privilege. The default prompt is "gs/1# ".

The **PROMPt** parameter specifies the string (maximum 14 characters) that the server will print on the local device (starting in column 1) to indicate Command mode if the port has User privilege. The default prompt is "GS/1> ".

The **WelcomeString** parameter specifies the string output from the GS/1 to the the port when the port becomes active. The maximum length of the string is 80 characters. The default string is "^M^JWelcome to your Gateway Server^J".

4.2.6 Bridge Implementation of X.3 Protocol

This section describes the Bridge implementation of the X.3 protocol. Table 4-14 indicates the correspondence between the port configuration parameters available through the Connection Service and the X.3 parameters 1 through 18. The table also indicates any X.3 parameter values that are altered or converted by the Connection Service.

In the Bridge implementation, the InterAction, CRPad, and LFPad parameters (X.3 parameters 6, 9, and 14, respectively) are defined as port parameters rather than as session parameters. After a session is disconnected, these parameters may be different from their default values.

In all parameter exchanges between a GS/1 or CS/1-X.25 and an X.25 host, parameter conversion is effected so that the host detects no inconsistency. The X.25 interface performs the conversion and retains the X.3 value locally, in case the host needs to read the parameters back. However, if the user alters the InterAction, BReakAction, or LFInsertion parameters (X.3 parameters 6, 7, and 13, respectively) after a session has been established with an X.25 host, the host may change the parameter values for compatibility.

For Local Editing (X.3 parameter 15) to function properly, the Bridge EOMChar parameter must be disabled.

Table 4-14 Bridge-to-X.3 Parameter Conversions

<i>Parameter No.</i>	<i>Bridge Name/Values</i>	<i>X.3 Name/Values</i>	<i>Conversion</i>
1	ECMChar 0-127	PAD recall character 0,1,32-126	X.3 value 1 converted to <CTRL P>; no conversion on other values
2	EchoData 0-127	Echo 0,1,32-126	None
3	DataForward 0 = None 1 = AlphaNum 2 = CR 4 = COntrol 8 = ESC 16 = EDiting 32 = FormEF 64 = Punct 128 = Term and combinations	Data Forward 0,1,2,4,8,16, 32,64, and combinations	When parameter 15 is enabled, value 8 (editing characters) is turned on locally and is transparent to the user; if the host reads the parameters back, value 8 does not appear in parameter list
4	IdleTimer 0, 1-255	Idle Timer 0,1-255	Bridge value=(X.3 value*3); X.3 values 85 through 255 are converted to 255 in the Bridge implementation
5	FlowControlFrom 0 = None 1 = XON_XOFF 2 = CTS_RTS 3 = ENQ_ACK	Flow Control From 0,1	None

(continued)

Table 4-14 Bridge-to-X.3 Parameter Conversions (continued)

<i>Parameter No.</i>	<i>Bridge Name/Values</i>	<i>X.3 Name/Values</i>	<i>Conversion</i>
6	InterAction 0 = Verbose 1 = Brief 4 = NoEcho 8 = Completion	Interaction 0,1,4, and combinations	Since prompt service signals cannot be suppressed separately from PAD service signals in the Bridge environment, the X.3 value 5 (4+1) is converted to 1 in the Bridge implementation; Value 4 is used for "Echo/NoEcho"
7	BReakAction 0 = Ignore 1 = OutofBand 4 = InBand 8 = EscDTM 16 = FlushVC	Breakaction 0,1,2,4,8,21, and combinations	X.3 value 2 (RESET) is not supported by the Bridge implementation; the Bridge value is FlushVC (output data is flushed when a break signal is detected)
8	FlushVC 0,1	Discard Output 0,1	None
9	CRPad 0-127	CR Padding 0-7	None
10	None	Line Folding 0-255	The Bridge implementation accepts this parameter, and performs no action with it

(continued)

Table 4-14 Bridge-to-X.3 Parameter Conversions (continued)

<i>Parameter No.</i>	<i>Bridge Name/Values</i>	<i>X.3 Name/Values</i>	<i>Conversion</i>
11	BAud	Baud Rate	The host should not set the baud rate parameter; if the host reads the parameter value, the Bridge values are converted to X.3 values
	0-50	0-110	
	1-75	1-134.5	
	2-110	2-300	
	3-134.5	3-1200	
	4-150	4-600	
	5-200	5-75	
	6-300	6-150	
	7-600	7-1800	
	8-1200	8-200	
	9-1800	9-100	
	10-2400	10-50	
	11-3600	11-75/1200	
	12-4800	12-2400	
	13-7200	13-4800	
	14-9600	14-9600	
	15-19.2K	15-19.2K	
	16-38.4K	16-48K	
	17-64K	17-56K	
	18-56K	18-64K	
	19-76.8		
	20-153.6K		
12	FlowControlTo	Flow Control To	None
	0 = None	0,1	
	1 = XON_XOFF		
	2 = CTS_RTS		
	3 = ENQ_ACK		

(continued)

Table 4-14 Bridge-to-X.3 Parameter Conversions (continued)

<i>Parameter No.</i>	<i>Bridge Name/Values</i>	<i>X.3 Name/Values</i>	<i>Conversion</i>
13	LFInsertion 0 = None 1 = OutputCtrl 4 = EchoCtrl and combinations	Line Feed Insertion 0,1,2,3, and combinations	X.3 value 2 (LF insertion after a <CR> from DTE) is not supported in Bridge implementation; no conversion on other values
14	LFPad 0-127	LF padding 0-7	None
15	LocalEditing 0,1	Local Editing 0,1	None
16	Erase 0-127	Char Delete 0-127	None
17	LineErase 0-127	Line Delete 0-127	None
18	ReprintLine 0-127	Reprint Line 0-127	None

APPENDIX A

CONNECTION SERVICE ERROR MESSAGES

This appendix provides an alphabetical list of all error messages generated by the Connection Service and describes the probable causes of each message. Unless specifically noted, the error messages apply to all Connection Service servers.

The error code listed for each message is the number generated if the port's InterAction parameter is set to Brief, which causes the server to return errors as numeric codes rather than as text strings. For the convenience of users who encounter only the Brief mode error numbers, Table A-1 at the end of the appendix lists the error messages by error number.

A.1 Text Messages

Aborted

Error code: 50

This message appears if the user terminates the interactive setting of a port's default parameters by pressing the escape key before the system has stepped through all parameters. All parameters set prior to the escape take effect, but the system does not prompt for more values.

The interactive setting of all default parameters for a port is initiated by entering the SETDefault command without specifying any parameters.

Ambiguous, try one of: <command names>

Error code: 55

This message appears if the user types an incomplete command name. The system lists all possible commands that could be made from the incomplete entry. Reenter the command using an unambiguous abbreviation of the command name.

Ambiguous parameter name, try one of: <parameter names>

Error code: 46

This message appears if the user types an incomplete parameter abbreviation in one of the commands that sets or displays a parameter value. The system lists all parameter names that could be assumed from the incomplete entry. Reenter the command using an unambiguous abbreviation of the parameter.

Autodisconnect timer expired

Error code: -12

This message appears if the user's port has been inactive longer than the interval specified by the AUToDisconnect parameter of the destination port. The default value of the AUToDisconnect parameter is 60 minutes for all ports whose DeVice parameter is set to Host; the parameter does not apply to ports whose DeVice parameter is set to Terminal and does not apply to GS/1 virtual ports.

Broadcast is not enabled for that port

Error code: 78

This message appears if the user attempts to broadcast a message to a port whose InterAction parameter is set to BroadcastOFF.

Can't - diskette write protected

Error code: 28

This message appears if the user issues a command requiring information to be stored on the system diskette while a write-protect tab is in place on the diskette. First remove the write-protect tab from the diskette, then enter the command again.

If this message appears in response to the Name command, the system may have placed a protective lock on the clearinghouse database. In this case, a subsequent attempt to enter the Name command results in a disk I/O error. To recover, reboot the server, using a system diskette that is not write-protected.

Can't - no memory

Error code: 37

This message appears if the system does not have enough memory available at the time a command is entered to complete execution of the command. In most cases, this is a temporary situation caused by an unusual circumstance, such as multiple users issuing simultaneous requests for a complex macro file. Wait until system activity has decreased and enter the command again. If this message appears in response to the DO command, the specified macro file may contain too many complex display commands. If the system fills all available buffers while waiting for a display to complete, it terminates the process (i.e., places the port in Listening mode).

Can't DEFine from a macro

Error code: 73

This message appears when a macro file that contains a DEFine command is executed with the DO command. Macro files cannot contain the DEFine command.

Macro files can, however, contain the DO command to call a different, predefined macro.

Can't REMoteSET this parameter

Error code: 75

This message appears if the user tries to use the REMoteSET command to change a parameter that can be changed only with the SET or SETDefault command.

The REMoteSET command can be used to change some but not all of the parameters that can be changed with the SET command. To display a list of all parameters that can be set with the REMoteSET command, enter the command followed by a question mark.

Can't save -- directory full

Error code: 30

This message appears on disk-based servers if the user tries to add another configuration or macro file after all available disk space for these files is used.

A disk-based CS/1 holds up to 96 configuration files and up to 96 macro files; a GS/1 holds up to 48 configuration files and up to 48 macro files; a disk-based CS/100 holds up to 32 configuration files and up to 32 macro files.

Can't SET yet -- no session

Error code: 77

This message appears if the user tries to set an active session parameter for a port with no current sessions.

When a port changes from Listening to Command mode, the system creates a working table of active port parameters by copying the port parameter portions of the port's default parameter table. When a connection with a remote device is established on that port, the server completes the active parameter table by copying the session parameters from the default parameter table. The SET command can be used only to change parameters that have an active value.

Can't SETD this parameter

Error code: 76

This message appears if the user tries to change the default value of the PRIVilege parameter.

For security purposes, the default value of the PRIVilege parameter is always User for all ports. In order to access higher privilege levels, the user must issue the SET PRIVilege command and enter the appropriate password. The higher privilege level remains in effect only as long as the port remains active.

Clearinghouse is out of memory

Error code: 19

This message appears if the system does not have enough memory available to process the command when a clearinghouse access request is entered. In most cases, this is a temporary situation caused by an unusually high level of system use. Wait until demand for system resources is lower and reissue the command.

Clearinghouse name in use

Error code: 6

This message appears if the user specifies in the Name command a clearinghouse name that is already defined in the local clearinghouse.

To change the assignment of a name that has already been defined, first remove the name from the clearinghouse with the UNName command, and then redefine it with the Name command.

Clearinghouse name invalid

Error code: 2

This message appears if the user specifies an illegal clearinghouse name in the Name or Connect command. The local name field in a clearinghouse name can include up to 10 alphanumeric characters, the first of which must be an alphabetic character, or up to 18 numeric digits. For more information on clearinghouse names, see Section 3.1.

Clearinghouse name not found

Error code: 11

This message appears if the server is unable to locate in any clearinghouse on the network a name specified in the Connect or SHow CHN <name> command. A failure to locate the name can mean either that the name has not been defined or that the server on which the name is defined is not currently available.

Clearinghouse name table is full

Error code: 18

This message appears if the clearinghouse name table is already full when the user issues the Name command. The Series/1 servers that boot from a local disk drive each support up to 80 clearinghouse names. A CS/100 that boots from a local disk drive supports up to 18 clearinghouse names. An NCS/150 supports a combined maximum of 256 clearinghouse names for all of its clients. An NCS/1 supports up to 4,096 clearinghouse names for all of its client servers.

Clearinghouse received no response

Error code: 22

This message appears if a Communications Server that boots from an NCS receives no answer to a clearinghouse access request sent to the NCS. The message could mean that the NCS is turned off or disconnected from the network, or that the NCS is momentarily busy handling other requests.

Clearinghouse value invalid

Error code: 16

This message appears if the user issues a command containing a logical name longer than 120 characters; the message does not appear as a GS/1 error message.

Directory empty

Error code: 31

This message appears if the user requests a display of the stored macro or configuration files before any files have been established.

DISKIO read error

Error code: 25

This message appears if the system is unable to complete a diskette read process. The most likely cause of the read error is deterioration of the diskette medium. Try replacing the working diskette with a backup copy.

DISKIO seek error

Error code: 24

This message appears if the system is unable to complete a diskette seek process. The most likely cause of the seek error is deterioration of the diskette medium. Try replacing the working diskette with a backup copy.

DISKIO write error

Error code: 26

This message appears if the system is unable to complete a diskette write process. The most likely cause of the write error is deterioration of the diskette medium. Try replacing the working diskette with a backup copy.

Drive door open or diskette missing

Error code: 27

This message appears if an attempt to read or write to the diskette fails because the drive door is open or the diskette is not in place in the drive.

File not found or in use

Error code: 29

This message appears if the NCS/150 fails to respond to a request from a client server for access to a configuration or macro file. The message may mean only that another device on the network is currently accessing the file. If the message appears repeatedly, however, the requested file may not exist.

Illegal request -- wrong state

Error code: -1

This message appears if the user issues a command that has no meaning for the port in its current state. This message appears, for example, in response to the DEQueue command issued at a port that has no queued connection request.

Insufficient privilege

Error code: 36

This message appears when a user issues a command that requires a higher privilege level than is currently in effect at the local port. There are three privilege levels: User, Local Network Manager, and Global Network Manager. Section 3.2 lists the default privilege level required for each command.

Invalid <command> syntax

Error code: 33

This message indicates a syntax error in the last command issued. The error could be with one of the fields in the command line or with the structure of the command line. For a syntax description of a command, enter the command name followed by a question mark.

Invalid DATE

Error code: 70

This message indicates a syntax mistake in the SET DATE command. The date entered must follow one of these formats:

```
yy/mm/dd hh:mm[:ss]
mm/dd/yy hh:mm[:ss]
```

Invalid <product type> command

Error code: 39

This message appears when the user issues a command that the server does not recognize. The message usually indicates a typing mistake, although it sometimes appears in response to a syntax error.

The message may also appear in response to a Connection Service command that is not available on the model of server with which the user is interacting. To display a list of all available commands, enter a single question mark.

Invalid remote command

Error code: 68

This message appears when a user in remote communication with a distant server issues a command that is not available in remote mode. Only a subset of the standard commands are available in remote mode. Specifically, commands used to create and manipulate new sessions are restricted. The REMoteSET, REMoteSHow, and RESume commands are unavailable on the Communications Server. On the Communications Servers and the GS/1, the Connect command may be used only to interconnect remote ports, and the SWitch and Transmit commands are unavailable.

To display a list of available commands, enter a single question mark.

Invalid session number

Error code: 42

This message appears when the user specifies an inappropriate session number in a command that accepts a session number as an argument. Either the specified session number does not exist or it is not a valid session number.

Valid session numbers are the digits 1 through 8. Sessions are numbered sequentially in the order in which they are created; each session retains its original session number even if sessions with lower numbers are subsequently terminated.

Macro definition too long

Error code: 72

This message appears in response to the DEFine command if the defined macro includes more than 256 characters.

If the commands to be included in the macro require more than 256 characters, split the contents into two or more macro files, and imbed the DO command in one of them to call the others.

Macros nested too deeply

Error code: 74

This message appears when a user executes with the DO command a macro that initiates a sequence of more than ten calls to other macros. Although the DO command may be embedded in a macro in order to call another macro, the nesting of macros is limited to ten.

Missing '=' after parameter <parameter name>

Error code: 43

This message appears in response to the SET, SETDefault, or REMoteSET command if the user omits the equal sign (=) between the parameter name and the parameter value. Section 3.2 describes these commands.

Missing <value> after parameter <parameter name>

Error code: 44

This message indicates that the parameter value is missing in the SET, SETDefault, or REMoteSET command.

To display a list of all values that can be specified for a given parameter, enter this command:

```
set <parameter name> = ?
```

Name Server is out of memory

Error code: 19

This message appears if the system does not have enough memory available to process the command when a Name Server access request is entered.

In most cases, this is a temporary situation caused by an unusually high level of system use. Wait until the demand for system resources is lower and reissue the command.

Name Server name in use

Error code: 6

This message appears if the user specifies in the Name command an internet name that is already defined in the local Name Server. On a server running XNS protocols, this message appears if the user specifies a clearinghouse name that is already defined on the local clearinghouse. To change the assignment of the name, first remove the name with the UNName command, and then redefine it with the Name command.

Name Server name invalid

Error code: 2

This message appears if the user specifies an illegal internet name in the Name or Connect command. For more information on internet names, see Section 3.1.

Name Server name not found

Error code: 11

This message appears if the server is unable to locate in any Name Server on the network a name specified in the Connect or SHow NAMES <name> command. A failure to locate the name can mean either that the name has not been defined or that the server on which the name is defined is not currently available.

Name Server name table is full

Error code: 18

This message appears on TCP servers if the internet name table is already full when the user issues the Name command. A CS/1 supports up to 64 internet names; a CS/100 supports up to 24 internet names.

Name Server value invalid

Error code: 16

This message appears if the user issues a command containing a logical name longer than 120 characters.

No access allowed

Error code: -13

This message appears if a user is unable to provide the correct password after issuing a connection request to an access-controlled port. If the user's port was configured to allow access to the device, then this message does not appear because the user is not required to issue a password.

First ascertain the password needed to make the connection, then reissue the connection request. To set up the port permanently for unrestricted access to the destination device, set the AccessWord parameter of the source port to match at least one value in the AccessGroup parameter of the destination port.

No current session

Error code: 40

This message appears if the user issues a command that affects a session when no session exists. The RESume, SWitch, and DEQueue commands, for example, have no meaning unless a suspended or queued session exists on the port.

No memory resource

Error code: -2

This message appears if the system does not have enough memory available to complete execution of the last command entered. In most cases, this is a temporary situation caused by an unusually high demand for system resources. Wait until system activity levels are lower and reissue the command.

No more sessions for this port

Error code: -9

This message appears in response to the Connect command if the source port is already connected to as many devices as allowed for that port.

The default maximum number of sessions for each port is two. This maximum can be changed with the MaxSessions parameter (refer to Section 4.2.1).

No other sessions

Error code: 41

This message appears if the user issues the SWitch command to change to another session when only one session exists on the port.

No response

Error code: -10

This message appears when a session has been terminated by the server at the host end because no activity has taken place on the circuit for the period of time specified by the AUToDisconnect parameter. The message may also appear if the server at the host end stops responding to packets from the server at the terminal end.

Parameter may not be SET, use SETD

Error code: 69

This message appears if the user tries to adjust a parameter with the SET command that can be changed only with the SETDefault command. The parameters that can be set only with SETDefault are InitMacro, DataBits, GlobalPassWord, GroupxPasswd, LocalPassWord, NMPrompt, PROMPt, and WelcomeString.

Parameter <name>: Value <value> is illegal

Error code: 47

This message appears if the user specifies a value that is not available for the parameter being set. Some parameters accept numeric or string values, and some parameters accept only values from a list of system-defined options.

To display a list of all settings available for a specific parameter, enter the SET command followed by the parameter name and a question mark.

Parameter <name>: Value <value> is out of range

Error code: 48

This message appears if the user specifies an illegal value for one of the parameters that accepts numeric values. To display the acceptable range for a parameter value, enter the SET command followed by the parameter name and a question mark.

Parameter <name> unknown

Error code: 34

This message appears if the user enters a word the server does not recognize in a place where the server expects a parameter name. This message could appear if, for example, the user inserts an address or parameter value at the wrong place in a command. For a list of all parameters available, refer to Section 4.0. To invoke a screen display of the parameters available with a specific command, enter the command name followed by a question mark:

<command name> ?

Portid out of range

Error code: 59

This message appears if the user specifies a port number that is not available on the server that implements the command. The CS/1 uses physical port numbers 0 through 31 and virtual port numbers 32 through 95; the CS/100 uses physical port numbers 0 through 13 and virtual port number 14; the GS/1 uses virtual port numbers 0 through 47.

Remote is busy

Error code: -5

This message appears in response to the Connect command if the requested destination port is already part of another virtual circuit.

Remote is disabled or nonexistent

Error code: -4

This message appears in response to the Connect command if the requested destination port does not respond to the connection request.

Usually, this message indicates that the destination device is turned off or disconnected. It can also mean that the port configuration of the destination device is not appropriate for the device. If this message appears when the destination device is actually available, check the setting of the UseDTRin parameter on the destination port. Ordinarily this parameter is set to AsDTR for a host port. If, however, the host does not generate a DTR signal, the UseDTRin parameter should be set to Ignore or AsDCD.

Remote received bad address

Error code: -6

This message appears if the user specifies an invalid port number as all or part of the destination address in a connection request.

Remote received bad parameters

Error code: -8

This message occurs only if a connection is made between a Bridge server and a non-Bridge server. When the connection is established, a set of parameters is exchanged between the two servers. If either server does not recognize one or more of the parameters, it sends this message to the other end of the connection.

Remote software incompatible

Error code: -3

This message appears if a user tries to interact with a remote server that is running a version of the communications software incompatible with the version running on the local server.

This occurs only if one or more servers on the network is running an obsolete version of software. Use the **SHow VERSion** command on each server to determine which is running obsolete software.

Reserved timer expired

Error code: -14

This message appears if the user failed to complete a queued connection within five minutes of being informed that the queued connection is available. When this message appears, the user's port is removed from the connection queue and the connection is given to the next port in the queue, if any.

To complete a queued connection when it becomes available, the user issues the **RESume** command. If a different session is active on the user's port when the notification is received, the user must first issue the **SWitch** command so that the queued session is current.

Rotary number out of range

Error code: 58

This message appears if the user specifies an illegal rotary number. Rotary numbers can be established in the range 128 through 135.

SET what?

Error code: 45

This message appears if the user omits the parameter name from the **SET** command. For a list of all parameters that can be set, enter the **SET** command followed by a question mark:

set ?

SHow parameters for which port?

Error code: 71

This message appears if a user issues the **SHow PARAMeters** command in remote mode without specifying a port number. Since a user in remote mode is communicating with a virtual network manager port, the **SHow PARAMeters** command cannot assume the local port as the default.

SHow what?

Error code: 51

This message appears if the user omits the keyword from the SHow command. For a list of all variations on the SHow command, enter the command followed by a question mark:

```
show ?
```

Sorry

Error code: 49

This message appears if the user failed to supply the correct password while trying to change privilege levels or connect to an access-controlled destination address.

If the user fails to supply the correct password on the previous 1000 attempts to change privilege level, no password prompt appears. Instead, this message appears immediately after the request. Passwords must be entered in the correct case and must match exactly the password established by the network manager. The default value for all passwords on a new server is null ("").

String truncated

Error code: 54

This message appears if the user enters a string that is too long for the command in which it is included.

The local name field of a clearinghouse name can contain up to 10 alphanumeric characters or up to 18 all-numeric characters. The domain and organization fields of a clearinghouse name can contain up to 10 alphanumeric characters. Filenames, passwords, and prompts can contain up to 14 characters. The welcome string can be up to 80 characters long. The Broadcast, Echo, and Transmit commands accept strings up to 82 characters long.

Timeout failure

Error code: -11

This message appears if a server receives no answer to a request for information across the network. The message most often means that the server to which the request is directed is turned off or disconnected.

Unknown errors

Error code: -7

This message appears if the server is unable to complete the last command entered and is unable to identify the source of the problem.

Unknown <product type> command

Error code: 38

This message appears if the server does not recognize the first word in a command. The message usually indicates a typing mistake, but it can also mean that the user has entered a valid command that is not available on the local server. For example, a server running an early software version may not recognize the DEQueue command.

For a list of all commands available to the local port at its current privilege level, enter a question mark.

A.2 Error Codes

Table A-1 lists all numeric error codes. Messages numbered -14 through -1 are errors reported by the Virtual Terminal Protocol. Messages 1 through 22 are errors reported by the Name Service. Messages 23 through 30 are errors reported by the DISKIO Service. Messages 31 through 59 represent other miscellaneous errors. Messages 60 through 66 are informational responses rather than error messages. Messages 68 to 77 are also primarily informational messages, but indicate that the command failed for the stated reason.

Table A-1 Brief Mode Error Codes

<i>Error Code</i>	<i>Equivalent Message</i>
-14	"Reserved timer expired"
-13	"No access allowed"
-12	"Autodisconnect timer expired"
-11	"Timeout failure"
-10	"No response"
-9	"No more sessions for this port"
-8	"Remote received bad parameters"
-7	"Unknown errors"
-6	"Remote received bad address"
-5	"Remote is busy"
-4	"Remote is disabled or nonexistent"
-3	"Remote software incompatible"
-2	"No memory resource"
-1	"Illegal request -- wrong state"
0	No error
1	(1)
2	"[Clearinghouse Name Server] name invalid"
3-5	(1)
6	"[Clearinghouse Name Server] name in use"
7-10	(1)
11	"[Clearinghouse Name Server] name not found"
12-15	(1)
16	"[Clearinghouse Name Server] value invalid"
17	(1)
18	"[Clearinghouse Name Server] name table is full"
19	"[Clearinghouse Name Server] is out of memory"
20	(1)
21	(1)
22	"Clearinghouse received no response" (2)
23	(1), (3)
24	"DISKIO seek error"
25	"DISKIO read error"
26	"DISKIO write error"
27	"Drive door open or diskette missing"
28	"Can't - diskette write protected"
29	"File not found or in use"
30	"Can't save -- directory full"
31	"Directory empty"
33	"Invalid <command> syntax"
34	"Parameter <name> unknown"
35	(1)

(continued)

Table A-1 Brief Mode Error Codes (continued)

<i>Error Code</i>	<i>Equivalent Message</i>
36	"Insufficient privilege"
37	"Can't - no memory"
38	"Unknown <server type> command"
39	"Invalid <server type> command"
40	"No current session"
41	"No other sessions"
42	"Invalid session number"
43	"Missing '=' after parameter <name>"
44	"Missing <value> after parameter <name>"
45	"SET what?"
46	"Ambiguous parameter name, try one of: <names>"
47	"Parameter <name>: Value <value> is illegal"
48	"Parameter <name>: Value <value> is out of range"
49	"Sorry"
50	"Aborted"
51	"SHow what?"
52	(1)
53	Not used
54	"String truncated"
55	"Ambiguous, try one of: <command names>"
56	"... failed" (4)
57	(1)
58	"Rotary number out of range"
59	"Portid out of range"
60	"Global Parameters saved"
61	"Statistics saved"
62	" interconnection formed" (5)
63	" disconnected" (5)
64	Not used
65	"File replaced"
66	"@" (6)
67	Not used
68	"Invalid remote command"
69	"Parameter may not be SET, use SETD"
70	"Invalid DATE"
71	"SHow parameters for which port?"
72	"Macro definition too long"
73	"Can't DEFine from a macro"
74	"Macros nested too deeply"
75	"Can't REMoteSET this parameter"

(continued)

Table A-1 Brief Mode Error Codes (continued)	
<i>Error Code</i>	<i>Equivalent Message</i>
76	"Can't SETD this parameter"
77	"Can't SET yet -- no session!"
78	"Broadcast is not enabled for that port"
(1)	Used only internally or in the VT Program Interface Service; does not appear in the standard Connection Service.
(2)	Not used in the GS/1 Connection Service.
(3)	For GS/1 Connection Service, see note (1), above.
(4)	Appears in conjunction with error code explaining failure.
(5)	Appears in conjunction with the "Connecting ..." or "Disconnecting ..." messages.
(6)	Listening mode symbol.

APPENDIX B

3270 SETUP MODE

This appendix describes 3270 setup mode. This information applies only to CS/1 ports on an SIO-3270 board. Three main menus and three submenus are used to manipulate the setup features.

To enter setup mode, use the following setup key combination:

SHIFT-ALT-SPACE

Hold down the SHIFT and ALT keys, and press the space bar. When setup mode is entered, Main Menu 1 appears.

Setup mode may also be entered by pressing the SHIFT key twice immediately after booting the SIO-3270. On some display stations (such as a personal computer containing an IRMA board), setup mode must be entered in this manner in order to set up an alternate key combination for entry into setup mode.

B.1 Setup Mode Commands

The titles of the three main menus are Menu 1, Menu 2, and Menu 3. The titles of the three submenus are Tab Setting, Function Keys, and Keyboard Definition. These menus are described in detail in following subsections.

The following commands may be used in any menu, except the Keyboard Definition submenu. In the Keyboard Definition submenu, only SHIFT-ALT-SPACE and the keyboard definition commands may be entered.

SHIFT-ALT-SPACE	Exits or enters setup mode.
SHIFT-ALT-DELETE	Reads default setup values. This command is useful upon initial power-on or as a temporary choice until all options are explored.
R	Recalls saved values from EEPROM (non-volatile) memory. This command is useful if temporary changes to setup parameters are made, and then the previously saved values are needed. When R is used, saved values overwrite values currently in operation.
S	Saves the current setup values into EEPROM memory. Changes to setup values remain in effect only until the server is powered off. Upon being powered on, the server reads new setup values from memory. Consequently, changed values must be saved into EEPROM memory in order to be read into memory when the server is powered on.
X	Clears the screen, exits setup mode, and resets the display station. When a display station makes a connection to certain host computers, the host may set certain terminal parameters to inappropriate values, resulting in abnormal display station operation. The X command is used to recall appropriate parameter values.

B.2 Main Menus

The following input keys are common to all three main menus. If a key is pressed that is not allowed, the display station bell rings and the key is ignored.

Left arrow	Displays the previous main menu.
Right arrow	Displays the next main menu.
Up arrow	Moves cursor to the previous line of the current menu.
Down arrow	Moves cursor to the next line of the current menu.
SPACE	Displays the next available option at the current line. Each line offers a predefined set of options. Pressing the space bar displays the next available option.
SHIFT-ALT-RESET	Enters the Keyboard Definition submenu.
T	Enters Tab Setting submenu.
F	Enters Function Keys submenu.

Pressing a key that is not allowed rings the display station bell.

The line at which the cursor is positioned is highlighted by brighter intensity in monochrome display stations and by a different color in color display stations.

Move the cursor to the desired line using the up and down arrows; then use the space bar to display the desired option. For most options, the displayed option takes effect when setup mode is exited. However, some options take effect immediately upon being displayed; these are noted below.

In the following descriptions, the default option is indicated by the character ">".

B.2.1 Main Menu 1 Options

Main Menu 1 is shown in Figure B-1.

MENU (1)		
ONLINE/LOCAL		ONLINE
LANGUAGE		ENGLISH US
EMULATION		VT-100
KEYBOARD		STANDARD
PAGE MODE		DISABLED
STATUS LINE		SI0-78

LEFT / RIGHT	PREV / NEXT SCREEN	S SAVE ALL PARAMETERS
UP / DOWN	PREV / NEXT LINE	R RECALL SAVED VALUES
SPACE	NEXT VALUE	T ENTER TABS MENU
SHIFT-ALT-RESET	KEYBOARD DEFINITION	F PROGRAM FUNCTION KEYS
SHIFT-ALT-DELETE	DEFAULT VALUES	X RESET TERMINAL
SHIFT-ALT-SPACE	EXIT SETUP MODE	

Figure B-1 Main Menu 1

Each option is described below. The default option is indicated by the character ">".

Online/Local This option determines whether characters entered after exiting setup mode are transmitted to the host, or echoed to the screen without being transmitted. Select Online to transmit to the host or Local to echo to the screen without transmission:

```

LOCAL
> ONLINE

```

Language

This option determines, for certain characters, the ASCII code that is generated when a particular key is pressed. For example, a French keyboard has keys marked é and è. For the ASCII é and è codes to be generated when those keys are pressed, French must be selected using this option. Table B-1 indicates the ASCII codes generated by various keys in each language.

Any language can be selected on any type of keyboard; the keyboard can then be matched to the language by marking the appropriate keys with decals or new key caps.

This option does not influence the language used in screen displays and prompts; English is always used in screen displays.

One of the following languages may be selected:

- > ENGLISH, U.S.A.
- ENGLISH, U.K.
- FRENCH
- SWED/FINN
- GERMAN
- ITALIAN
- DANISH
- SPANISH

Table B-1 ASCII Codes Generated in Available Languages

Language	ASCII Code											
	23	24	40	5b	5c	5d	5e	60	7b	7c	7d	7e
English, U.S.A.	#	\$	@	[\]	^	'	{		}	~
English, U.K.	£	\$	@	[\]	^	'	{		}	~
French	#	\$	à	°	ç	§	^	'	é	ù	è	..
Swedish/ Finnish	#	ö	É	Ä	Ö	Å	Ü	é	ä	ö	å	ü
German	#	\$	§	Ä	Ö	Ü	^	'	ä	ö	ü	ß
Italian	#	\$	@	°	\	é	^	ù	à	ò	è	ì
Danish	#	\$	@	Æ	Ω	Å	^	'	æ	Ø	å	~
Spanish	R	\$	@	i	Ñ	*	^	'	°	ñ	}	~

* With Language set to Spanish, ASCII code 5d prints as a space.

Emulation	<p>A CS/1 containing an SIO-3270 can emulate a VT100 or an Extended VT100. Usually, VT100 emulation is used to interface to DEC hosts, and Extended VT100 emulation is used to interface to IBM hosts. Select one of the following emulation modes:</p> <ul style="list-style-type: none">> VT-100EXTD VT-100
Keyboard	<p>Because similar IBM display stations have different keyboard layouts, the SIO-3270 can be set up for custom keyboard definition. If custom keyboard definition is selected, the keyboard is mapped according to entries made using the Keyboard Definition submenu, described in Section B.3.3. Custom or standard keyboard definition takes effect immediately. Select one of the following options:</p> <ul style="list-style-type: none">> STANDARDCUSTOM
Page Mode	<p>If page mode is enabled, the server stops when the screen becomes filled and requires the user to press the Next Page combination (SHIFT-ALT-DEL) before input may resume. With this option disabled, the screen scrolls when full. Select one of the following options:</p> <ul style="list-style-type: none">> DISABLEDENABLED
Status Line	<p>This option determines whether the status line is controlled by the CS/1-3270 or by the host. Select one of the following:</p> <ul style="list-style-type: none">> SIO-3270HOST

B.2.2 Main Menu 2 Options

Main Menu 2 is shown in Figure B-2.

MENU (2)		
AUTO NEW LINE		DISABLED
AUTO LINE WRAP		DISABLED
CONTROL REPRESENTATION		DISABLED
CURSOR TYPE		UNDERLINE
CURSOR BLINK		DISABLED
CLICK		AUDIBLE

LEFT / RIGHT	PREV / NEXT SCREEN	S SAVE ALL PARAMETERS
UP / DOWN	PREV / NEXT LINE	R RECALL SAVED VALUES
SPACE	NEXT VALUE	T ENTER TABS MENU
SHIFT-ALT-RESET	KEYBOARD DEFINITION	F PROGRAM FUNCTION KEYS
SHIFT-ALT-DELETE	DEFAULT VALUES	X RESET TERMINAL
SHIFT-ALT-SPACE	EXIT SETUP MODE	

Figure B-2 Main Menu 2

Each option is described below. The default option is indicated by the character ">".

Auto New Line This option determines whether the server performs a linefeed automatically when the Return key is pressed. Disable this option to perform a linefeed with return; enable it to perform return only:

> DISABLED
ENABLED

Auto Line Wrap	With auto line wrap enabled, the cursor automatically advances to the first column of the next line when the end of a line is reached. With this option disabled, the applications program is responsible for advancing the cursor at the end of the line. Select one of the following options: > DISABLED ENABLED
Control Representation	By default, control characters are nonprinting characters. With control representation enabled, control characters are printed as a caret followed by the appropriate character, e.g., ^C. Enabling control representation is often useful for debugging. Select one of the following options: > DISABLED ENABLED
Cursor Type	The cursor can be set to appear as an underscore or as a block. This option takes effect immediately. Select one of the following options: > UNDERLINE BLOCK
Cursor Blink	With cursor blink enabled, the cursor flashes on and off. This option takes effect immediately. Select one of the following options: > DISABLED ENABLED
Click	With click set to audible, the display station emits an audible click each time a key is pressed. This option takes effect immediately. Select one of the following options: SILENT > AUDIBLE

B.2.3 Main Menu 3 Options

Main Menu 3 is shown in Figure B-3.

MENU (3)		
SHIFT + ALT DEFAULT MAP		NO
HOST IBM ONLY		NO
MARGIN BELL		DISABLED

LEFT / RIGHT	PREV / NEXT SCREEN	S SAVE ALL PARAMETERS
UP / DOWN	PREV / NEXT LINE	R RECALL SAVED VALUES
SPACE	NEXT VALUE	T ENTER TABS MENU
SHIFT-ALT-RESET	KEYBOARD DEFINITION	F PROGRAM FUNCTION KEYS
SHIFT-ALT-DELETE	DEFAULT VALUES	X RESET TERMINAL
SHIFT-ALT-SPACE	EXIT SETUP MODE	

Figure B-3 Main Menu 3

Each option is described below. The default option is indicated by the character ">".

Shift + Alt Default Map This option should be set to Yes only on personal computers containing an IRMA board. Setting this option to Yes enables the user to press the three keys CURSOR BLINK, ALT CURSOR, and SPACE in sequence, not simultaneously, to enter or exit setup mode. In page mode, it also enables the user to press the three keys SHIFT, ALT, and NEWLINE in sequence to go on to the next page. Select one of the following:

- > NO
- YES

Host IBM Only

If Host IBM Only is set to Yes, then the Escape sequence ESC# is transmitted when setup mode is exited. This Escape sequence is used by the host interface to refresh the screen. Select one of the following:

- > NO
- YES

Margin Bell

With margin bell enabled, the display station bell rings when the cursor reaches the eighth column before the last column of the screen, similar to a bell on a typewriter. Select one of the following options:

- > DISABLED
- ENABLED

B.3 Submenus

The submenus include the Tab Setting, Function Keys, and Keyboard Definition Submenus.

Exiting a submenu returns the user to the menu from which the submenu was entered, with the cursor positioned where it was when the submenu was entered.

Pressing a key that is not allowed rings the display station bell.

B.3.1 Tab Setting Submenu

To enter the Tab Setting submenu, enter the following command from any main menu:

T

When this command is entered, the Tab Setting Submenu, shown in Figure B-4, appears.

```

TAB SETTING

      T      T      T      T      T      T      T
1234567890123456789012345678901234567890123456789012...

-----
LEFT / RIGHT      PREV / NEXT POSITION      TAB MOVE TO NEXT TAB STOP
RETURN           BACK TO FIRST POSITION T  EXIT TAB MENU
SPACE           SET / RESET TAB STOP   S  SAVE ALL PARAMETERS
SHIFT-ALT-DELETE DEFAULT VALUES       R  RECALL SAVED VALUES
SHIFT-ALT-SPACE  EXIT SETUP MODE       X  RESET TERMINAL
    
```

Figure B-4 Tab Setting Submenu

Each T in the Tab Setting submenu represents a tab position. To change the tab positions, use the left and right arrow keys or the TAB key to move to the desired location. Then press the space bar to set ("T") or remove (space) tab stops.

To exit the Tab Setting submenu, enter:

T

B.3.2 Function Keys Submenu

To enter the Function Keys submenu, enter the following command from any main menu:

F

When this command is entered, the Function Keys Submenu, shown in Figure B-5, appears.

```

                                FUNCTION KEYS

PF5

PF6

PF7

PF8

PF9

PF10

PF11

PF12

-----
F                                EXIT FUNCTIONS KEYS MENU    | ^ = CTRL |
SHIFT PF5, PF6, ..., PF12  PROGRAM THE SELECTED PF

SHIFT-ALT-DELETE  DEFAULT VALUES          S  SAVE ALL PARAMETERS
SHIFT-ALT-SPACE   EXIT SETUP MODE          R  RECALL SAVED VALUES
                                                X  RESET TERMINAL

```

Figure B-5 Function Keys Submenu

When programming is initiated by pressing a function key, the display beneath the dashed line switches to the following:

```

-----
SHIFT PFx          END PROGRAMMING OF THIS PF          | ^ = CTRL |
SHIFT OTHER PFK   LINK AND END PROGRAMMING

SHIFT-ALT-DELETE  DEFAULT VALUES          S  SAVE ALL PARAMETERS
SHIFT-ALT-SPACE   EXIT SETUP MODE          R  RECALL SAVED VALUES
                                                X  RESET TERMINAL

```

Functions keys can be programmed individually, or they can be linked. When the first key of one or more linked keys is pressed, the string saved in each linked key immediately follows the first, as though all of the linked keys had been pressed. For example, suppose function keys PF5 and PF6 are programmed as follows:

FUNCTION KEYS		
PF5	connect &00003140%080002	PF6
PF6	0035e2!131^M	
.		
.		
.		

This display indicates that PF6 is linked to PF5. When PF5 is pressed, the following string would be echoed and entered:

```
connect &00003140%0800020035e2!131
```

Control characters may be entered by pressing the desired key. They are shown as the control symbol ("^" in the above display) followed by the appropriate letter. The note "^ = CTRL" beneath the dashed line shows the symbol that represents Control.

For example, to enter a Return code, simply press the Return key. The Return code is shown as "^M" in the above display.

Linking keys allows the user to press only one function key to echo more than 24 characters at a time.

To program a function key, follow these steps:

1. Press the SHIFT key and the function key that is to be programmed. Doing so clears the key of any previous programming.
2. Enter up to 24 characters to program that key. Non-ASCII characters, which are not allowed, ring the display station bell.
3. Finish programming in one of two ways:
 - Save the string by pressing SHIFT and the function key being programmed.
 - Save the string and link another function key to the one being programmed by pressing SHIFT and another function key.

When another key is linked, the number of the linked key appears after the key being programmed.

To exit the Function Keys submenu, enter:

```
F
```

B.3.3 Keyboard Definition Submenu

To enter the Keyboard Definition submenu, enter the following command from any main menu:

SHIFT-ALT-RESET

**** NOTE ****

Only the left arrow key, right arrow key, SHIFT-ALT-RESET, SHIFT-ALT-SPACE, and the delete key can be used to give commands while the Keyboard Definition Menu is displayed. All other keys are recognized as defining the displayed key.

SHIFT-ALT-DELETE cannot be used to read default values; use DELETE to retract a single definition, or exit the Keyboard Definition menu and then use SHIFT-ALT-DELETE to restore all default values.

Be careful to define only those keys that require it.

When this command is entered, the Keyboard Definition Menu, shown in Figure B-6, appears.

KEYBOARD DEFINITION

PRESS KEY CORRESPONDING TO: ^0
SCAN CODE: DEFAULT

LEFT / RIGHT : PREV / NEXT CHARACTER
DEL : RETRACT LAST DEFINITION
SHIFT-ALT-RESET : EXIT KEYBOARD DEFINITION
SHIFT-ALT-SPACE : EXIT SETUP MODE
ANY OTHER KEY : DEFINITION OF THE DISPLAYED CHARACTER

Figure B-6 Keyboard Definition Submenu

The menu displays the ASCII code in question. The user must press the key or key sequence that will generate the displayed ASCII code.

More than one key or key sequence can be defined to generate the same ASCII code by defining the code once, then redisplaying that character and defining it a second time, and so on.

When the user presses the appropriate key or key sequence, a scan code representing that key sequence is displayed. The scan code defines the key sequence that will generate the displayed ASCII code. This information is intended for use by service personnel.

To display the desired ASCII code, use the right and left arrow keys. To erase the last key definition, use the delete key. To exit the Keyboard Definition submenu, use SHIFT-ALT-RESET. Pressing any other key defines the pressed key as the character to be echoed for the displayed ASCII code.

When alphabetic characters are defined, both the uppercase and lowercase values of the character are affected.

After specifying the custom values, exit the Keyboard Definition submenu using SHIFT-ALT-RESET. For custom keyboard definition to take effect, the KEYBOARD option of Main Menu 1 must be set to CUSTOM. Before saving the customized values, exit setup mode and check that each customized key echoes the appropriate character. Then enter setup mode and use the S command to save all setup options to EEPROM memory.

Custom keyboard definition is saved for the port from which it was mapped. Each time the display station attached to that port is powered on, the custom keyboard definition is used.

For example, suppose a user needs to interchange the "Q" and "A" on a keyboard. The following steps would accomplish this:

1. Enter the Keyboard Definition submenu by pressing SHIFT-ALT-RESET.
2. Press the right arrow until "A" is displayed.
3. Press the Q key. When the key is pressed, the new scan code for that character appears.
4. Press the right arrow until "Q" is displayed.
5. Press the A key. When the key is pressed, the new scan code for that character appears.
6. Exit the Keyboard Definition submenu by pressing SHIFT-ALT-RESET.
7. Display Main Menu 1, and check that the KEYBOARD option is set to the value CUSTOM.
8. Exit setup mode by pressing SHIFT-ALT-SPACE.
9. Check the customized values. When A is pressed, a "q" is echoed, and vice versa. When SHIFT and A are pressed, a "Q" is echoed, and vice versa.
10. If the keyboard is defined as desired, enter setup mode to save all setup values.

APPENDIX C**CONNECTIONS INVOLVING A GS/1 OR CS/1-X.25**

Connections across GS/1s and connections involving CS/1-X.25s are easily accomplished. Consider Figure C-1, which shows a Public Data Network attached to a local area network, such as Ethernet, via a GS/1. Four types of connections are typically used in such a network configuration:

- PDN terminal-to-LAN host: terminal P on the Public Data Network to host L on the LAN
- LAN terminal-to-PDN host: terminal L on the LAN to host P on the Public Data Network
- PDN host-to-X.25 LAN host: host P on the Public Data Network to host X1 on the LAN
- X.25 host-to-X.25 host: host X1 to host X2, both on the LAN

Each of these types is described in the following subsections, which refer to Figure C-1.

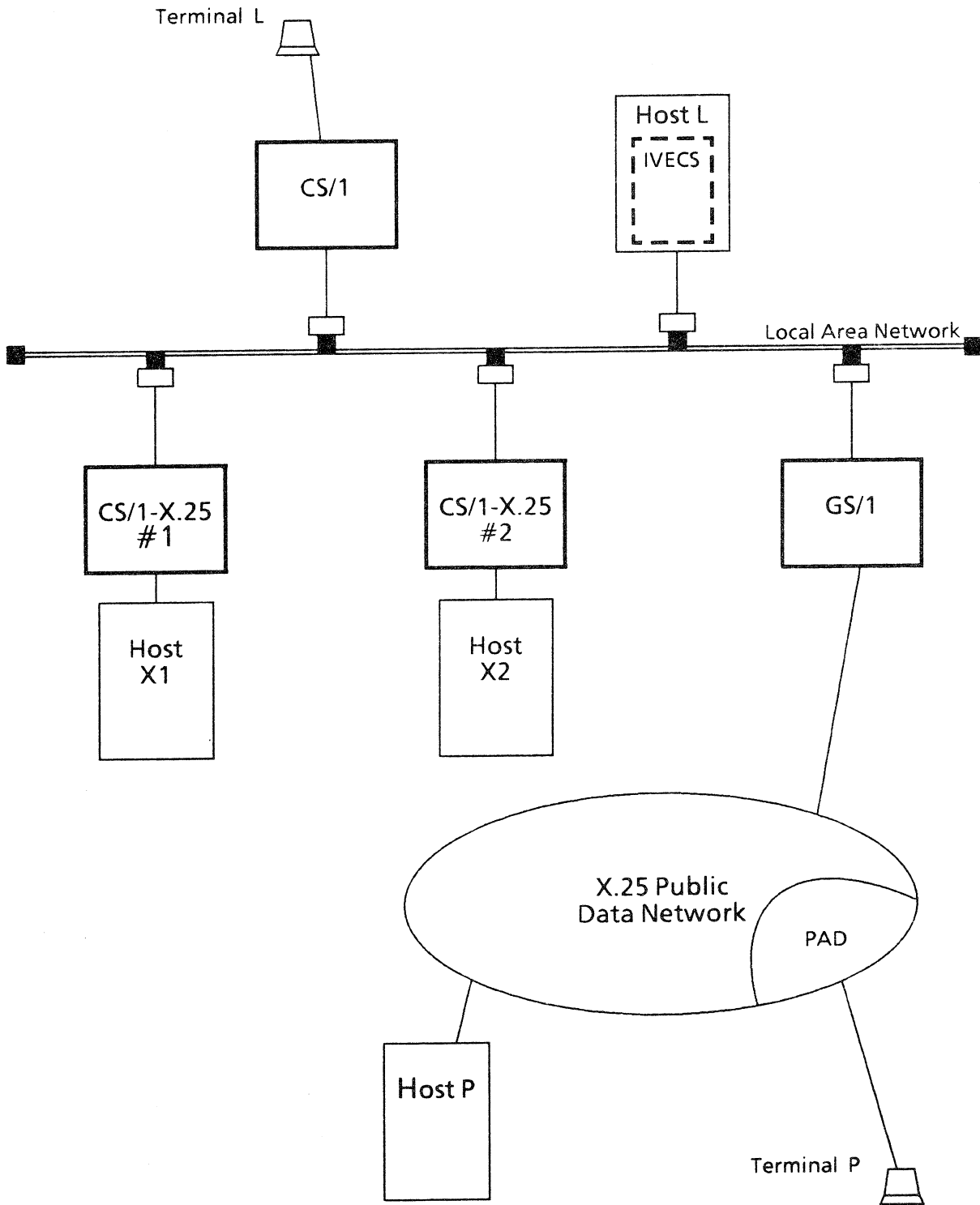


Figure C-1 Network with GS/1 and CS/1-X.25s

C.1 PDN Terminal to LAN Host

A connection from a terminal on a PDN (such as terminal P in Figure C-1), through a GS/1, to a host on a LAN (such as host L) may be established in two ways:

- Using standard Connection Service commands
- Using the X.25 automatic connection service

C.1.1 Using the Connection Service

To establish the connection using standard Connection Service commands, the user at terminal P issues an X.25 call request to the X.25 address of the GS/1. In the X.25 call request, the first octet of the Call User Data Area must equal 1. The GS/1 responds with a Connection Service prompt. To complete the connection to host L, the user would then issue a Connect command.

When the GS/1 receives an X.25 call request, it compares the address received in the request to its record of the X.25 address of the line on which the address was received. If the addresses match and if the Connection Service user interface is enabled on the line, the GS/1 sends the terminal the standard Connection Service prompt. The addresses are considered matching if the Data Network Identification Code and host address fields match (see Sections 3.1.6 and 4.2.1). Non-matching addresses are discussed below.

C.1.2 Using the Automatic Connection Service

The automatic connection service automatically establishes a connection from a terminal device on an X.25 PDN (such as terminal P in Figure C-1) to a device on a LAN (such as host L) without any interaction with the Connection Service. This feature enhances security on incoming calls by preventing users from accessing the Connection Service, and, as a result, from accessing any other devices on the LAN.

To make the service available, the network manager must:

- Establish an X.25 address as a clearinghouse name
- Suppress the Connection Service interface on the affected line

To establish a clearinghouse name, the network manager uses the Name command to establish an X.25 address as a clearinghouse name on the LAN. The address must be the address assigned by the X.25 network to one of the lines connecting the X.25 network with the GS/1. For example, a command with the following format can be used:

```
Name xxxx = %<eeeeeeeeeee>!<rrr>
```

Each element represents the following:

xxxx The X.25 address of any of the X.25 lines to the GS/1
 eeeeeeeeeeee Ethernet address of the IVECS
 rrr IVECS rotary port number

To suppress the Connection Service interface on the affected line, the network manager may use one of the following two methods.

Method 1: Disable the Connection Service interface on the affected line during system generation.

With the interface disabled, the GS/1 supports connections in both directions (i.e., from the LAN to the X.25 network, and from the X.25 network to the LAN). No access to the user interface is possible.

Method 2: Assign the line a different X.25 address during system generation than the address assigned by the X.25 network.

With a false address, the server supports connections from the X.25 network to the LAN. The server cannot, however, support connections from the LAN to the X.25 network unless the X.25 network allows multiple address assignments for a single physical line. If one line can have two X.25 addresses, then a user on the X.25 network connecting to the address known by the Gateway Server can access the user interface, but a user connecting to the other address cannot access the user interface.

To use the automatic connection service, the user issues an X.25 call request to the X.25 address of the GS/1. In the X.25 call request, the first octet of the Call User Data Area must equal 1. When the GS/1 receives an X.25 call request, it compares the address received in the request to its record of the X.25 address of the line on which the address was received. In this case, the address received in the request may or may not match* the GS/1's record of the X.25 address of the line on which the address is received, depending on whether method 1 or method 2 was used to suppress the Connection Service.

If method 1 was used, then the address specified in the request matches the GS/1's record of the X.25 address of the line on which the address is received. However, the Connection Service user interface has been disabled on the line, so the GS/1 cannot send the Connection Service prompt. Instead, the GS/1 Connection Service treats the address in the request as a clearinghouse name; it establishes a connection between the requesting device and the port represented by that clearinghouse name.

If method 2 was used, then the addresses do not match. Regardless of whether the Connection Service user interface has been enabled or disabled on the line, the Connection Service treats the address in the request as a clearinghouse name; it establishes a connection between the requesting terminal and the port represented by that clearinghouse name.

In both cases, if the address is not found in the clearinghouse, the Connection Service rejects the call request.

Clearinghouse names used with this service can also be associated with rotaries.

* The addresses are considered matching if the Data Network Identification Code and host address fields match (see Sections 3.1.6 and 4.2.1).

C.2 LAN Terminal to PDN Host

A connection from a terminal attached to a Communications Server on the LAN (such as terminal L in Figure C-1) to an X.25 host on the Public Data Network (such as host P) is established using standard Connection Service commands.

The network manager can facilitate such a connection using clearinghouse names. To give the user greatest flexibility, the clearinghouse name should specify the GS/1's Ethernet address and rotary port. The requesting user then appends host P's X.25 address to the clearinghouse name.

For example, a command with the following format defines a clearinghouse name that resolves to the GS/1's Ethernet address and rotary port number:

```
Name hostP = %<eeeeeeeeee>!<rrr>
```

Each element represents the following:

hostP Any clearinghouse name

eeeeeeeeee Ethernet address of the GS/1

rrr GS/1 rotary port number

With the clearinghouse name appropriately defined, the user at terminal L issues a connection request, appending host P's X.25 address to the clearinghouse name, for example:

```
connect hostP#1234561234
```

Alternatively, the network manager can restrict the user by including all three elements in the clearinghouse name: the GS/1's Ethernet address, rotary port, and host P's X.25 address.

C.3 PDN Host to X.25 LAN Host

A connection from an X.25 host attached to a Public Data Network (such as host P in Figure C-1) to an X.25 host attached to a CS/1-X.25 on the LAN (such as host X1) is established using the GS/1 call extension feature. Call extension allows a host-to-host connection through the GS/1.

This feature derives its name from the fact that the X.25 call request packet issued by host P contains both the X.25 address of the GS/1 and an "extension" address; when the GS/1 processes such a packet, it automatically establishes a connection to the device indicated by the extension address.

To implement call extension, the network manager must:

- Ensure that the PDN host issues a call request packet in the appropriate format
- Establish an X.25 address as a clearinghouse name
- Configure each affected line as a DTE interface

To ensure the correct call request format, the network manager must configure the PDN host to issue a call request packet with the appropriate destination address and Call User Data Area. The X.25 call request packet has the format shown in Figure C-2.

X.25 Header	Length of Source Addr	Length of Dest Addr	Destination Address	Source Address	Facility	Call User Data Area
-------------	-----------------------	---------------------	---------------------	----------------	----------	---------------------

Figure C-2 Format of X.25 Call Request Packet

The X.25 call request packet must contain the X.25 address of the GS/1 in the destination address field.

The last 16 bytes of the X.25 call request packet are the Call User Data Area. This area must contain the extension. The Call User Data Area has the format shown in Table C-1, where each "c" represents one bit of the extension. The information indicated by "u" and "v" is not needed for call extension.

The digits represented by the "c"s in Table C-1 are defined as a clearinghouse name below.

When the GS/1 receives an X.25 call request packet that conforms to this format, it automatically creates a connection from the source to the destination indicated by the extension.

The presence or absence of the Connection Service user interface on the line has no effect.

<i>Octet</i>	<i>Bits</i>							
	<i>8</i>	<i>7</i>	<i>6</i>	<i>5</i>	<i>4</i>	<i>3</i>	<i>2</i>	<i>1</i>
<i>1</i>	1	1	0	0	0	1	0	0
<i>2</i>	0	0	0	1	0	0	0	0
<i>3</i>	0	0	0	1	c	c	c	c
<i>4</i>	0	0	0	1	z	z	z	z
<i>5</i>	c	c	c	c	c	c	c	c
<i>6</i>	c	c	c	c	c	c	c	c
<i>7</i>	u	u	u	u	u	u	u	u
<i>8</i>	v	v	v	v	v	v	v	v

To establish a clearinghouse name, the network manager defines the digits of the Call User Data Area (represented by the "c"s in Table C-1) as a clearinghouse name that resolves to a port on CS/1-X.25 #1. For example, a command with the following format can be used:

Name 0cccc = &<nnnnn>%<eeeeeeeeeee>!<rrr>

Each element represents the following:

0cccc Appropriate digits from the Call User Data Area, including a leading zero

nnnnn LAN network number

eeeeeeeeeee Ethernet address of CS/1-X.25 #1

rrr CS/1-X.25 #1 rotary port number

To configure each affected line as a DTE interface, the network manager must use system generation. System generation is described in the *Network Management Guide*.

C.4 X.25 Host to X.25 Host

A connection can be established from an X.25 host attached to a CS/1-X.25 (such as host X1 in Figure C-1) to another X.25 host attached to a CS/1-X.25 (such as host X2), both on the LAN.

To implement this type of connection, the network manager must:

- Ensure that the calling X.25 host issues a call request packet in the appropriate format
- Establish a clearinghouse name that resolves to host X2's Ethernet address and rotary port number

To ensure the correct call request format, the network manager must configure the PDN host to issue a call request packet with the appropriate destination address. The X.25 call request packet has the format shown in Figure C-2, Section C.3.

The destination address field of the X.25 call request packet must contain the X.25 address of the GS/1.

To establish a clearinghouse name the network manager defines the ASCII equivalent of the contents of the destination address field as a numeric clearinghouse name that resolves to a port on CS/1-X.25 #2.

For example, a command with the following format can be used:

```
Name dddd = %<eeeeeeeeee>!<rrr>
```

Each element represents the following:

- dddd Contents of the destination address field, in ASCII
- eeeeeeeeee Ethernet address of CS/1-X.25 #2
- rrr CS/1-X.25 #2 rotary port number

INDEX

- Access control, 2-11, 2-16. See also
 - AccessGroup parameter, AccessWord parameter
 - access group passwords, 2-22
- AccessGroup parameter, 2-16, 3-17, 4-6, 4-7, 4-25, 4-27, 4-34, 4-44
- AccessWord parameter, 2-16, 3-17, 4-6, 4-7, 4-25, 4-27, 4-34, 4-44
- Address list, 3-9, 3-10
- Asynchronous devices, 2-5
- Asynchronous interfaces, 2-5, 2-6
- Asynchronous ports, 3-21
- At sign (@), 3-29
- Audit trail, 2-17, 4-24
- AUDITServerAddr parameter, 2-17, 4-23, 4-24
- AUTODisconnect parameter, 4-6, 4-7, 4-26, 4-34
- Autolisten interval, 3-29
- AUTOLogoff parameter, 4-6, 4-7
- Automatic connection service, 2-21, C-4
- Automatic disconnect interval, 2-7
- BAud parameter, 3-38, 3-48, 4-11, 4-12, 4-47
- Bisynchronous interface, 2-5, 2-6
- Bit-synchronous interface, 2-5
- BootServerAddr parameter, 2-17, 4-23, 4-24
- Break key, 3-22
- BReakAction parameter, 3-45, 4-8, 4-15, 4-16, 4-20, 4-26, 4-27, 4-34, 4-35, 4-38, 4-44, 4-46
- BReakChar parameter, 3-22, 4-8, 4-15, 4-16, 4-34, 4-39, 4-41
- Breaks
 - in-band, 3-56
 - out-of-band, 3-56
- Broadcast address, 2-17, 3-16, 3-45
 - TCP, 3-16
 - XNS, 3-16
- Broadcast command, 3-16
- Broadcast messages, 4-9
- BSPad, 4-11, 4-12, 4-37, 4-46, 4-48
- BSDelay, 4-12
- BUffersize parameter, 4-6, 4-7, 4-26
- Call extension, 2-21, C-6
- Call queuing
 - clearinghouse names, 3-18
 - destination port and, 2-16
 - Listen command, 2-17
 - requesting port and, 2-17
 - reserved state, 3-29
 - RESume command, 2-16, 3-18
 - session number, 3-18
- Call user data area, C-3, C-4, C-6
 - format of, C-7
- Carriage control characters, 3-7
- Character-synchronous devices, 2-5
- Characters, 3-6, 3-8
 - special, 3-7, 3-9
- Clearinghouse names, 2-16, 2-21, 3-17, 3-50, 3-51, 4-24, 4-43
 - assigning, 3-30
 - deleting, 3-58
 - domain name, 3-9
 - establishing, 3-10
 - local name, 3-9
 - organization name, 3-9
 - using, 3-10
- Command format
 - address field, 3-1
 - keyword, 3-1
 - parameters, 3-1
 - verb, 3-1
- Command mode, 2-9, 3-17, 3-29, 3-40, 4-1, 4-2, 4-8, 4-16, 4-18, 4-21, 4-25, 4-27, 4-35, 4-40, 4-42, 4-44
- Commands, 3-14 through 3-60
 - abbreviation of, 3-4
 - Broadcast, 3-16
 - Connect, 2-7, 3-17, 3-22
 - DEFine, 3-21, 3-33, 4-8, 4-35
 - DEQueue, 3-25
 - DisConnect, 3-26
 - DO, 3-22, 3-27
 - Echo, 3-28
 - Listen, 3-29, 4-26
 - Name, 3-10, 3-13, 3-30, 3-41, C-3
 - Pause, 3-22, 3-33
 - ReaD, 3-34, 3-47, 4-2, (figure) 4-3

Commands (continued)

REMOTE, 3-22, 3-36
 REMoteSET, 2-4, 3-38
 REMoteSHow, 3-39
 RESume, 3-18, 3-22, 3-40, 3-55
 ROtary, 3-13, 3-31, 3-41
 SAve, 3-43, 3-47, 4-2, (figure) 4-3
 SET, 2-4, 2-8, 3-2, 3-6, 3-45, 4-1, 4-2,
 (figure) 4-3, 4-26
 SETDefault, 2-4, 2-8, 3-6, 3-10, 3-47,
 4-1, 4-2, (figure) 4-3, 4-26
 SHow, 3-22, 3-28, 3-33, 3-49
 SHow ADDRess, 3-50
 SHow AllSessions, 3-50
 SHow AttachedNets, 3-50
 SHow CHNames, 3-9, 3-50, 3-51
 SHow CONFigurations, 3-51
 SHow DATE, 3-51
 SHow DefaultParameters, 3-51
 SHow GlobalPARAmeters, 3-51
 SHow GRoupPassWords, 3-51
 SHow InternetPorts, 3-41, 3-51, 3-53
 SHow LineStatus, 3-52
 SHow MACros, 3-22, 3-52
 SHow NAMES, 3-12, 3-51, 3-52
 SHow NetMap, 3-52
 SHow PARAmeters, 3-52
 SHow RemoteNets, 3-53
 SHow ROtaries, 3-41, 3-53
 SHow SECURITYSTATistics, 3-53
 SHow SESSions, 3-53
 SHow STATistics, 3-22, 3-53, 3-60
 SHow VERSion, 2-24, 3-53
 SHow VirtualPorts, 3-53
 SHow X25Addresses, 3-53
 SHow X25Connection, 3-53
 SWitch, 3-55
 syntax, 3-1, 3-5
 Transmit, 3-56
 UNDefine, 3-22, 3-57
 UNName, 3-30, 3-58
 UNSave, 3-59
 ZeroStats, 3-60
 Configuration files, 2-22
 deleting, 3-59
 Configuration parameters. See Parameters
 Configuration tables, 3-43
 named, 3-34
 numbered, 3-34
 Connect command, 2-7, 3-17

Connect command (continued)

in macros, 3-22
 CONNectAudit parameter, 4-23, 4-24
 Connection Service
 access to, 2-1
 features, 2-5
 operation of, 2-1 through 2-3
 overview, 2-1
 software configuration, 2-1, 2-4
 Connection Service commands. See
 Commands
 Connections
 among server types, (table) 2-7
 creating, 2-1 through 2-3, 2-7, 3-17,
 3-22
 Control characters, 3-7 through 3-9
 CRDelay, 4-11
 CRPad parameter, 4-11, 4-37, 4-46
 CS/1 with SIO-3270, B-1 through B-14
 CS/1-X.25, 2-19 through 2-21 (figure), C-1,
 (figure) C-2
 Data Transfer mode, 2-9, 3-17, 3-29, 3-40,
 4-1, 4-2, 4-9, 4-16, 4-18, 4-19, 4-27,
 4-40, 4-41, 4-42
 DataBits parameter, 3-48, 4-11, 4-12, 4-37
 DataForward parameter, 4-15, 4-16, 4-20,
 4-27, 4-39, 4-40, 4-45
 DATE parameter, 4-23, 4-24, 4-43
 DefaultGateway parameter, 4-23, 4-24
 DEFine command, 3-21, 3-33, 4-8, 4-35
 Deleting
 configuration files, 3-59
 names, 3-58
 DEQueue command, 3-25
 Destination port, call queuing and, 2-16
 DeVice parameter, 4-6, 4-8, 4-26, 4-34
 DisConnect command, 3-26
 DisconnectAction parameter, 4-15, 4-17
 Disk drive, internal, 3-30
 Diskless systems, 2-22
 DO command, 3-22, 3-27
 DO TIMING option, 4-16
 DOrain parameter, 4-23, 4-24, 4-43
 DUplex parameter, 4-11, 4-12
 Echo command, 3-28
 ECHOData parameter, 4-15, 4-17, 4-20,
 4-27, 4-38, 4-41, 4-45
 ECHOMask parameter, 4-15, 4-17, 4-27
 ECM parameter. See Connect command

- ECMChar parameter, 3-17, 3-45, 4-8, 4-15, 4-18, 4-34, 4-38, 4-41, 4-45
- Editing parameters
 - asynchronous, 4-21, 4-22
 - GS/1, 4-42
 - 3270, 4-21, 4-22
- End of Message (EOM) parameter, 3-56, 4-15, 4-18, 4-39, 4-41
- ERase parameter, 4-21, 4-42, 4-48
- Error messages, A-1 through A-18. Also see individual commands
- ERRorAudit parameter, 4-23, 4-24
- Ethernet addresses
 - network address field, 3-8
 - specifying, 3-8
- Ethernet network, C-1
- FFDelay parameter, 4-11, 4-12
- FFPad parameter, 4-11, 4-12, 4-37, 4-46, 4-48
- Filenames, alphanumeric, 3-34
- FlowControlFrom parameter, 4-14, 4-15, 4-18, 4-38, 4-40, 4-45
- FlowControlTo parameter, 4-14, 4-15, 4-18, 4-38, 4-40, 4-47
- FlushVC parameter, 4-15, 4-19, 4-46
- Form effectors, (table) 3-7
- Global Network Manager privilege level, 2-11
- Global parameters
 - asynchronous, 4-23 through 4-25
 - GS/1, 4-43, 4-44
 - 3270, 4-23 through 4-25
- Global rotary, 2-14, 3-9, 3-10, 3-17
- GlobalPassWord parameter, 4-23, 4-24, 4-44
- GroupxPasswd parameter, 2-16, 4-23, 4-25, 4-44
- GS/1
 - call extension, C-6
 - configuring, 4-32 through 4-48
 - connections, 2-19 through 2-21 (figure), C-1 through C-7
 - virtual ports, 3-21
- Help facility, 2-12, 3-2, 3-36
 - typical dialogue, (figure) 2-12
- Host configuration, asynchronous, 4-26
- Hybrid interfaces, 2-6
- IdleTimer parameter, 4-15, 4-19, 4-20, 4-39, 4-41, 4-45
- Initialization macros, 4-8, 4-36
- InitMacro parameter, 2-13, 3-21, 3-23, 4-6, 4-8, 4-33, 4-35
- InterAction parameter, 3-16, 3-22, 3-27, 3-28, 4-6, 4-8, 4-26, 4-33, 4-34, 4-35, 4-46
- Internet addresses, 3-11, 3-13
- Internet names, 3-11, 3-12
 - assigning, 3-30
 - deleting, 3-58
 - establishing, 3-13
 - Internet Name Service, 3-13
 - using, 3-13
- Internetwork Bridges, 2-5
- IRMA board, B-1
- LFDelay, 4-11, 4-12
- LFInsertion parameter, 4-15, 4-19, 4-20, 4-27, 4-38, 4-40, 4-41, 4-44, 4-48
- LFPad parameter, 4-11, 4-48
- LineERase parameter, 4-21, 4-42, 4-48
- LinePRotocol parameter, 4-11, 4-12, 4-27
- Listen command, 3-29, 4-26
- Listening mode, 2-9, 2-17, 3-17, 3-26, 4-8, 4-27, 4-35
- Local and Global Rotaries, difference between, (figure) 2-15
- Local area network, C-1 through C-8
- Local Network Manager privilege level, 2-11
- LocalEDiting parameter, 4-21, 4-42, 4-48
- LocalPassWord parameter, 4-23, 4-25, 4-44
- Logical connection. See Connection
- Logical names
 - clearinghouse, 2-14, 2-15, 3-30
 - deleting, 3-58
 - internet, 2-14, 3-30
- LogoffStr parameter, 4-23, 4-25
- LongBReakAction parameter, 4-15, 4-20, 4-28
- Macro files, 2-22
- Macros, 3-2, 4-8, 4-36
 - creating, 3-21
 - deleting, 3-22, 3-57
 - displaying, 3-22
 - endless loop, 3-22
 - escaping, 3-22
 - executing, 3-22

Macros (continued)

- initialization, 4-6, 4-8, 4-35
- names, 3-21
- port initialization, 2-6, 2-13
- prompt for, 3-21
- system initialization, 2-13, 3-21, 3-23
- text of, 3-21
- MaxSessions parameter, 4-6, 4-9, 4-33, 4-35
- MOMode parameter, 3-1, 4-15, 4-20, 4-27, 4-38, 4-42
- Modem control lines, asynchronous, 4-29 through 4-31
- Modems, 4-7, 4-29 through 4-31, 4-34
- Modes of operation, (figure) 2-10
 - Command, 2-9, 3-17, 3-29, 3-40, 4-1, 4-2, 4-8, 4-16, 4-18, 4-21, 4-25, 4-27, 4-35, 4-40, 4-42, 4-44
 - Data Transfer, 2-9, 3-17, 3-29, 3-40, 4-1, 4-2, 4-9, 4-16, 4-18, 4-19, 4-27, 4-40, 4-41, 4-42
 - Listening, 2-9, 2-17, 3-17, 3-26, 4-8, 4-27, 4-35
- Name command, 3-10, 3-13, 3-30, 3-41, C-3
- Named configuration files, 3-34
- NCS/1. See Network Control Servers
- NCS/150. See Network Control Servers
- Network with GS/1, (figure) C-2
- Network bootstrap, required PROMs, 2-22 through 2-23
- Network Control Servers, 2-17, 3-21
 - access groups, 2-22
 - client servers, 3-10
 - configuration files, 2-22
 - macro files, 2-22
 - NCS/1, 3-11
 - NCS/150, 3-10 through 3-11
 - passwords, 2-22
- Network management
 - functions, 2-18, 3-17
 - port (port 136), 2-18, 3-17, 3-18
 - reports, 3-53
- NMPrompt parameter, 4-23, 4-25, 4-44
- Numbers, conventions, 3-6
- Organization parameter, 4-23, 4-24, 4-43
- Parameter tables, 4-1, 4-26
- Parameters, 2-16
 - AccessGroup, 2-16, 3-17, 4-6, 4-7, 4-25, 4-27, 4-34, 4-44

Parameters (continued)

- AccessWord, 2-16, 3-17, 4-6, 4-7, 4-25, 4-27, 4-34, 4-44
- AUDITServerAddr, 2-17, 4-23, 4-24
- AUTODisconnect, 4-6, 4-7, 4-26, 4-34
- AUTOLogoff, 4-6, 4-7
- BAud, 3-38, 3-48, 4-11, 4-12, 4-47
- BootServerAddr, 2-17, 4-23, 4-24
- BRreakAction, 3-45, 4-8, 4-15, 4-16, 4-20, 4-26, 4-27, 4-34, 4-35, 4-38, 4-44, 4-46
- BRreakChar, 3-22, 4-8, 4-15, 4-16, 4-34, 4-39, 4-41
- BSDelay, 4-12
- BSPad, 4-11, 4-12, 4-37, 4-46, 4-48
- BUffersize, 4-6, 4-7, 4-26
- changing, 3-45, 3-47, 4-1
- CONNectAudit, 4-23, 4-24
- CRDelay, 4-11
- CRPad, 4-11, 4-37, 4-46
- DataBits, 3-48, 4-11, 4-12, 4-37
- DataForward, 4-15, 4-16, 4-20, 4-27, 4-39, 4-40, 4-45
- DATE, 4-23, 4-24, 4-44
- DefaultGateway, 4-23, 4-24
- DeVice, 4-6, 4-8, 4-26, 4-34
- DISconnectAction, 4-15, 4-17
- DOMain, 4-23, 4-24, 4-43
- DUPlex, 4-11, 4-12
- ECHOData, 4-15, 4-17, 4-20, 4-27, 4-38, 4-41, 4-45
- ECHOMask, 4-15, 4-17, 4-27
- ECMChar, 3-17, 3-45, 4-8, 4-15, 4-18, 4-34, 4-38, 4-41, 4-45
- EOM, 3-56, 4-15, 4-18, 4-39, 4-41
- ERase, 4-21, 4-42, 4-48
- ERRorAudit, 4-23, 4-24
- FFDelay, 4-11, 4-12
- FFPad, 4-11, 4-12, 4-37, 4-46, 4-48
- FlowControlFrom, 4-14, 4-15, 4-18, 4-38, 4-40, 4-45
- FlowControlTo, 4-14, 4-15, 4-18, 4-38, 4-40, 4-47
- FlushVC, 4-15, 4-19, 4-46
- GlobalPassWord, 4-23, 4-24, 4-44
- GroupxPasswd, 2-16, 4-23, 4-25, 4-44
- IdleTimer, 4-15, 4-19, 4-20, 4-39, 4-41, 4-45
- InitMacro, 2-13, 3-21, 3-23, 4-6, 4-8, 4-33, 4-35

- Parameters (continued)
 - InterAction, 3-16, 3-22, 3-27, 3-28, 4-6, 4-8, 4-26, 4-33, 4-34, 4-35, 4-46
 - LFDelay, 4-11, 4-12
 - LFInsertion, 4-15, 4-19, 4-20, 4-27, 4-38, 4-40, 4-41, 4-44, 4-48
 - LFPad, 4-11, 4-48
 - LineERase, 4-21, 4-42, 4-48
 - LinePRotocol, 4-11, 4-12, 4-27
 - LocalEDiting, 4-21, 4-42, 4-48
 - LocalPassWord, 4-23, 4-25, 4-44
 - LogoffStr, 4-23, 4-25
 - LongBReakAction, 4-15, 4-20, 4-28
 - MaxSessions, 4-6, 4-9, 4-33, 4-35
 - MOde, 3-1, 4-15, 4-20, 4-27, 4-38, 4-42
 - NMPrompt, 4-23, 4-25, 4-44
 - Organization, 4-23, 4-24, 4-43
 - PARlty, 3-48, 4-11, 4-13
 - PermanentVC, 2-6, 2-7, 4-6, 4-9
 - PrimaryNS, 3-13, 4-23, 4-25
 - PRiilege, 4-6, 4-10, 4-33, 4-36
 - PROMPt, 4-23, 4-25, 4-44
 - ReprintLine, 4-21, 4-42, 4-48
 - saving, 3-43
 - SecondaryNS, 4-23, 4-25
 - specifying values of, 3-6
 - StopBits, 3-48, 4-11, 4-13
 - string values, 3-6
 - TabDelay, 4-11, 4-12
 - TabPad, 4-11, 4-12
 - UseDCDout, 4-11, 4-13, 4-29, (figure) 4-30, 4-31
 - UseDTRin, 4-11, 4-14, 4-18, 4-29, 4-31
 - VERBatim, 4-22, 4-43
 - WelcomeString, 4-23, 4-25, 4-44
 - WordERase, 4-22, 4-43
 - XOFF, 4-15, 4-20
 - XON, 4-15, 4-20
 - xxDelay, 4-11, 4-12
 - xxPad, 4-11, 4-12, 4-37, 4-46, 4-48
- PARlty parameter, 3-48, 4-11, 4-13
- Passwords, 2-16, 3-23
- Pause command, 3-33
 - in macros, 3-22
- PermanentVC parameter, 2-6, 2-7, 4-6, 4-9
- Physical address fields
 - Ethernet addresses, 3-8
 - network address, 3-8
 - optional number, 3-8
 - port number, 3-8
- Physical ports, 3-11
- Port configuration
 - asynchronous server, 4-4 through 4-31
 - GS/1, 4-32 through 4-48
 - overview, 4-1 through 4-3
 - parameters, 4-1 through 4-48
 - sample asynchronous, 4-26 through 4-31
 - 3270 server, 4-4 through 4-31
- Port initialization macros, 2-6, 2-13
- Port numbers, 3-41
- Port 136, 2-18, 3-17, 3-18
- Port physical parameters
 - asynchronous, 4-11 through 4-14
 - GS/1, 4-37
- Port problems, 4-26 through 4-28
- Port transmission parameters
 - asynchronous, 4-6 through 4-10
 - bit-synchronous, 4-6 through 4-10
 - character-synchronous, 4-6 through 4-10
 - GS/1, 4-33 through 4-36
 - 3270, 4-6 through 4-10
- Ports, physical vs. virtual, 2-8
- PrimaryNS parameter, 3-13, 4-23, 4-25
- Privilege levels, 4-10, 4-36
 - Global Network Manager, 2-11, 3-21
 - Local Network Manager, 2-11
 - User, 2-11
- PRiilege parameter, 4-6, 4-10, 4-33, 4-36
- PROMPt parameter, 4-23, 4-25, 4-44
- Protocol families, TCP/IP and XNS, 2-5
- Protocol transparent servers, 2-5
- Public Data Network (PDN), 2-15, 2-19, C-1 through C-8
- Q. See Connect command
- Queued connection, 3-40
- ReaD command, 3-34, 3-47, 4-2, (figure) 4-3
- Release numbers
 - firmware, 2-24, 2-26
 - software, 2-24, 2-25
- REMOTE command, 3-36
 - in macros, 3-22
- Remote mode, 2-5, 3-36
- REMOteSET command, 2-4, 3-38
- REMOteSHow command, 3-39
- ReprintLine parameter, 4-21, 4-42, 4-48
- RESume command, 3-18, 3-40, 3-55
 - in macros, 3-22

- Rotaries, (figure) 2-15
 - global, 2-14, 3-9, 3-10, 3-17
 - local, 2-14, 3-10
 - numbers, 3-10
- ROtary command, 3-13, 3-31, 3-41
- Rotary numbers, 3-10
 - adding, 3-41
 - assigning, 3-41
 - removing, 3-41
- SAve command, 3-43, 3-47, 4-2, (figure) 4-3
- SecondaryNS parameter, 4-23, 4-25
- Security, 2-16, 2-21, 4-7, 4-25, 4-34
- Servers
 - CS/1. asynchronous, 2-22
 - CS/1. bisynchronous, 2-22
 - CS/1. bit-synchronous, 2-22
 - CS/1-TCP, 2-22
 - CS/1 with SIO-3270, 2-22, B-1 through B-14
 - CS/100, asynchronous, 2-22
 - CS/100, bisynchronous, 2-22
 - CS/100-TCP, 2-22
 - CS/200, 2-22
 - IVECS, 2-22
 - NCS, 2-22. See also Network Control Servers
 - TCP, 4-4, 4-6, 4-7, 4-16, 4-19, 4-20, 4-23, 4-24
- Session editing parameters
 - asynchronous, 4-21, 4-22
 - GS/1, 4-42, 4-43
 - 3270, 4-21, 4-22
- Session number, 3-6
- Session transmission parameters
 - asynchronous, 4-15 through 4-20
 - GS/1, 4-38 through 4-41
- Sessions
 - active, 3-38
 - management, 2-7
 - number, 3-6
 - queued, 3-40
- SET command, 2-4, 2-8, 3-2, 3-6, 3-45, 4-1, 4-2, (figure) 4-3, 4-26
- SETDefault command, 2-4, 2-8, 3-6, 3-10, 3-47, 4-1, 4-2, (figure) 4-3, 4-26
- Setup mode, B-1 through B-14
- SHoW ADDRess command, 3-50
- SHoW AllSessions command, 3-50
- SHoW AttachedNets command, 3-50
- SHoW CHNames command, 3-9, 3-50, 3-51
- SHoW command, 3-28, 3-33, 3-49
 - in macros, 3-22
 - keywords, 3-49
- SHoW CONFIgurations command, 3-51
- SHoW DATE command, 3-51
- SHoW DefaultParameters command, 3-51
- SHoW GlobalPARAmeters command, 3-51
- SHoW GRoupPassWords command, 3-51
- SHoW InternetPorts command, 3-41, 3-51, 3-53
- SHoW InternetServers command, 3-51
- SHoW LineStatus command, 3-52
- SHoW MACros command, 3-22, 3-52
- SHoW NAMES command, 3-12, 3-51, 3-52
- SHoW NetMap command, 3-52
- SHoW PARAmeters command, 3-52
- SHoW RemoteNets command, 3-53
- SHoW ROTaries command, 3-41, 3-53
- SHoW SECuritySTATistics command, 3-53
- SHoW SESSions command, 3-53
- SHoW STATistics command, 3-22, 3-53, 3-60
- SHoW VERSion command, 2-24, 3-53
- SHoW VirtualPorts command, 3-53
- SHoW X25Addresses command, 3-53
- SHoW X25Connection command, 3-53
- SNA host, 2-5, 2-6
- Special characters, 3-7, 3-9
 - default local editing characters, (table) 3-3
 - keyboard symbols, (table) 3-2
 - SET command and, 3-2
- StopBits parameter, 3-48, 4-11, 4-13
- Strings, 3-6
 - conventions, 3-7
- SWitch command, 3-55
- Syntax notation, 3-5
- System initialization macros, 2-13, 3-21, 3-23
- TabDelay parameter, 4-11, 4-12
- TabPad parameter, 4-11, 4-12
- TCP addresses
 - class, 3-11 through 3-12
 - format, (table) 3-11
 - Internet address, 3-11 through 3-12
 - internet name, 3-11 through 3-12
 - number, 3-11 through 3-12
 - physical port, 3-11 through 3-12
 - port number, 3-12
 - specifying, 3-11 through 3-12

- TCP servers, 4-4, 4-6, 4-7, 4-16, 4-19, 4-20, 4-23, 4-24
- Telnet, 4-16
- Terminal configuration, asynchronous, 4-26 through 4-28
- Third-party connection, 2-6, 2-7
- 3270 setup mode, B-1 through B-14
 - commands, B-1
 - function keys, B-11, B-12
 - IRMA board, B-1
 - keyboard definition, B-13, B-14
 - main menu 1, B-3 through B-5
 - main menu 2, B-6, B-7
 - main menu 3, B-8, B-9
 - main menus, B-2
 - submenus, B-10
 - tab setting, B-10
- Timeout failure, 3-37
- Transmit command, 3-56
- UNDefine command, 3-22, 3-57
- UNName command, 3-30, 3-58
- UNSave command, 3-59
- UseDCDout parameter, 4-11, 4-13, 4-29, (figure) 4-30, 4-31
- UseDTRin parameter, 4-11, 4-14, 4-18, 4-29, 4-31
- User privilege level, 2-11
- VERBatim parameter, 4-22, 4-43
- Vertical bars, 4-2
- Virtual circuit, 2-1 through 2-3
 - establishing, (figure) 2-2
- Virtual ports, X.25 interface and, 2-8
- WelcomeString parameter, 4-23, 4-25, 4-44
- Wildcard character, asterisk (*), 3-9
- WordERase parameter, 4-22, 4-43
- X.25 addresses, 3-8, C-3
 - remote connection to, 3-17
- X.25 automatic connection service
 - Data Network Identification Code, C-3
 - false address, C-4
 - X.25 address, 3-8, C-3
- X.25 call request, C-3
 - format, C-6
- X.25 connections, 2-19 through 2-21 (figure), C-1 through C-8
- X.25 interface, 2-6
 - automatic connection service, 2-5, 2-21, C-3
 - virtual ports and, 2-8
- X.3 protocol, 4-45
- XOFF parameter, 4-15, 4-20
- XON parameter, 4-15, 4-20
- xxDelay parameter, 4-11, 4-12
- xxPad parameter, 4-11, 4-12, 4-37, 4-46, 4-48
- ZeroStats command, 3-60

Bridge Communications, Inc.
2081 Stierlin Road
Mountain View, CA 94043
Telephone: 415/969-4400