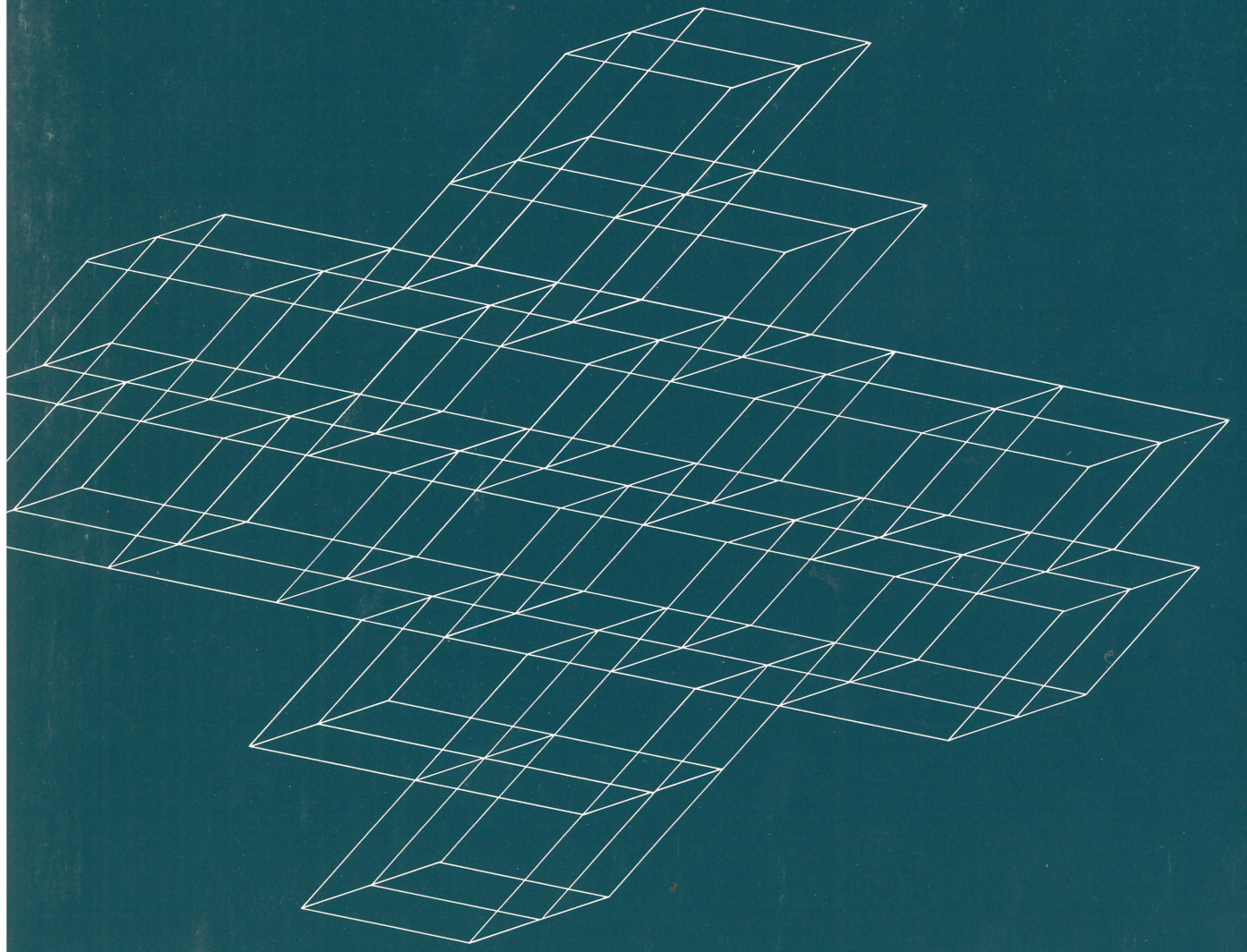
Bridge Communications Inc.

Network Management Guide



BRIDGE COMMUNICATIONS, INC.

NETWORK MANAGEMENT GUIDE

09-0067-00

March 1986

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

** ACKNOWLEDGMENTS **

Bridge Communications, Inc., would like to acknowledge the assistance of Citibank Inc., N.A., in the preparation of this publication.

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.

Part Number	Date	Description	Affected Pages
09-0067-00	03/86	First Release	All

PREFACE

This guide is grouped into five major sections and four appendices:

Section 1.0 Introduction: Describes the purpose and scope of this guide, the network manager's role, and the types of network management.

Section 2.0 Network Installation and Validation: Describes guidelines and instructions for installing and testing a Local Area Network.

Section 3.0 Network Configuration: Describes software configuration, access control, clearinghouse and internet names, and macros.

Section 4.0 Network Operation: Describes the documentation that the network manager should maintain, preventive maintenance, and troubleshooting.

Section 5.0 Network Planning: Describes guidelines and procedures for adding servers, for segmenting the network with a GS/4, for providing redundancy, and for ensuring network system compatibility.

Appendix A Describes system generation.

Appendix B Explains the port configuration parameters and provides sample configurations for various kinds of devices.

Appendix C Describes the diskette duplicating, diskette formatting, and memory dump procedures.

Appendix D Provides a list of error messages generated by the MP and MCPU monitors.

REFERENCES

The following publications describe the Bridge Communications, Inc., product line:

[1] *Product Line Overview* (Bridge Communications, Inc.)

[2] *Software Technical Reference Manual* (Bridge Communications, Inc.)

[3] *Series/1 Planning and Installation Guide* (Bridge Communications, Inc.)

[4] *Series/100 Planning and Installation Guide* (Bridge Communications, Inc.)

[5] *Series/200 Planning and Installation Guide* (Bridge Communications, Inc.)

[6] *IVECS Planning and Installation Guide* (Bridge Communications, Inc.)

[7] *NCS/1 Installation and Operation Guide* (Bridge Communications, Inc.)

[8] *NCS/150 Installation and Operation Guide* (Bridge Communications, Inc.)

[9] *CS/1-SNA Support Guide* (Bridge Communications, Inc.)

[10] *Connection Service User's Guide* (Bridge Communications, Inc.)

[11] *Cable Guide* (Bridge Communications, Inc.)

The following publications describe Ethernet, the Xerox Network System protocols, the TCP/IP protocols, and X.25 standards:

[12] *The Ethernet, A Local Area Network: Data Link Layer and Physical Layer Specifications,* Version 1.0 (Digital Equipment Corporation, Intel Corporation, and Xerox Corporation, 1980)

[13] *The Ethernet, A Local Area Network: Data Link Layer and Physical Layer Specifications,* Version 2.0 (Digital Equipment Corporation, Intel Corporation, and Xerox Corporation, 1980)

[14] *Internet Transport Protocols,* XSIS 028112 (Xerox Corporation, 1981)

[15] *Courier: The Remote Procedure Call Protocol,* XSIS 038112 (Xerox Corporation, 1981)

[16] *TCP/IP Internet Protocol Transition Workbook* (SRI International, 1982)

[17] *Draft Revised CCITT Recommendation X.25,* COM VII No. 489 (CCITT Study Group VII, 1980)

[18] *Telenet X.25 Documentation Service,* PE-xx.001.04B (GTE Telenet Communication Corporation, 1979)

The following publications describe network management techniques:

[19] Leong, John. "Nuts-and-bolts Guide to Ethernet Installation and Interconnection," *Data Communications* (September 1985), 267-276.

[20] Moore, Connie, and McAuliffe, Rob. "An Effective Way to Design and Implement a Local Network," *Data Communications* (October 1985), 267-278.

CONTENTS

TABLES

FIGURES

1.0 INTRODUCTION

A network manager should be designated to oversee and maintain the network at every Local Area Network (LAN) installation. This publication describes the responsibilities of the network manager and provides instructions, guidelines, and suggestions for managing a Bridge LAN.

This publication incorporates the experience gained by Bridge Communications, Inc., and its customers in the installation and management of over 350 LANs. The material is divided into sections that describe the four stages of network operation:

- *Network Installation and Validation.* Section 2.0 describes the steps required for installing and validating all types of servers and the Ethernet itself, including tap and transceiver installation. Use this section as a guide to installation and validation information in this and other Bridge manuals.
- *Network Configuration.* Section 3.0 describes guidelines for customizing a network, including software configuration, access control, naming, and macros.
- *Network Operation.* Section 4.0 describes the network management reports, preventive maintenance, and troubleshooting.
- *Network Planning.* Section 5.0 describes adding servers, segmenting networks, compatibility, and redundancy.

Sections 2.8, 3.5, and 4.6 include samples of control documents pertaining to that section's topic.

This publication includes references to specific information in other Bridge publications where appropriate.

1.1 The Network Manager's Role

Every Local Area Network requires an individual or group of individuals to manage the network. Managing the network includes the following responsibilities:

- Installing and configuring the network, including
  - installing and testing the network components
  - configuring port and session parameters
  - assigning clearinghouse and internet names
  - defining security and access restrictions
  - installing revisions and upgrades
- Maintaining the network, including
  - setting up and implementing procedures for problem reporting, configuration changes and additions, and server backup
  - monitoring network performance and statistics to detect potential problems before network users are affected
  - centralizing problem reporting and troubleshooting and acting as the liaison with Bridge
  - managing spare components
- Implementing security features and procedures, including
  - restricting access to network resources and network management commands and operations
  - protecting sensitive resources
  - detecting attempts to gain unauthorized access
- Setting up and maintaining network management documentation
- Maintaining an operation log
- Planning for network growth and evolution

Monitoring error and traffic rates prevents problems and helps the manager plan for growth. For example, one network manager was responsible for a large LAN consisting of several segments connected by repeaters. By monitoring Ethernet errors over a period of time, the manager recognized that all of the servers on one segment had consistently higher error rates. By tracking the problem to a faulty repeater, the problem was corrected before it caused a lengthy interruption in service.

The justification for designating a network manager becomes increasingly apparent as the network grows. A single individual may be able to manage a LAN consisting of a few Communications Servers, a minicomputer, and several personal computers sharing a disk and printer. But when the network is used to share computing resources among hundreds or thousands of users, several individuals must oversee the daily operation of the network. If a LAN is spread among many buildings or encompasses many large departments, a network manager should be appointed for each building or department, with one person overseeing the entire operation.

1.2 Types of Network Management

Network management can be server-based, NCS/150-based, or NCS/1-based, or based on some combination of these three. Each type of network management is described below.

Server-based

Each Communications Server offers the following services:

- Local bootstrap service
- Local configuration and macro file service
- Clearinghouse service distributed among all servers on the network
- Network management reports

Managing the network without a Network Control Server is recommended only for small networks with, for example, 15 or fewer servers. Each Bridge server must be accessible for such network management tasks as preventive maintenance or troubleshooting. Each server's diskette must be maintained and updated individually.

For servers of the same type (e.g., all CS/1-As), one diskette may be copied several times, and then the copies may be modified on each individual server for its configuration.

NCS/150-based

The NCS/150 provides six services to Communications Servers in a Bridge local area network environment:

- Bootstrap service for up to 40 homogeneous products (CS/1, CS/100, CS/200, or IVECS), or a mix of 25 of any two of these products; each NCS supports only servers running the same protocol set as the NCS
- Configuration service for up to 40 servers with 64 shared configurations
- Macro file service for up to 128 macros
- Clearinghouse service for up to 254 names, or on an NCS/150 running TCP software, internet name service for up to 500 names
- Time service
- Audit trail printout service

NCS/1-based

The NCS/1 is a more powerful Network Control Server that expands and adds to the services provided by the NCS/150. The services and features offered by the NCS/1 include the following:

- Bootstrap service for up to 256 client servers (CS/1, CS/100, CS/200, or IVECS)
- Configuration service for up to 256 client servers, with 512 shared configurations
- Macro file service for up to 512 macros, with macro editing capability
- Clearinghouse service for up to 4,096 names
- Time service
- Disk-based audit trail with report generation and graphic display

- Sysgen capability for CS/1, CS/100, CS/200, and IVECS
- Multiple window network manager interface
- Network monitoring utilities
- Backup of bootstrap, configuration, global parameter, macro, and clearinghouse files to secondary NCSs

On a network without an NCS, the bootstrap, configuration file, macro file, and clearinghouse services are distributed among the individual Communications Servers on the network. The time and audit trail services are available only on a network with an NCS/150 or NCS/1.

The NCS simplifies network management and maintenance by centralizing these functions, eliminating the need for individual management of each client server. Configurable port, session, system, and network parameters are dynamically specified and retained in the NCS.

The NCS also allows the use of Communications Servers in environments where temperature levels, dust levels, or security considerations preclude the use of an internal disk drive on each Communications Server.

The NCS audit trail service collects information about session connection and disconnection, reasons for disconnections, and excessive errors. This information is not available on individual Communications Servers and is easy to read and interpret when gathered in the audit trail.

The NCS/1 is a UNIX-based* work station.

* UNIX is a trademark of AT&T Bell Laboratories.

2.0 NETWORK INSTALLATION AND VALIDATION

This section describes installing and testing a Local Area Network, including servers, coaxial cable, taps, and transceivers.

2.1 Installation Overview

The procedures involved in installing a LAN and preparing it for daily operation on the network include the following:

- Coaxial cable, terminator, tap, and transceiver installation
- Cable validation
- Server hardware configuration and installation
- System generation or firmware configuration (not required on all servers)
- Server startup and checkout
- Port configuration
- Network-to-device validation

These procedures are described in a number of manuals. Table 2-1 shows where the instructions for each procedure for each Bridge product may be found.

Table 2-1 Procedures Directory

	CS/1-A & CS/100-A	*Other CS/1s & CS/100s*	*CS/200*	*IVECS*	*GS*	*NCS*
Cable, tap & transceiver installation	NMG*	NMG*	NMG*	NMG*	NMG*	NMG*
Cable validation	NMG	NMG	NMG	NMG	NMG	NMG
Hardware configuration & installation	Getting Started	P&I**	P&I**	P&I**	P&I**	NCS I&O***
System generation or firmware configuration	NMG	NMG	P&I	n/a	NMG	NCS I&O
Startup and Checkout	Getting Started	P&I	P&I	P&I	P&I	NCS I&O
Port configuration	Getting Started	NMG	NMG	NMG	NMG	NCS I&O
Network-to-device validation	NMG	NMG	NMG	NMG	NMG	NMG

* Network Management Guide (this manual)

** Planning and Installation Guide: For Series/1 products (e.g., GS/3), see the Series/1 Planning and Installation Guide. For Series/100 products (e.g., CS/100), see the Series/100 Planning and Installation Guide. For Series/200 products, see the Series/200 Planning and Installation Guide. For the IVECS, see the IVECS Planning and Installation Guide.

*** For the NCS/150, see the NCS/150 Installation and Operation Guide. For the NCS/1, see the NCS/1 Installation and Operation Guide.

2.2 Coaxial Cable, Tap, and Transceiver Installation

Installation of coaxial cables, taps, and transceivers is the responsibility of the customer and should be performed by a qualified contractor in accordance with local regulations.

The most common Ethernet cable is the standard 50-ohm, yellow PVC-jacketed coaxial cable. This type of cable is suitable for almost all applications, but cannot be used in plenum installations. TFE coated cable may be used for plenum installation, but it is much stiffer and has a larger bending radius. *

Most coaxial cable consists of four main layers, as shown in Figure 2-1. Starting with the innermost, these layers are:

Center conductor	Thick, tin-plated copper wire
Dielectric	Plastic foam material with a thin layer of foil bonded to its outer surface
Electrostatic shielding	Three layers: thin, fine braid; thin foil; and wide, thick braid; provides shielding and acts as a ground
Jacket	Outer jacket, usually marked at 2.5-meter intervals; commonly PVC or TFE

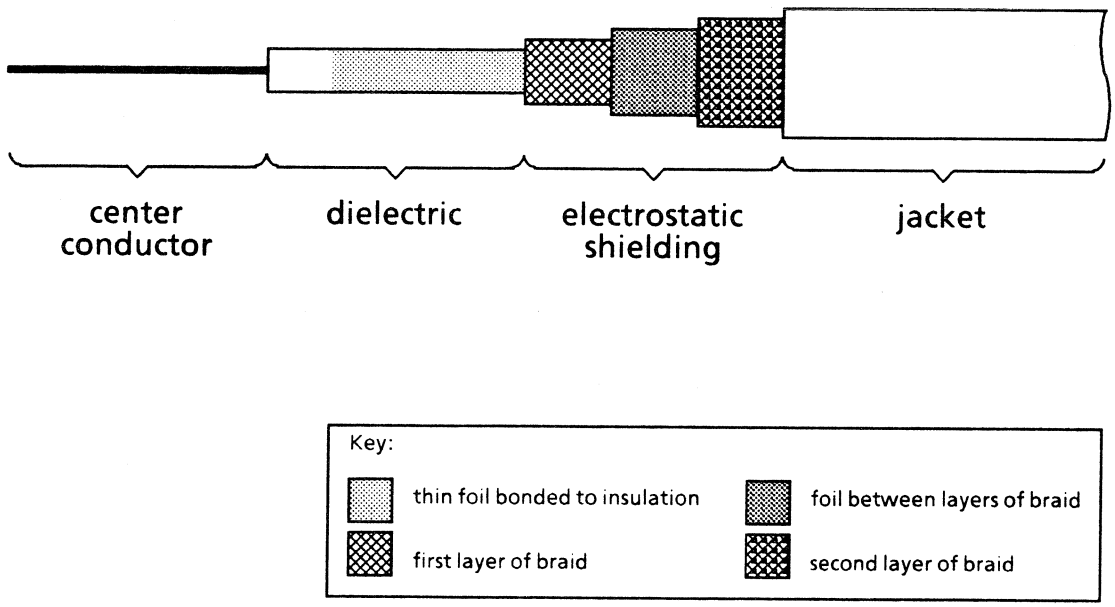


Figure 2-1 Coaxial Cable Layers

* As stated in reference [19].

2.2.1 Cable Installation

The following guidelines should be observed when installing coaxial cable.

1. Wear protective goggles or a face mask, especially when clipping cable or removing shielding.
2. Keep the cable ends tightly sealed during transportation, storage, and installation to prevent damage caused by moisture or foreign matter. After removing a portion of cable from a spool, reseal the cut end of the cable remaining on the spool.
3. Do not exceed the minimum bend radius of the cable as specified by the manufacturer.
4. Do not twist the cable or exceed the maximum recommended pulling force of the cable. When removing cable from a spool, unroll the cable; do not pull cable from the roll.
5. Route cables to allow easy access when stations are added, moved, or serviced. Ensure that nothing strikes or dents the cable during installation and that the routing of the cable is such that it will not be physically degraded during service.
6. Install the cable in segments connected with in-line extenders for flexibility and ease of fault isolation.

   The maximum length of a single Ethernet containing no repeaters is 500 meters. Section lengths of 23.4 meters, 70.2 meters, and 117 meters produce the minimum signal reflection. The best signals are produced when all parts of the cable are obtained from the same manufacturer.
7. Most Ethernet coaxial cable is marked at 2.5-meter (8.2-foot) intervals. Place transceivers at these marks to minimize wave effects. If the cable is not marked, measure the distance between transceivers.

   To facilitate troubleshooting, number these markings sequentially during installation and maintain complete, accurate documentation that indicates the location of the marking numbers and describes the cable trays, conduits, and raceways. Draw and maintain a cable-plant diagram, an example of which is shown in Section 2.8.
8. Firmly attach all transceivers to the building; transceivers must not rely on the cable for physical support. Some installations install protective brackets around each transceiver. A side-mount transceiver may be used to facilitate attachment to the building. The transceiver may be placed in a retainer or attached to a bracket if necessary. Do not allow the cable tapping clamp to be grounded.
9. Where cable does not run through supportive raceways or conduits, support it every 4.5 meters (15 feet). Ensure that supporting clamps do not pinch, dent, or deform the cable.
10. Terminate cable ends with a 50-ohm terminator, as described in Section 2.2.2. Terminators need not be placed at a 2.5-meter mark; most terminators are installed midway between two 2.5-meter markings.
11. Install the cable as a logically continuous length, with no branches. Do not use tee connectors.

12. The cable must be grounded at one, and only one, point. Grounding the cable at a single point ensures reliable communications and prevents safety hazards during installation and maintenance. Cables that are not grounded or that are grounded at more than one point may appear to function, but problems will occur as network size and traffic increase.

    To ground the cable, connect the electrostatic shielding to a reliable earth ground at one of the terminators. All elements connected to the shielding (e.g., transceiver tap block, segment connection barrels, terminators) must be isolated to ensure that the cable is grounded at one point only.

    If the cable is divided by repeaters (not in-line extenders), each segment of the cable must be grounded individually, as shown in Figure 2-2. Grounding is not passed through the transceivers that attach each cable segment to the repeater.

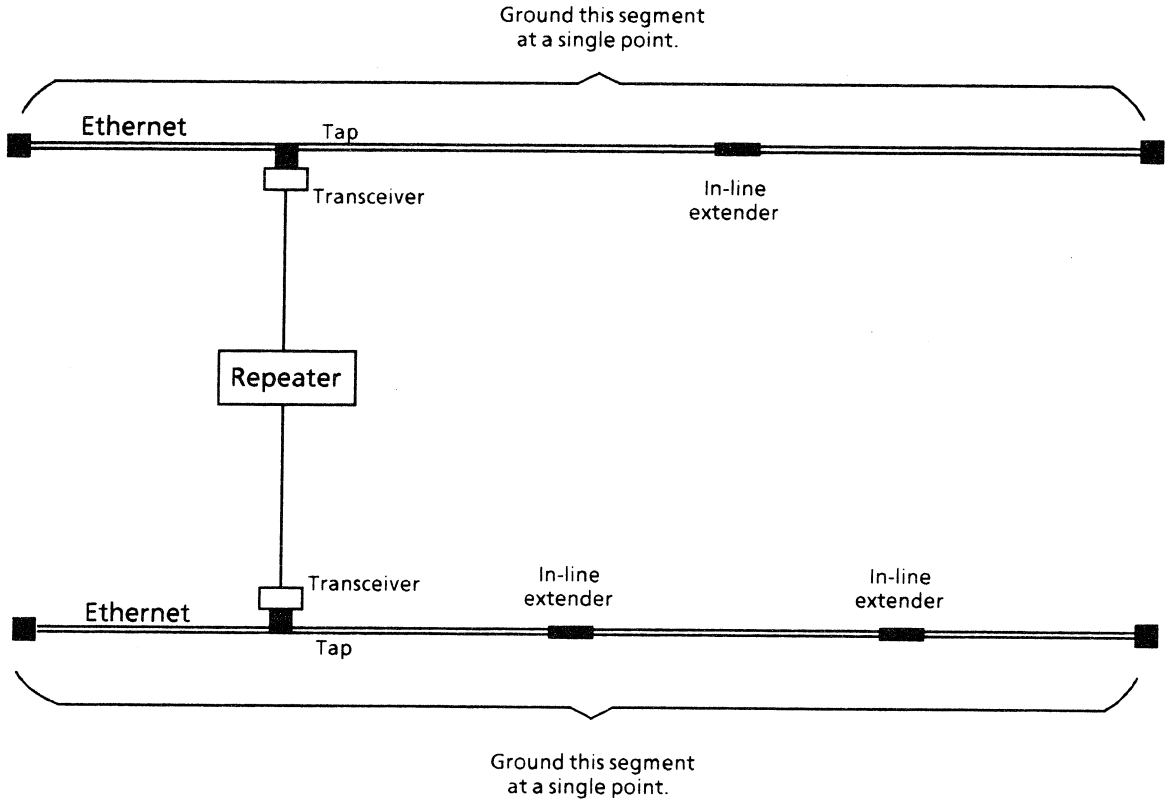


Figure 2-2 Grounding Cable Segments Attached by a Repeater

A large Ethernet system should be installed in sections. After installing each section, perform the following electrical continuity tests to detect problems caused by faulty connectors or damaged cable:

1. Thoroughly inspect all cables for manufacturing faults or shipping damage.
2. Test each cable length for electrical continuity.
3. Remove the terminator from one end of the cable and check for a 50-ohm resistance between the electrostatic shielding and center conductor. The opposite end of the cable must have a terminator installed during testing. Check the other end of the cable in this manner.
4. If a Time Domain Reflectometer (TDR) is available, use it to verify successful installation of each section.

A Time Domain Reflectometer is a valuable tool for testing, installing, and troubleshooting cables. TDRs can be used to determine the position of such problems as cable shorts, damage, kinks, and bad connectors. The TDR sends out a sample pulse and, depending on the resultant return pulse, indicates abnormalities.

A TDR should be used to test the cable before being unrolled from the spool and after being first installed. A hard copy of the TDR graphs should be kept as a reference point.

The TDR may be used to determine the distance between a test point and the location of the problem. The TDR is attached by removing a terminator and attaching the TDR to the end of the cable. With an accurate cable-plant diagram and record of marker numbers, the affected section of cable is easy to find. For example, if the problem is 175 meters from the TDR, then the problem is near marker number 70 (175/2.5).

Where possible, the cable, taps, and transceivers should be placed where users will be unable to disturb them. In Figure 2-3, the components within the dashed lines should be out of reach of network users. However, these components should be accessible to network maintenance personnel. It is best to place servers, especially those that boot from a local diskette, where they are readily accessible. The longer drop cables required to accomplish this should be evaluated against the convenience of easy access.

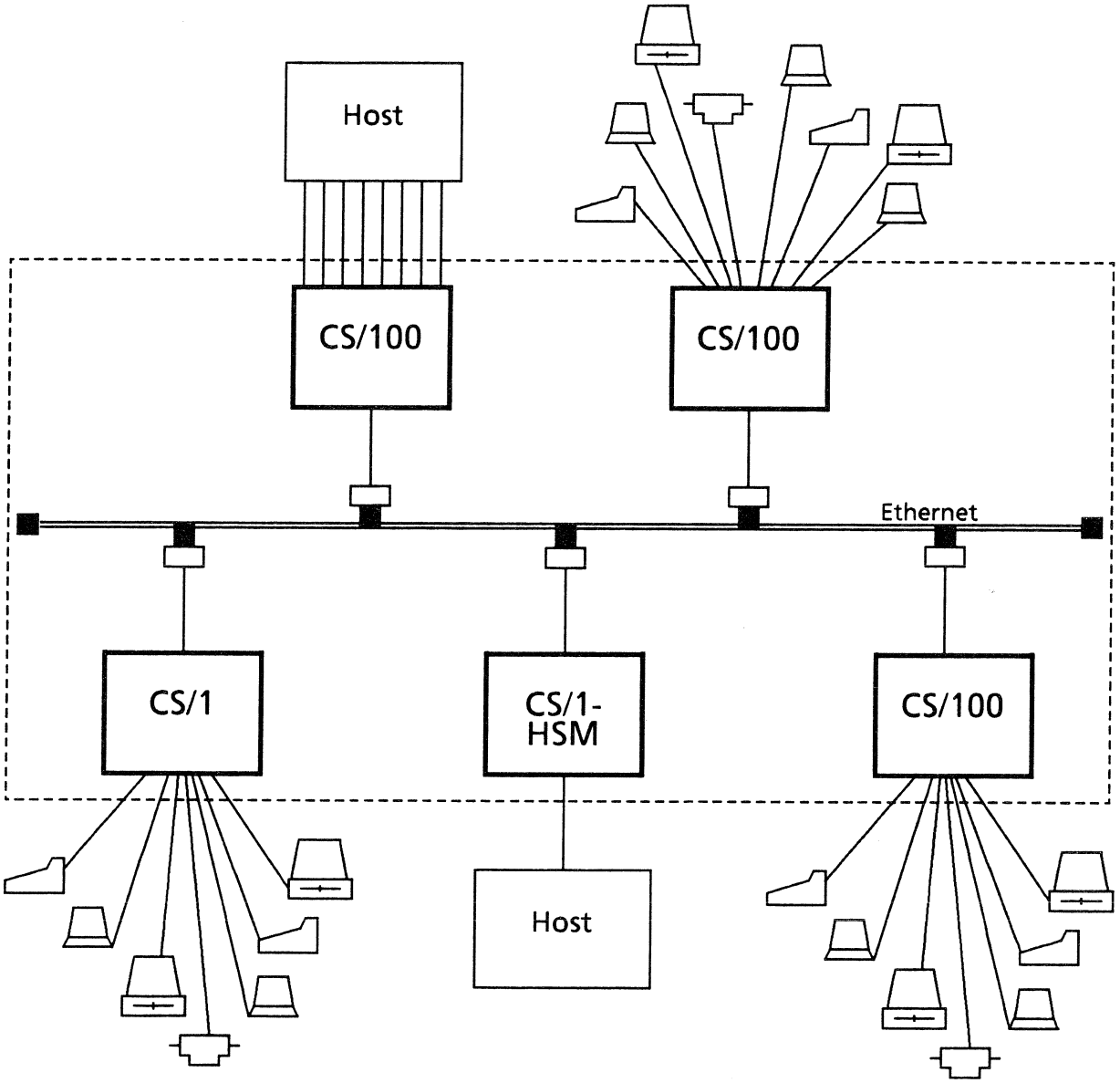


Figure 2-3 Network Maintenance Accessibility

2.2.2 Connector and Terminator Installation

An N-series connector must be installed at each end of any length of coaxial cable. The cable must then be either terminated by attaching a terminator or extended using a barrel extender. The cable may be extended up to a length of 500 meters (1640 feet).

Two types of N-series connectors are available: crimpable (e.g., K-Grip) and screw-on (e.g., Amphenol). Crimpable connectors, the type available from Bridge, require the use of a hand-crimp tool for installation. Screw-on connectors are more expensive and can be installed using an X-ACTO knife, a crescent wrench, and a soldering iron. The cable installation tool kit (designated CBL-CITK), available from Bridge Communications, Inc., facilitates installation of crimpable connectors, terminators, and extenders. The kit includes the following:

- N-series connector hand-crimp tool kit
- Ten N-series connectors (male)
- Four barrel extenders (female to female)
- Four 50-ohm cable terminators (female)
- Transceiver-tapping tool kit

The procedures for installing crimpable and screw-on connectors are outlined below.

Crimpable Connectors

Crimpable connector installation is facilitated by the use of jacket and dielectric trim-jigs. If the trim-jigs are not used, the cable must be measured by hand, as specified in the following steps.

1. Cut the cable end square and slip the connector sleeve over the jacket.
2. Cutting through the jacket and shielding to the dielectric, make the first cut 13/32 in. from the square end. Cutting through the jacket to the shielding, make the second cut 19/32 in. from the square end. The jacket trim-jig may be used to score the jacket at these locations so that it can be removed easily.
3. Remove the jacket up to the first cut.
4. Remove the shielding from the square end up to the first cut, exposing the final layer of foil bonded to the dielectric. The layer of foil that is bonded to the dielectric need not be removed.
5. Remove the jacket up to the second cut, exposing the shielding.
6. Remove 7/32 in. of the dielectric to expose the center conductor. To use a dielectric trim-jig, pass the dielectric through the hole in the end of the trim-jig, butting the outer jacket against the shoulder. Trim off the protruding dielectric flush with the end of the trim-jig.
7. Place the contact pin on the center conductor and use the hand-crimp tool to crimp it onto the center conductor.
8. Install the connector over the dielectric and under the shielding. The shielding may be split 1/4 in. axially in two places to facilitate entry of the connector. The end of the connector must be flush with the end of the contact pin.
9. Slide the sleeve to the end of the cable and up against the connector.
10. Use the hand-crimp tool to crimp the sleeve.

11. To terminate the cable, thread a 50-ohm N-series terminator into the connector and tighten it firmly. To extend the cable, thread an N-series barrel extender into the connector, tighten it firmly, and attach the extender to another section of cable.

Screw-on Connectors

1. Cut the cable end square and strip 2/10 in. of the jacket.
2. Install the collar on the cable, followed by the rubber gasket and boot. The boot should be the closest to the square end.
3. Fold all three layers of the shielding back against the boot.
4. Strip the dielectric back to the shielding (approximately 1/8 in.) to expose the center conductor.
5. Solder a contact pin to the center conductor, ensuring that the pin is pressed against the dielectric.
6. Thread the connector into the collar and tighten it.
7. To terminate the cable, thread a 50-ohm N-series terminator into the connector and tighten it firmly. To extend the cable, thread an N-series barrel extender into the connector, tighten it firmly, and attach the extender to another section of cable.

2.2.3 Tap and Transceiver Installation

Bridge recommends installing all planned taps and transceivers prior to the initial use of the network, because an incorrectly installed tap and transceiver can short out the entire network. Subsequent installation of transceivers should, if possible, be performed after regular business hours and should be followed by TDR testing.

To install taps and transceivers supplied by Bridge, follow these steps:

1. Acquire the number of taps and transceivers necessary to install the system.
2. Acquire a transceiver tapping tool kit (designated CBL-TTK; also included in the cable installation tool kit). The kit consists of three tools:

   - Coring tool with cylindrical, serrated blade (A0003-D0-1)
   - Scraping tool with chisel blade (A0003-D1-0)
   - Punching tool with probe (A0003-D2-0)

**** NOTE ****

The tools are sharp and fragile. Do not drop or mishandle them.

3. Locate the 2.5-meter mark nearest the required drop and place the tap so that the threaded hole is centered over the mark.
4. With the tap centered, tighten it firmly using a 9/16 in. open-end wrench. Hold the body of the tap so that the cable is not twisted during tap installation.

5. Insert the coring tool (A0003-D0-1) into the threaded hole on the tap body and, using a back-and-forth motion, turn the coring tool until the tool bottoms out (resistance increases).

**** CAUTION ****

Overtightening may damage the tap threads.

6. Orient the tap so that the coring tool is hanging downward; tap lightly on the threaded stud in the body of the clamp so that the material removed from the cable falls out through the center of the tool.
7. Remove the coring tool. The cable has been cut through the jacket and shielding to the foil bonded to the dielectric.
8. Insert the scraping tool (A0003-D1-0) into the threaded hole in the tap and rotate the tool clockwise several turns. The scraping tool removes the shielding.
9. Remove the scraping tool. Using a small screwdriver or probe, carefully and thoroughly clean out any remaining bits of wire or foil, which may short the coaxial system.

**** CAUTION ****

To ensure proper operation of the tap and network, the shielding must be cut cleanly, and all metal debris must be completely removed. If necessary, repeat steps 8 and 9 to ensure that no debris remains.

10. Insert the punching tool (A0003-D2-0) into the threaded hole in the tap. Tighten the tool gently until it resists further tightening, indicating that it has made contact with the center conductor of the coaxial cable. Do not overtighten.
11. Remove the punching tool.

**** NOTE ****

When the tool is removed, the center conductor of the coaxial cable may not be visible. For transceivers with non-spring-loaded probes, this should not cause transmission problems. However, for any transceiver with a spring-loaded probe, repeat steps 8 through 10 to ensure that the conductor is visible.

12. Insert the probe end of the transceiver gently into the threaded hole of the clamp. Turn the transceiver until the O-ring seal makes contact with the clamp, then turn a half-turn more to tighten. Do not overtighten. When several transceivers are installed, they may not be oriented in the same direction. Do not attempt to face them all the same way, because this may result in overtightening.
13. Secure the transceiver as required, ensuring that the coaxial cable clamp end is not grounded.

2.2.4 Transceiver Removal and Reinstallation

To remove a transceiver, follow these steps:

1. Unscrew the transceiver and carefully remove it from the tap. Ensure that the O-ring seal is in place. Protect the probe end of the transceiver.
2. Leave the tap in place and check that it is clean and free of particles. Screw a tap block plug into the tap.

If a transceiver must be reinstalled, use a new tap. Locate the new tap the minimum possible distance from the original one; the new tap may be located a maximum of 1 in. (2.5 cm) on either side of the original tap. Follow the tap installation procedure in Section 2.2.3 to reinstall the tap and transceiver.

2.3 Fiber Optic Networks

Bridge products can operate on an optical fiber cable system. A Bridge LAN based on fiber optic cable provides reliable, high-speed data exchange among computers and other digital devices within a moderately sized geographical area. Fiber optic systems can address requirements that are difficult to meet with other media.

The advantages of fiber optic systems include the following:

- Electromagnetic immunity and signal confinement: Optical fiber neither picks up nor emits electromagnetic energy. The fiber is immune to industrial plant impulse noise, radar, lightning-induced surge, and other electromagnetic interference that could affect signals.
- Security: The nature of fiber optic cable makes it difficult to tap illegally. This feature makes fiber optic systems ideal for outside installation between buildings.
- Increased geographical range: The maximum cable length is specified as a radius from a central point; with several cables radiating from the star coupler, the area covered is much larger.
- Small size: Optical fiber is much thinner and lighter than coaxial Ethernet.

The components of a Bridge fiber optic cable plant, shown in Figure 2-4, include the following:

- Ethernet-compatible optical transceivers
- Fiber optic cable pairs
- Optical star couplers
- Fiber optic repeaters

The transceiver converts an electrical signal to an optical signal, which is carried on the transmit fiber of each fiber optic cable pair. The data travels to the star coupler, which outputs the signal onto all the receive fibers of each pair. The data is then received by the transceivers.

Standard transceiver cables are used to connect servers to the optical transceivers.

There are two types of optical fiber: glass clad silica (GCS) and plastic clad silica (PCS). Graded index GCS is available with the following core cladding diameters (in micrometers): 50/125, 62.5/125, 85/125, and 100/140. GCS is also available in single mode. PCS is available with a 200 micrometer core diameter.

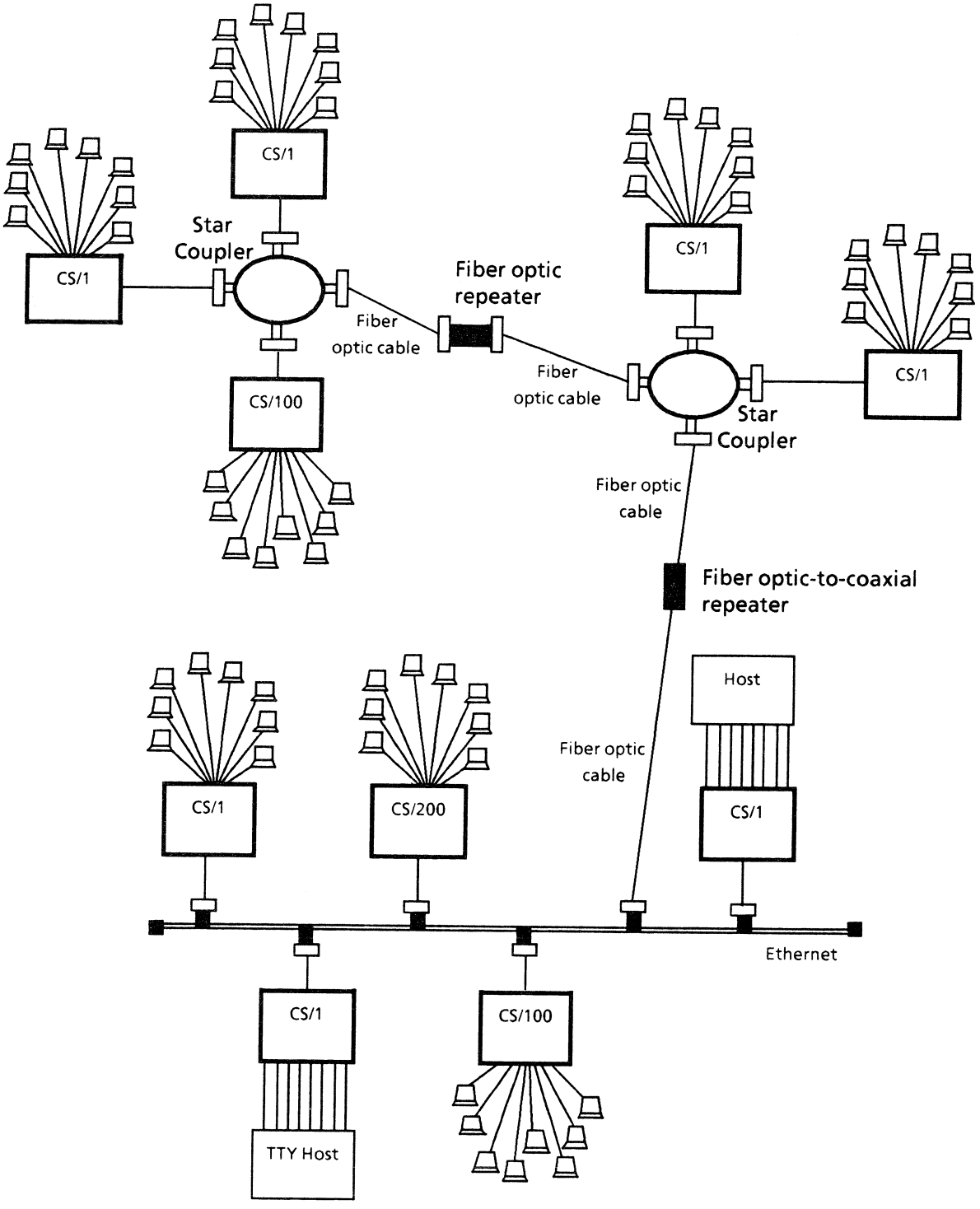


Figure 2-4 Typical Fiber Optic Network

The type of cable that is appropriate for a given installation depends on the configuration of the network and the environment into which the cable will be installed:

- Simplex, duplex, and multichannel fiber optic cables are available to meet the various local network requirements.
- Plenum cables with Teflon* outer jackets are used where cables are installed in open cable trays.
- Armored cable is used for systems that require direct burial.
- Flame retardant cables are available to meet UL VW-1 specifications.
- Cables are available with both loose and tight tube construction. Tight tube construction, where the fiber is in intimate contact with the plastic jacket, is better suited to installations where small bend radii are required. It is slightly easier to connect than cable with loose tube construction. Loose tube construction has less optical attenuation and better performance at lower temperatures than tight tube construction.

A variety of fiber optic cable types are available. Bridge recommends cable with the following characteristics:

- 100 micrometer core/140 micrometer cladding
- Attenuation (aF) of 6 dB/Km at 850 nm or less
- Two fibers per cable

Connectors must be of SMA type (Amphenol 906). Bridge recommends high-quality metallic connectors.

Star couplers are available with 4, 8, 16, and 32 ports. A pair of fibers runs from every network node to the star coupler.

The fiber optic network must conform to the following specifications:

- Maximum of 32 optical transceivers per star segment
- Maximum of 32 star segments, for a total of 1024 devices on the network
- No more than two repeaters in the path between any two servers
- Transceiver cable (from transceiver to server) no more than 50 meters long
- Maximum segment length between 0.5 Km and 2.5 Km, depending on the star size
- Maximum internode spacing of 2.5 Km

The maximum length of the fiber segments originating from the star must be computed as a function of the star size and the immediate connectors used. The flux budget is the allowable system loss between any two nodes (for bit error rate less than 10E-9). Contact an authorized Bridge service representative for assistance in planning a fiber optic network.

---

* Teflon is a registered trademark of the E.I. duPont Company.

2.4 Transceiver Connectors and Coupling

Bridge servers may be attached to Ethernet Version 1.0, Ethernet Version 2.0, or IEEE 802.3 transceivers, and also operate with Digital Equipment Corporation DELNI equipment. Transceivers may be AC- or DC-coupled. Bridge recommends using a given type of transceiver cable with the same type of transceiver (e.g., Ethernet Version 1.0 transceivers with Ethernet Version 1.0 transceiver cables).

Table 2-2 lists examples of transceivers that have been tested by Bridge Communications, Inc. The table indicates each transceiver's coupling, whether it is fiber optic, and its version.

Although Bridge servers operate with transceiver eliminators, the eliminators introduce greater cable delays than standard transceivers and may result in some violation of the Ethernet specifications.

Table 2-2 Transceivers Tested by Bridge Communications

Manufacturer	*Model*	*Coupling*	*Version*	*Fiber Optic*
BICC/Isolan	1110	AC	802.3	
Codenoll	3020	both	1.0	
Technology Corp.	3030	both	802.3	x
DEC	DELNI-8A	AC	n/a*	
	H4000	AC	2.0	
Seicor FiberLAN	Net 10 Optical	AC	**	x
TCL Inc.	2010I ***	AC	802.3	
	2010IS ***	AC	802.3	
	2010EC ***	AC	1.0	
	MTU 2110-A0	AC	1.0	
	MTU 2110-AI	AC	****	
	MTU 2110-B0	AC	1.0	
	MTU 2110-BI	AC	****	
3Com	3C100	DC	1.0	

* For servers with EC/1 boards, the DELNI must be attached to a Version 1 transceiver.
** Available in every version.
*** Recommended by Bridge Communications, Inc.
**** Available in Version 2.0 and IEEE 802.3.

2.5 Device Cables

A detailed description of the cables available from Bridge for use on Bridge servers is provided in the *Cable Guide* (reference [11]). In addition, each *Planning and Installation Guide* (except for the IVECS) contains descriptions of the cables used with the described servers.

If a standard cable described in the *Cable Guide* or the *Planning and Installation Guide* is appropriate, order the cable from Bridge Communications, Inc., specifying the cable identifier. The standard length of all cables is 25 feet.

If the application requires any deviation from the specifications listed in these manuals, Bridge recommends three alternatives:

1. Modify the standard cables by extracting and reinserting pins as appropriate. The standard cables are built with nonmolded boots to facilitate this type of rework. Label all modified cables.
2. Build custom cable in accordance with the diagrams and guidelines provided in the *Cable Guide*.
3. Order custom cable from Bridge Communications, Inc. The customer must provide custom cable specifications using the format shown in the *Cable Guide*. The cost of custom cable includes a nonrefundable set-up charge.

In all cases where cables must be run through conduits, custom cables should be built on-site. However, initial network checkout should be performed using standard cables; Bridge recommends ordering a few standard cables of each type required at the installation for use during initial network checkout.

2.6 Network Cable Validation

After installing all planned cable, terminators, taps, and transceivers, the cable should be validated before beginning network operation. Follow these steps:

1. Check all cable terminators for tightness.
2. Test all equipment, such as transceivers and repeaters, as recommended by the manufacturer.
3. Remove the terminator from one end of the cable and check for a 50-ohm resistance between the electrostatic shielding and center conductor. The opposite end of the cable must have a terminator installed during testing. Check the other end of the cable in this manner.
4. If a Time Domain Reflectometer (TDR) is available, use it to verify successful installation of each section. Section 2.2.1 describes TDRs.

2.7 Network-to-Device Validation

A specialized network testing and troubleshooting tool, the Packet Generation software, is available as an option from Bridge Communications, Inc. The Packet Generation software is used to validate all hardware involved in the connection from the network, through the server, to the attached device by sending a continuous stream of packets from one server port to another server port on the network.

Three versions, each supplied on diskette, are available: asynchronous, for servers supporting asynchronous devices; TCP, for servers running the TCP/IP protocols; and bisynchronous, for servers supporting bisynchronous and bit-synchronous devices. Each version is described in the following sections.

By letting the Packet Generation software run overnight, or at least for several hours, the network manager can accumulate a large sample of statistics. For every version of the packet generator, these statistics may be interpreted using the guidelines in Section 4.2. Network validation using the Packet Generation software may be performed while the network is operational, although the server running the Packet Generation software should be used for that purpose only.

2.7.1 Asynchronous Packet Generator

Two versions of the asynchronous packet generator are available: one for the CS/1-A (designated SW/PKTGEN-A) and one for the CS/100-A or NCS/150 (designated SW/PKTGEN-100 & 150). For the CS/1-A, the packet generator allows connections to virtual ports 32 through 63, for a total of 32 connections to the packet generator. For the CS/100-A or NCS/150, the packet generator allows connections to virtual ports 2 through 14, for a total of 13 connections to the packet generator. For convenience, these ports may be assigned to a rotary.

Be sure to boot the CS/100 packet generator on a CS/100-A and the CS/1 packet generator on a CS/1-A. Once the appropriate packet generator has been booted on a given unit, connections can be made to the packet generator from both CS/1s and CS/100s.

The following procedure assumes that the user connects to the packet generator from a terminal attached to a Communications Server elsewhere on the network, as shown in Figure 2-5. However, because the Packet Generation software includes the complete Connection Service software, the user can connect to the packet generator from a terminal attached to any port on the same server that is running the Packet Generation software.

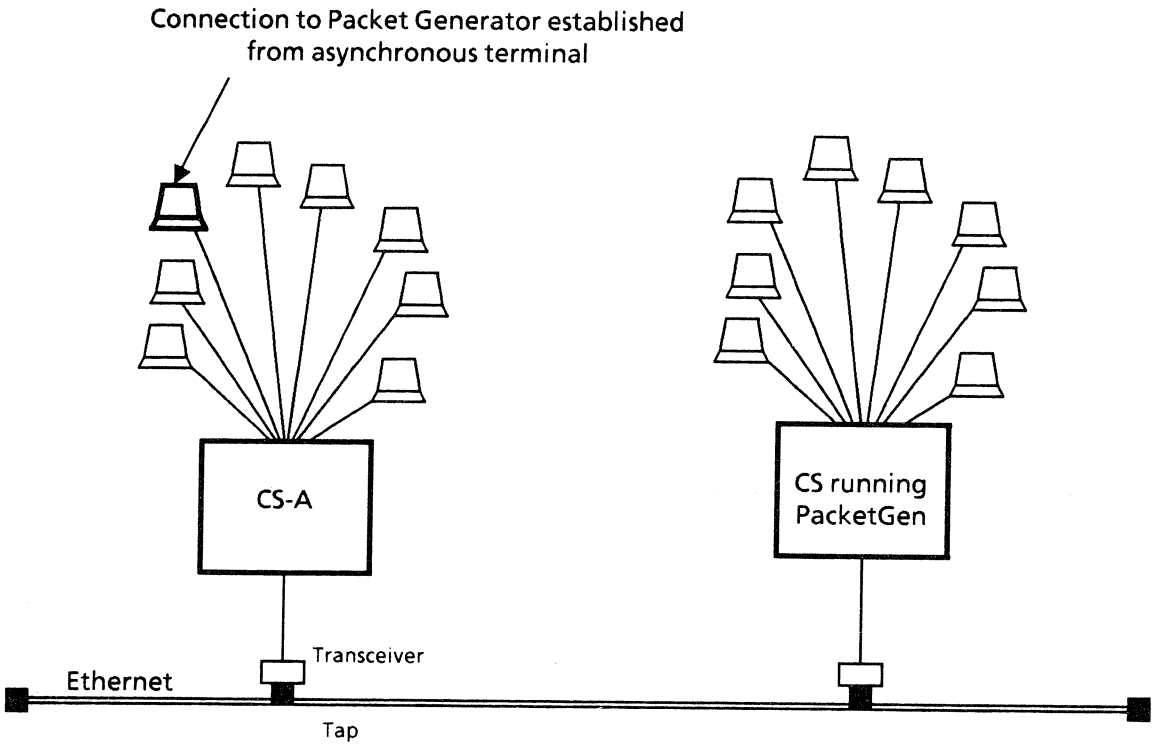


Figure 2-5 Running the Asynchronous Packet Generator Software

To test the network using the asynchronous packet generator, follow these steps:

1. Boot the appropriate packet generator software on a CS/1-A, CS/100-A, or NCS/150.
2. If desired, assign the packet generator virtual ports to a rotary. For example, assigning the following rotary on a CS/1-A allows all connections to be made to port !128:

```
rotary !128=!32-!63
```

3. Boot the standard Connection Service software on a second Communications Server elsewhere on the network.

4. From a terminal port on the second server, make a connection to the server running the packet generator software, specifying the Ethernet address of the server running the packet generator and the rotary defined above or a virtual port number. For example, to connect to packet generator rotary 128 on a CS/1-A, enter the following command and press the return key:

```
connect <address>!128
```

Or, to connect to packet generator virtual port 2 on a CS/100-A, enter the following command and press the return key:

```
connect <address>!2
```

The system responds with the packet generator prompt:

```
PKTGEN>
```

To establish more than one simultaneous session, make additional connections to the rotary or use a different virtual port number for each session.

5. Begin transmission of test packets by entering the following command and pressing the return key:

```
g
```

The remote server starts sending test packets to the terminal, with a 2-second pause between packets. Each packet contains one header line and 22 lines of data, as shown in Figure 2-6.

6. Inspect the display on the terminal screen. The characters should line up in vertical columns, as shown in Figure 2-6. Irregular rows and columns indicate lost characters.

7. Let the packet generator run at least one hour. Test results are most reliable if the transmission is allowed to continue for several hours. Bridge recommends running the tests for 24 hours in order to measure the effect of any daily transient factors (e.g., electrical machinery starting in the morning on a business day) and to get a reference base of error rates for your installation.

8. To stop the tests, suspend transmission of test packets by pressing the <BREAK> key. Transmission of test packets may be resumed by entering the command:

```
g
```

9. After stopping the tests, return the terminal port to Command mode by entering the ECMChar (usually <CTRL-^>). Then terminate the connection by entering the following command:

```
dc
```

```
CS/1  port !32  PACKET #  1  Wed Dec 31 16:01:23 1969
!"#$%&'()*+,-./0123456789:;<=>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[]^_`abcdefghijklmnop
!"#$%&'()*+,-./0123456789:;<=>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[]^_`abcdefghijklmnop
!"#$%&'()*+,-./0123456789:;<=>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[]^_`abcdefghijklmnop
!"#$%&'()*+,-./0123456789:;<=>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[]^_`abcdefghijklmnop
!"#$%&'()*+,-./0123456789:;<=>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[]^_`abcdefghijklmnop
!"#$%&'()*+,-./0123456789:;<=>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[]^_`abcdefghijklmnop
!"#$%&'()*+,-./0123456789:;<=>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[]^_`abcdefghijklmnop
!"#$%&'()*+,-./0123456789:;<=>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[]^_`abcdefghijklmnop
!"#$%&'()*+,-./0123456789:;<=>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[]^_`abcdefghijklmnop
!"#$%&'()*+,-./0123456789:;<=>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[]^_`abcdefghijklmnop
!"#$%&'()*+,-./0123456789:;<=>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[]^_`abcdefghijklmnop
!"#$%&'()*+,-./0123456789:;<=>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[]^_`abcdefghijklmnop
!"#$%&'()*+,-./0123456789:;<=>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[]^_`abcdefghijklmnop
!"#$%&'()*+,-./0123456789:;<=>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[]^_`abcdefghijklmnop
!"#$%&'()*+,-./0123456789:;<=>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[]^_`abcdefghijklmnop
!"#$%&'()*+,-./0123456789:;<=>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[]^_`abcdefghijklmnop
!"#$%&'()*+,-./0123456789:;<=>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[]^_`abcdefghijklmnop
!"#$%&'()*+,-./0123456789:;<=>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[]^_`abcdefghijklmnop
!"#$%&'()*+,-./0123456789:;<=>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[]^_`abcdefghijklmnop
!"#$%&'()*+,-./0123456789:;<=>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[]^_`abcdefghijklmnop
!"#$%&'()*+,-./0123456789:;<=>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[]^_`abcdefghijklmnop
!"#$%&'()*+,-./0123456789:;<=>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[]^_`abcdefghijklmnop
```

Figure 2-6 Asynchronous Packet Generator Screen Display

2.7.2 TCP Packet Generator

The TCP packet generator is available only on a CS/1 running TCP protocols. It allows connections to virtual ports 48 through 63, for a total of 16 connections to the packet generator. Information on TCP addresses is available in reference [10].

To test the network using the TCP packet generator, follow these steps:

1. Using the system generation procedure described in Section A.6, assign an internet address for the packet generator.
2. Boot the server and assign ports 48 through 63 to a rotary. For example:

   ```
   rotary !128=!48-!63
   ```

3. From a terminal attached to an asynchronous port on the server, assign an internet address to the rotary defined in the previous step. For example:

   ```
   setdefault (!128) ip=192.9.200.1
   ```

4. Make a connection to the rotary defined in the previous step. For example:

```
connect 192.9.200.1
```

The user interface of the TCP packet generator is the same as that of the asynchronous packet generator. Continue the procedure with step 5 of Section 2.7.1.

2.7.3 Bisynchronous Packet Generator

The bisynchronous packet generator is used to send packets to a CS/1-BSC or CS/1-SDLC. Virtual ports 32 through 63 are available, for a total of 32 connections to the packet generator.

Figure 2-7 shows the typical components involved in the packet generation test. The bisynchronous Packet Generation software is booted on a CS/1-A or CS/1-A/BSC with an attached asynchronous terminal. The server to be tested is a CS/1-BSC or CS/1-SDLC with a 3276-2 or 3276-2-emulator attached. The port to which the 3276-2 is attached must be configured for 3270 compatibility, described in reference [10], and its PassCheck parameter must be set to Strip. The 3276-2 must be configured to recognize control unit address 0(x'40'). Data is delivered to device address 0(x'40').

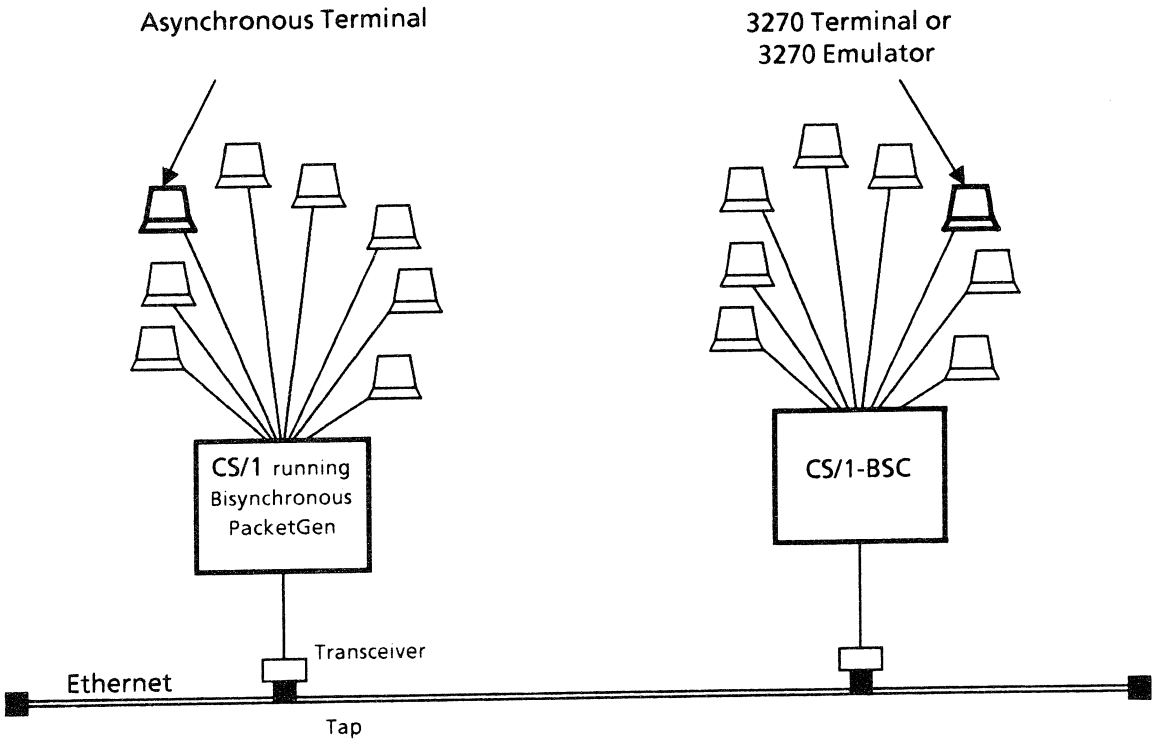


Figure 2-7 Running the Bisynchronous Packet Generator Software

The Packet Generation software includes the complete Connection Service software. The following procedure assumes that the user connects to the packet generator from a terminal attached to an asynchronous Communications Server elsewhere on the network, as shown in Figure 2-7. However, if the server running the Packet Generation software includes an asynchronous board, the user can connect to the packet generator from an asynchronous terminal attached to the asynchronous portion of the server.

The bisynchronous packet generator has no commands. Once a connection is made to the packet generator, packet transmission begins and continues until the connection is disconnected.

To test the network using the bisynchronous packet generator, follow these steps:

1. Boot the packet generator software on a Communications Server to which an asynchronous terminal is attached.
2. Boot the standard Connection Service software on a CS/1-BSC or CS/1-SDLC with an attached 3276-2 elsewhere on the network.
3. From the asynchronous terminal, raise the privilege level to local or global network manager and establish a third-party connection from a virtual port of the packet generator to the port to which the 3276-2 is attached.

   For example, to establish a third-party connection from the packet generator virtual port 32 on a server with Ethernet address %080002000A6C to a CS/1-BSC with the Ethernet address %080002006559 and with a 3276-2 attached to port 0, enter the following command and press the return key:

   ```
   c (%080002000A6C!32) %080002006559!0
   ```

   The packet generator issues screens to the 3276-2 every 20 seconds. Each packet contains one header line and 23 lines of data, as shown in Figure 2-8.
4. Inspect the display on the terminal screen. The characters should line up in vertical columns, as shown in Figure 2-8. Irregular rows and columns indicate lost characters.
5. Let the packet generator run at least one hour. Test results are most reliable if the transmission is allowed to continue for several hours. Bridge recommends running the tests for 24 hours in order to measure the effect of any daily transient factors (e.g., electrical machinery starting in the morning on a business day) and to get a reference base of error rates for your installation.
6. To stop the tests, disconnect the third-party connection. For example:

   ```
   dc (%080002000A6C!32)
   ```

```
CS/1   3270     PACKET     GEN
;-/|,%_]?‘:#@’=abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789
;-/|,%_]?‘:#@’=abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789
;-/|,%_]?‘:#@’=abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789
;-/|,%_]?‘:#@’=abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789
;-/|,%_]?‘:#@’=abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789
;-/|,%_]?‘:#@’=abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789
;-/|,%_]?‘:#@’=abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789
;-/|,%_]?‘:#@’=abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789
;-/|,%_]?‘:#@’=abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789
;-/|,%_]?‘:#@’=abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789
;-/|,%_]?‘:#@’=abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789
;-/|,%_]?‘:#@’=abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789
;-/|,%_]?‘:#@’=abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789
;-/|,%_]?‘:#@’=abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789
;-/|,%_]?‘:#@’=abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789
;-/|,%_]?‘:#@’=abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789
;-/|,%_]?‘:#@’=abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789
;-/|,%_]?‘:#@’=abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789
;-/|,%_]?‘:#@’=abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789
;-/|,%_]?‘:#@’=abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789
;-/|,%_]?‘:#@’=abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789
;-/|,%_]?‘:#@’=abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789
;-/|,%_]?‘:#@’=abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789
```

Figure 2-8 Bisynchronous Packet Generator Screen Display

2.7.4 Displaying Generated Statistics

The information in this section applies to all types of servers for which a packet generator is available.

After running the Packet Generator long enough to accumulate a reliable sample of statistics, display and analyze the statistics by following these steps:

1. At another terminal port on the server used to make a connection to the packet generator, change the privilege level to local or global network manager using the SET PRIVilege command.

2. Display the statistics for the server used to make a connection to the packet generator by entering the following command:

   ```
   show stats s
   ```

   The system displays a statistics report similar to that shown in Figure 4-2, Section 4.2.1.

3. Display the recorded statistics for the server that ran the packet generator by entering the following command:

```
show (<address>) stats s
```

where <address> is the Ethernet or internet address of the server running the packet generator.

Again, the system displays a statistics report similar to Figure 4-2, Section 4.2.1.

4. Analyze the error statistics using the guidelines described in Section 4.2.7.

Additional validation may be necessary depending on the arrangement of the network. Run the packet generator software on different servers in order to test different sets of connections. If transceiver eliminators or repeaters are used, run the packet generator across the maximum number of repeaters and transceiver eliminators. Boot the Packet Generation software on one server closest to one end of the network, and connect to that server from a terminal attached to a server at the opposite end of the network.

If one server on the network is consistently unreliable, the problem could be either with the transceiver connecting the server to the network or with the server itself. Before concluding that the server is not working, connect it to a transceiver that is known to operate correctly and run the tests again.

If failure of a server-to-device connection is suspected, make a connection from a terminal attached to that server to another server running the Packet Generation software.

The Packet Generator can be run across Gateway Servers. To do so, boot the Packet Generator software on a Communications Server on one network. Then make a connection to it from a Communications Server on a second network that is accessible via a Gateway Server.

An apparently sluggish response and frequent interrupts on the SIO processor may be the result of a noisy cable causing frequent transitions on the RS-232-C handshake lines (e.g., DCD, CTS). To determine whether these lines are causing the problem, insert an RS-232-C jumper box between the server and the device cable, with only data lines connected and handshake lines jumpered high. If response picks up, then the lines should be permanently removed from the cable or, if they are required for the attached device, the cable shielding should be improved.

2.8 Installation and Validation Control Documents

This section includes examples of network management documentation related to network installation and validation.

Network Map

Figure 2-9 shows a network map. The network map shows the locations of the following:

- All servers. Three-part codes, such as 2E12, identify the server and port number for each office:
  - The first number identifies each server within a department
  - The department is indicated by a letter
  - The letter is followed by the port number to which the office's SIO cable is attached
- Route of the Ethernet throughout the building, showing taps and transceivers, repeaters, in-line connectors, and terminators.
- Cable marker numbers

Each hardware component in the building should be labeled with the appropriate codes from this map. For example, each SIO cable should be labeled at both the device end and the terminal end with its department, server, and port codes.

The network manager should maintain a list that correlates each server's department and server codes to its Ethernet or IP address. The audit trail and network map report using addresses. The manager then correlates the address to the code of the involved server using this list.

The network map should be independent of personnel moves and changes. It may be coordinated with a personnel map to determine what components are involved when, for example, a particular user calls with a problem.

In addition to the network map, system generation can be used to append each user's port number to the Communications Server prompt. With a server's default prompt set to its two-part code (e.g., 2E), the prompt indicates both the server and port number for each user. For troubleshooting, the network manager knows what components are involved simply by asking for the user's prompt. Sysgen is described in Appendix A.

Network and personnel maps should be verified periodically.

Network Request Form

Figure 2-10 shows a network request form. This form, completed by the requesting network user, documents requests for additional terminals, printers, and other devices.

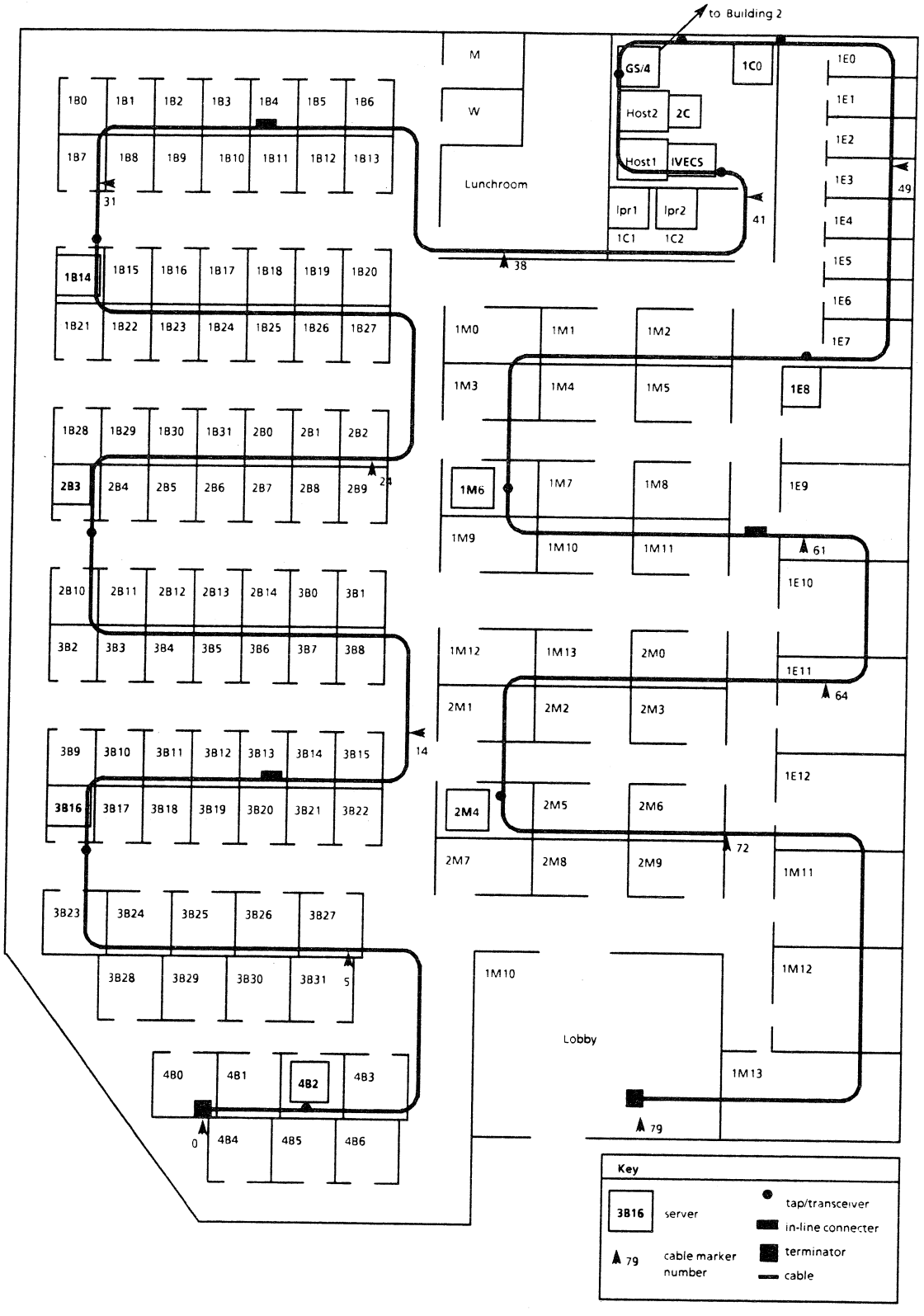


Figure 2-9 Network Map

NETWORK REQUEST FORM

Return completed form to
Network Management Department.

DATE: _____

REQUESTER: _____

DEPARTMENT: _____

REQUEST: _____

SIGNATURE: _____

For Network Mgmt. Department Use Only:

Status: _____ Form #_____
Scheduled Completion Date: _____
Actual Completion Date: _____

Figure 2-10 Network Request Form

3.0 NETWORK CONFIGURATION

This section describes software configuration, access control, clearinghouse and internet names, and macros.

3.1 Software Configuration

Once a server has been installed, some software configuration may be necessary. Bridge servers have two sets of software-controlled parameters: system generation parameters and configuration parameters.

3.1.1 System Generation

System generation parameters apply to an entire Bridge server. These parameters typically need to be changed only once for a given installation. The parameters are modified through the Sysgen program, described in Appendix A.

System generation is used to adjust CS/1, CS/100, CS/200, and Gateway Server system generation parameters to meet the needs of a specific installation. The results of the system generation are recorded on the system diskette, which should be backed up afterward.

System generation is, in most cases, used only to make modifications for custom software or nonstandard installations, or, on TCP servers, to specify the server's internet address. Unless specifically required, avoid using different system generation parameters on various servers.

**** NOTE ****

> Giving a User privilege level to commands that can change stored names, macros, rotaries, or default configurations (e.g., Name, UNDefine, ROtary, SETDefault) is not recommended.

Each Communications Server can be sysgenned to append each user's port number to the Communications Server prompt. With a server's default prompt set to its two-part code (e.g., 2E), described in Section 2.8, the prompt indicates both the server and port number for each user. For troubleshooting, the network manager knows what components are involved simply by asking for the user's prompt. For specific instructions, refer to Appendix A.

If system generation is run on a server that boots from an NCS/1, then system generation must also be run on the NCS/1 to ensure that the server's parameters are the same on its own local diskette and on the NCS/1. In addition, the appropriate files must be copied to the server's secondary NCS. This way, the server will receive the correct parameters whether it is booted from its own local diskette, from its NCS/1, or from its secondary NCS.

The following servers always require system generation:

All Gateway Servers	CS/1-TCP
CS/1-BSC running SPMUX software	CS/1-X.25
CS/1-HSM	CS/100-TCP
CS/1-SNA	NCS/150-TCP

Other servers may or may not require system generation depending on the needs of the installation. Appendix A provides further details on the appropriate use of system generation.

3.1.2 Port Configuration

After the network manager runs the Sysgen program, default values for the port configuration parameters should be adjusted to reflect local requirements. Port configuration parameters apply to individual ports and may need to be changed more frequently than system generation parameters. Port configuration parameters can be changed dynamically using the ReaD, SET, SETDefault, and REMoteSET commands. Appendix B describes port configuration parameters.

Create and maintain backups for each server after it has been fully configured.

An efficient way to configure a large network is to define a few generic default parameter files, with one file for every major port type used throughout the network (e.g., VT100 terminals, VAX* host ports, dial-out modems, and so on). These generic files may then be used to configure the majority of ports on the network, thereby limiting the proliferation of varied configurations on similar devices.

Keep accurate, current records of the configuration of each server. Keeping these records online on an NCS/1 or on a host computer connected to a Communications Server allows network configuration and other network management operations to be automated.

* VAX is a trademark of Digital Equipment Corporation.

3.2 Access Control

Local and Global network manager passwords should be changed periodically.

Access to specified ports and specified servers can be restricted for system security by establishing access groups. Access groups should be carefully and thoroughly planned to prevent problems as the network increases in size.

Access groups are defined by using the AccessGroup and AccessWord parameters, which together determine which ports can make connections to which ports. 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 numbers appear, the system prompts the user for a password associated with the AccessGroup parameter for the destination port.

For example, assume the AccessWord parameter of all Communications Server ports on the network is set to the default of 1. The following commands place ports 1 through 16 of the server on which the commands are entered in access group 2:

```
setdefault (!1) accessgroup=2
setd (!2) ag=2
setd (!3) ag=2
setd (!4) ag=2
setd (!14) ag=2
setd (!15) ag=2
setd (!16) ag=2
```

The following command defines the Group2Passwd as "accounting":

```
setd group2passwd="accounting"
```

With this configuration, any user attempting to access ports 1 through 16 of the configured server from outside group 2 would be required to enter the password "accounting" before the connection could be established.

A user on a public network who makes a connection to the local network should not be allowed to make a subsequent connection outside the local network. In this situation, any toll charges for long-distance calls resulting from a subsequent connection are charged to the local network, not to the original user.

Access groups are not available on TCP servers.

3.3 Clearinghouse/Internet Names

Clearinghouse or internet names should be defined to simplify access to resources such as hosts, printers, modems, and so on. Assigning names to individual terminals is unnecessary, except for those to which the global network manager frequently sends broadcast strings.

Bridge recommends keeping a local or global network manager privilege level for the Name and UNName commands. Access to the Name and UNName commands should be limited to the smallest possible number of people, and only to those with an understanding of the Bridge clearinghouse or internet name system.

The clearinghouse and internet name systems are described in detail in the *Connection Service User's Guide* (reference [10]).

Within a network or group of interconnected networks, if the same name is defined more than once and mapped to different addresses or address lists, sessions to that name can be misrouted, resulting in lost data. To prevent this, ensure that no name is defined more than once within a single network. If internetworks are used, every name should be defined once on each network.

Assigning a name to each server, without specifying ports on the server, enables easy reference to that server for network management tasks. For example, ports on a server named "cs2a" can be easily referenced in broadcast and listen commands:

```
broadcast (cs2a!7) "Your listing is finished."
listen (cs2a!3)
```

3.4 Using Macros

A macro is a high-level command defined by the network manager and composed of multiple individual Connection Service commands. Macros may be used to simplify the user interface for less sophisticated users, to provide customized commands for specific applications, and to enhance certain features of the user interface.

Macros that need to be accessed from multiple Communications Servers must be defined on each Communications Server or on the NCSs from which the servers boot. Ensure that macros with a given purpose stored on different servers have the same name and contents. For example, a macro that sets parameters for interaction with a given personal computer should not be named "apple_params" on one server and "mac_set" on another server.

Each Communications Server has the facility to execute a selected macro upon power-on or reset of the server and, for each port, upon entering Command mode from Listening mode. Macros executed in this way are called initialization macros. A macro named INIT is executed automatically whenever a Communications Server is powered on or reset; this is the system initialization macro. The InitMacro parameter of each terminal port can be assigned the name of a macro to be executed whenever the device attached to that port enters Command mode from Listening mode; this is the port initialization macro.

For servers that boot from an NCS, the system initialization macro is called init.<xxxx>, where <xxxx> are the last four digits of the unit'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.

Macros may be nested.

**** NOTE ****

System initialization macros are executed at global network manager privilege level automatically.

If a macro is executed at global network manager privilege level, and the macro includes a line setting the privilege level to global network manager followed by a line containing the global password, then the password will generate an error message when it is read. To prevent this, first set the privilege level to user:

```
set privilege = user
set privilege = gnm
<password>
```

This often occurs in macros that are executed as the system initialization macro.

The macros in this section include the complete names of most commands and parameters. However, because macros are limited in length to 256 bytes, it is best to use the minimum unambiguous abbreviation of commands and parameters in macros that may approach this limit.

3.4.1 Logging On

The following macro provides a way for users to access a given application directly, bypassing the Bridge user interface completely. For example, when the user enters "do logon" at the Communications Server prompt, the following macro establishes a connection to "host" and requests the application package "Wordsmith":

```
define logon = (
connect host ecm
pause 2
transmit "WORDSMITH^M"
resume
)
```

The Pause command is included to allow time for the host to send a prompt to the port before the Transmit command is executed.

Remember to end the string in the Transmit command with a caret (^) followed by an upper case "M".

3.4.2 Automatic Dialing

Macros can be used with a smart modem to dial a specific host automatically. For example, suppose a smart modem is attached to a Communications Server port with the clearinghouse name "modem", and that the Dow Jones service is reached by dialing the number (408)555-4400. The following macro allows the user simply to enter "do dow" to access the service:

```
define dow = (
connect modem ecm
pause 1
transmit "ATDT4085554400^M"
resume
)
```

Remember to end the string in the Transmit command with a caret (^) followed by an upper case "M".

3.4.3 Setting Special Parameters

In many environments, different hosts require different settings for such parameters as flow control or character echoing. Macros can be established to set these parameters automatically. For example, the following macros enable the user to enter "do wordstar" or "do remotehost" to connect to the specified host and set the appropriate parameters:

```
define wordstar = (
connect cpmhost ecm
set flowcontrolfrom=none flowcontrolto=none
set echodata=off
resume
)

define remotehost = (
connect remhost ecm
set flowcontrolfrom=xon_xoff flowcontrolto=xon_xoff
set echodata=on
resume
)
```

3.4.4 Configuring Port Parameters

Macros may be used to configure port parameters when, for example, equipment is moved or added to an existing Communications Server. The procedure is similar for host ports, terminal ports, and modem ports.

Ports may also be configured by saving port configuration files in named files and copying the appropriate file into a port's default configuration file using the ReaD command. Reference [10] describes this method.

Host Port

The following macro is an example that contains the commands that would otherwise be executed individually to configure a host port:

```
define host_conf = (
setd (host_port) DeVice=Host
setd (host_port) UseDCDout=(OnConnection, NoToggle)
setd (host_port) UseDTRin=AsDTR BReakAction=IGnore
setd (host_port) BAud=9600 DataBits=8
setd (host_port) PARIty=None IdleTimer=1
)
```

After defining the macro, define a temporary clearinghouse or internet name, specifying the address of the port to be configured. For example, the temporary name "host_port" corresponds to the name used in the SETDefault commands in the above macro:

```
name host_port=<%Ethernetaddress!portID>
```

To configure the port, run the macro:

```
do host_conf
```

Terminal Port

The following macro is an example that contains the commands that would otherwise be executed individually to configure a VT220 terminal port:

```
define VT220_conf = (
setd (VTport) DeVice=Terminal BAud=9600 PARIty=None
setd (VTport) DataBits=8 BReakAction=(EscDTM)
setd (VTport) UseDTRin=IGnore
setd (VTport) UseDCDout=(AlwaysAssert, NoToggle)
)
```

After defining the macro, define a temporary clearinghouse or internet name, specifying the address of the port to be configured. The temporary name "VTport" corresponds to the name used in the SETDefault commands in the above macro:

```
name VTport=<%Ethernetaddress!portID>
```

To configure the port, run the macro:

```
do VT220_conf
```

Modem Port

The following macro is an example that contains the commands that would otherwise be executed individually to configure a dial-out modem port:

```
define modem_conf = (
setd (modem_port) DeVice=Host BAud=1200 PARIty=None
setd (modem_port) DataBits=8 BReakAction=IGnore
setd (modem_port) UseDTRin=AsDCD
setd (modem_port) UseDCDout=(OnConnection, ToggleonDisc)
)
```

After defining the macro, define a temporary clearinghouse or internet name, specifying the address of the port to be configured. The temporary name "modem_port" corresponds to the name used in the SETDefault commands in the above macro:

```
name modem_port=<%Ethernetaddress!portID>
```

To configure the port, run the macro:

```
do modem_conf
```

3.4.5 Sharing a Printer

The following macros show how to share a printer among hosts.

The first macro is used to check availability of the printer.

Each host's printer port is attached to a Communications Server port named, for example, lpr1, lpr2, and so on, as shown in Figure 3-1. The printer is connected to a Communications Server port named, for example, diablo. The second macro is used to establish the connection from the server port lpr1 (or lpr2) to the server port diablo.

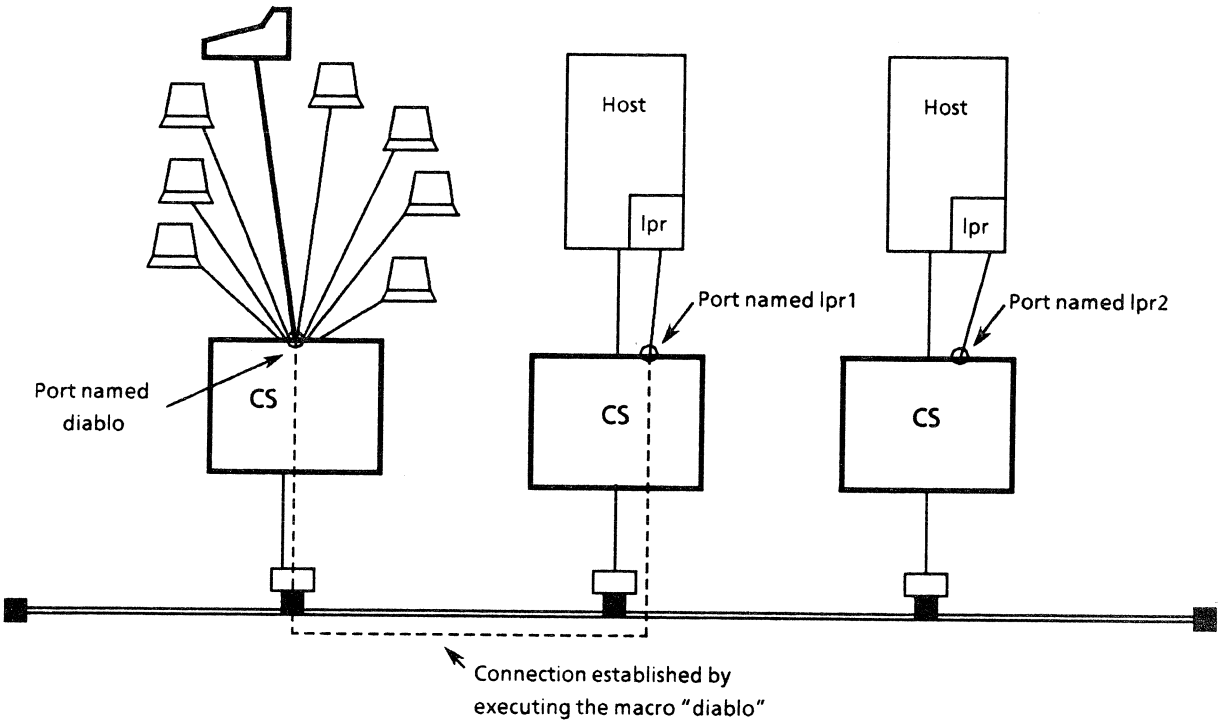


Figure 3-1 Sharing a Printer Among Hosts

To check availability of the printer, the user executes the following macro:

```
define Diablo_status = (
set interaction=nomacroecho
set privilege=user
set privilege=gnm
<password>
echo "Status of the Diablo is indicated by sessions listed"
echo "below; any session means the Diablo is unavailable:"
echo "    "
show (lpr1) sessions
pause 5
set privilege=user
set interaction=macroecho
)
```

To establish a connection from the port named lpr1 to the port named diablo, as shown in Figure 3-1, the user must execute the following macro before beginning the print operation:

```
define diablo = (
set interaction=nomacroecho
set privilege=user
set privilege=gnm
<password>
set interaction=macroecho
connect (lpr1) diablo
set priv=user
set interaction=macroecho
)
```

The AUToDisconnect interval on the server port to which the host's printer port is attached should be reduced to, for example, five minutes. This way, the connection is broken automatically five minutes after the last character of the file is printed.

These macros set the privilege level to user and then to global network manager so that if they are executed at global network manager privilege level, the line containing the password will not generate an error message.

3.4.6 Displaying Multiline Messages

The following macro displays a multiline message. Assigned as a given port's initialization macro, the macro displays its message each time the terminal enters Command mode from Listening mode. The message may be used to remind the user of the commands required to access common applications.

```
define help = (
set interaction=nomacroecho
echo " "
echo " To use the accounting system, enter"
echo " 'c accounts' and press the RETURN key."
echo " To use the word processor, enter"
echo " 'c wp' and press the RETURN key."
set interaction=macroecho
)
```

Alternatively, the WelcomeString parameter could be defined to read:

```
Hello!  Type "do help" and press RETURN for instructions.
```

The user would then enter "do help" to receive the help messages in the above macro.

3.4.7 Setting Up Connections Automatically

For some servers, such as the CS/1-BSC or CS/100-BSC, it is often necessary to establish third-party connections upon powering on the server. These connections can be established automatically using a system initialization macro like the following, where bsctermx and bschostx are clearinghouse names:

```
define bisync_setup = (
connect (bscterm1) bschost3
connect (bscterm2) bschost4
connect (bscterm3) bschost5
connect (bscterm4) bschost1
connect (bscterm5) bschost2
set priv=user
)
```

Third-party connections are also used to establish a connection between a host and printer, as shown in Section 3.4.5.

Assigned as an initialization macro for a source server, the following macro creates a connection from port 13 of the source server ("host1") to port 25 of the destination server (Ethernet address ending in "001f") whenever the source server is booted.

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

```
define init.1234 = (
connect (host1!13) &00003140%08000200001f!25
)
```

Because system initialization macros are automatically executed at global network manager privilege level, there is no need to include a command to raise the privilege level to global network manager in these macros.

3.4.8 Changing the Baud Rate on a Dial-out Modem

The following macro, assigned as the initialization macro on the port to which the dial-out modem is attached, allows the user to set the baud rate to 1200.

```
define baudset=(
connect modem1 ecm
remoteset baud=300
echo " If your modem is 300 baud, press <BREAK> within"
echo " 5 seconds and then type 'resume' to continue."
echo " If your modem is 1200 baud, wait 10 seconds "
echo " and then continue."
pause 10
remoteset baud=1200
resume
)
```

If the user presses the break key, execution of the macro is stopped, leaving the baud rate at the default. The user must then enter "resume" to continue.

3.5 Network Configuration Control Documents

This section includes examples of network management documentation related to network installation and validation.

Macro Directory

Figure 3-2 shows a portion of a macro directory. Such a directory is particularly useful in networks with no NCS. A macro directory may be maintained as a hardcopy or on-line document.

Macros are listed by macro name. Each entry includes a brief description of the macro's function and a listing of the macro's contents. The directory notes the identification codes (from the network map) for the server or port the macro serves as an initialization macro. Although the network manager may not be able to log every macro defined on the system, this directory helps avoid duplication and provides examples or standards for writing new macros.

Clearinghouse Name and Internet Name Directories

Figure 3-3 is a clearinghouse name directory. Each clearinghouse name defined on the system is listed with its associated Ethernet address and, if applicable, the port and rotary numbers. Figure 3-4 is an internet name directory. Each internet name defined on the system is listed with its internet address.

Resource Log

Figure 3-5 is a resource log. This on-line document lists every server on the network and, for each port on each server, the cable number, attached resource or user, clearinghouse or internet name, and the name of the configuration table defined for that port. If a port's configuration varies from that of the named configuration table, differences are noted. Because this is an on-line document, it is convenient to use an editor (or host commands) to locate user names, resources, and so forth.

Port Configuration Log

Figure 3-6 shows a portion of a port configuration log. The log contains the named configurations listed in the resource log. Parameters are grouped by type and listed in the order they appear on the screen. For example, the first group under the configuration named diablo is port transmission parameters, the second group is port physical parameters, and the third group is session transmission parameters.

Site Management Forms

Figures 3-7 through 3-16 show site management forms for all Bridge servers. These forms call for information such as the server's hardware, software, clearinghouse names, rotaries, and port configurations. One form should be completed and maintained for each server on the network. Table 3-1 lists the appropriate form for each type of server.

Table 3-1 Directory of Site Management Forms

Server	*Figure*	*Form Title*
CS/1	3-7	CS/1 Site Management Form
CS/100	3-8	CS/100 Site Management Form
CS/200	3-9	CS/200 Site Management Form
IVECS	3-10	IVECS Site Management Form
GS/1	3-11	GS/1 Site Management Form
GS/3	3-12	GS/3 Site Management Form
GS/4	3-13	GS/4 Site Management Form
GS/6	3-14	GS/6 Site Management Form
NCS/150	3-15	NCS/150 Site Management Form
NCS/1	3-16	NCS/1 Site Management Form

For the NCS/1, hardcopy of most management information can be created using the print utility with the SHow command, instead of being maintained manually. The following information should be printed:

- List of named configurations
- List of backup servers
- Global parameters
- List of clearinghouse names

```
"PC" sets configuration parameters for interaction with a
personal computer.
    MACRO pc = (
    set ia=nme
    p 1
    set lfp=7
    set crp=7
    p 1
    )

"Eng_versions" displays the revision levels of all Communications
Servers in the Engineering area.
    MACRO eng_versions = (
    sh (cs_1eng) version
    sh (cs_2eng) version
    sh (cs_4eng) version
    sh (cs_lab) version
    )

"Host2_to_nec" establishes a connection from Host2's third
printer port (lp3) to the NEC77.  Initialization macro for
CS/1 %080002006559.
    MACRO init.6559 = (
    do host2_to_nec
    )

    MACRO host2_to_nec = (
    set ia=nme
    set pr=u
    set pr=g
    password
    c (host2_lp3) nec77
    set pr=u
    )

"Dc_host2_nec" breaks the connection from Host2's third printer
port (lp3) to the NEC77.
    MACRO dc_host2_nec = (
    set ia=nme
    set pr=u
    set pr=g
    password
    dc (host2_lp3)
    dc (nec77)
    )
```

Figure 3-2 Portion of a Macro Directory

CLEARINGHOUSE NAMES

NAME	SERVER	PORT	ROTARY	COMMENTS
cs_1mkt	080002000b38			
cs_2mkt	080002002467			
cs_4mkt	080002005875			
cs_5bdg	08000200066b			
cs_5mkt	080002005569			
cs_6mkt	080002005868			
cs_7bdg	080002004009			
cs_7mkt	080002006559			
ncsconsole	080002000457	31		
mktlaser	080002006559	0		
nec77	080002006559	7		
vax1_lp1	08000200003a	1		
vax1async	08000200003a	5		
vax2_lp1	08000200003a	6		
vax2_lp2	08000200003a	7		
vax4_lp2	08000200003a	11		
vax4async	08000200003a	13		
vax4async	08000200003a	14		
altos_lp1	08000200003a	29		
altos_lp0	08000200003a	30		
vax3async	08000200003a	130	11-15	
altos	08000200003a	131	17-18,20-21,24-26	
hayes12	080002000405	4	128	
hayes12	080002000405	5	128	
vax1_lp2	080002000405	7		
ti810a	080002000405	8		
diablo	080002000405	9		
cs_x25	080002000017			
vax1	080002000017	0	128	
vax1	080002000017	128	0-23	
ncs1	080002003471			
ncs150	080002000b26			
ncslocterm	080002000b26	0		
ncsbu	080002002902			

Figure 3-3 Clearinghouse Name Directory

INTERNET NAMES

NAME	SERVER	PORT	ROTARY	COMMENTS
altos	192.9.200.030	131	17-18,20-21,24-26	
altos_lp1	192.9.200.128	29		
altos_lp0	192.9.200.052	30		
mktlaser	192.9.200.223	0		
vax1_lp1	192.9.200.080	1		
vax1async	192.9.200.104	5		
cs_7mkt	192.9.200.228			
vax2_lp1	192.9.200.121	6		
vax4_lp2	192.9.200.217	11		
vax2_lp2	192.9.200.004	7		
vax4async	192.9.200.060	13		
vax4async	192.9.200.142	14		
cs_1mkt	192.9.200.105			
cs_2mkt	192.9.200.030			
cs_4mkt	192.9.200.248			
cs_5bdg	192.9.200.040			
cs_5mkt	192.9.200.199			
cs_6mkt	192.9.200.161			
cs_7bdg	192.9.200.200			
vax3async	192.9.200.170	130	11-15	
hayes12	192.9.200.182	4	128	
hayes12	192.9.200.110	5	128	
vax1_lp2	192.9.200.207	7		
ti810a	192.9.200.134	8		
diablo	192.9.200.232	9		
vax1	192.9.200.140	128	0-23	
ncs150	192.9.200.109			
ncsbu	192.9.200.058			

Figure 3-4 Internet Name Directory

```
Server cs_1adm (077e)
Serial: 1052   Map code: A02

port cable  resource          ch name          config.

!0   1a0    A. Sparkelon                      term
!1   1a1    G. Reagal                         term
!2   1a2                                      term
!3   1a3    R. McLaughlin                     term
!4   1a4    K. Fretzman                       term
!5   1a5                                      term
!6   1a6                                      term
!7   1a7                                      term
!8   1a8                                      term
!9   1a9                                      term
!10  1a10                                     term
!11  1a11                                     term
!12  1a12                                     term
!13  1a13                                     term
```

```
Server cs_1mkt (0b27)
Serial: 0920   Map code: M02

port cable  resource          ch name          config.

!0   1m0    K. Libman                         term
!1   1m1    D. Kaufmann                       term
!2   1m2                                      term
!3   1m3    Operator                          term
!4   1m4    C. Jackson                        term
!5   1m5    L. Chou                           term
!6   1m6    data entry                        term
!7   1m7    data entry                        term
!8   1m8    data entry                        term
!9   1m9                                      term
!10  1m10                                     term
!11  1m11                                     term
!12  1m12                                     term
!13  1m13                                     term
```

Figure 3-5 Resource Log

```
Server cs_2adm (5958)
Serial: 2037   Map code: A01

port cable  resource          ch name        config.

!0   2a0    H. Remington                    term
!1   2a1    Common File                     term
!2   2a2    D. Dunn                         term
!3   2a3    F. Schyler                      term
!4   2a4                                    term
!5   2a5                                    term
!6   2a6    J. Gonder                       term
!7   2a7    E. Comeaux                      term
!8   2a8    R. Best                         term
!9   2a9                                    term
!10  2a10                                   term
!11  2a11                                   term
!12  2a12                                   term
!13  2a13                                   term
```

```
Server cs_2mkt (1638)
Serial: 2037   Map code: M01

port cable  resource          ch name        config.

!0   2m0    S. Luster                       term
!1   2m1    consultant                      term
!2   2m2    L.R. Chambers                   term
!3   2m3                                    term
!4   2m4                                    term
!5   2m5    J. McVitty                      term
!6   2m6    J. Amundson                     term
!7   2m7    D. Krage                        term
!8   2m8    W. O'Riley                      term
!9   2m9    W. Flinston                     term
!10  2m10   B. Hoolihan                     term
!11  2m11   R. Zimmerman                    term
!12  2m12   I. Reinarz                      term
!13  2m13   J. Graber                       term
```

Figure 3-5 Resource Log (continued)

```
Server cs_hosts1 (02a6)
Serial: 1222   Map code: C01

port cable  resource          ch name          config.

!0          local term                         term
!1   25     vax1 tty00        vax1_lp1         host au=d
!2   26     vax1 tty01        ktest1           host
!3   27     vax1 tty02        vax1_uuo         host fcf=fct=d au=d
!4   28     vax1 tty03        vax1_uui         host fcf=fct=d au=d
!5   29     vax1 tty04        vax1async        host
!6   30     vax2 ttyh0        vax2_lp1         host au=d
!7   31     vax2 ttyh1        vax2_lp2         host au=d
!8   32     vax2 ttyh2        vax2_uuo         host fcf=fct=d au=d
!9   33     vax2 ttyh3        vax2_uui         host fcf=fct=d au=d
!10  34     vax2 ttyh4        vax2_lp3         host au=5
!11  35     vax4 tty01        vax4_lp2         host
!12  36     vax4 tty02        ktest4           host
!13  37     vax4 tty03        vax4async        host
!14  38     vax4 tty04        vax4async        host
!15  39     vax4 tty05        bridgenet        term
!16  EA     vax2 tty0a        vax2_lp4(cjh)    host
!17  41     altos tty01                        host
!18  42     altos tty02                        host
!19  43     altos tty03                        host
!20  44     altos tty04                        host
!21  45     altos tty05                        host
!22  51     vax2 ttyh8                         host
!23  EE     altos tty07                        host
!24  3      altos tty08                        host
!25  4      altos tty09                        host
!26  5      altos tty10                        host
!27  6      altos tty11                        host
!28  7      altos tty12       altos_uuo        host fcf=fct=d au=d
!29  8      altos tty13       altos_lp1        host
!30  9      altos tty14       altos_lp0        host au=d
!31  10     altos tty15                        host
```

Figure 3-5 Resource Log (continued)

```
Server cs_7mkt (1945)
Serial: 1027   Map code: M03

port cable  resource          ch name        config.

!0   7m0    laser printer     mktlaser       host
!1   7m1    TI810 printer     WP810a         host
!2   7m2                                     term
!3   7m3                                     term
!4   7m4    D. Ferrand                      term
!5   7m5    D. Jacobson                     term
!6   7m6    TI810 printer     WP810b         host
!7   7m7    NEC77 printer     nec77          term
!8   7m8    mkt TI810 printer mkt810         term
!9   7m9                                     term
!10  7m10                                    term
!11  7m11                                    term
!12  7m12                                    term
!13  7m13                                    term
```

```
Server cs_modem2 (0405)
Serial: 1018   Map code: C02

port cable  resource          ch name        config.

!0   5      local term                      term
!1   E23    Modtech 9401923                 modem_in ba=300
!2   E22    Hayes12 9401922                 modem_in ba=l_ab
!3   E21    Hayes12 9401921                 modem_in ba=l_ab
!4   E19    Hayes3 9401919    hayes12       modem_out ba=1200
!5   E20    Hayes12 9401920   hayes12       modem_out ba=1200
!6   E24    Hayes12 9692596                 modem_in ba=l_ab
!7   56     vax1ttyh2         vax1_lp2      host audt=d
!8   21     TI810             ti810a        ti810a
!9   23     diablo            diablo        diablo au=5
```

Figure 3-5 Resource Log (continued)

```
Server ncs1 (3471)
Serial: 1007   Map code: C03

port cable  resource          ch name         config.

ttya        cs_xxx!7
ttyb        cs_xxx!8
ttys0       epson printer
ttys1       laser writer
ttys2
ttys3
```

```
Server ncs150 (0b26)
Serial: 1359   Map code: C04

port cable  resource          ch name         config.

!0   5      cs_eng4!24        ncslocterm      term
!1   e      Oki printer                       host
```

Figure 3-5 Resource Log (continued)

```
CONFIGURATION FOR diablo
AccessGroup = 1
AUtodisconnect = 15
BUffersize = 82
DeVice = Host, Glass
BAud = 1200
BSPad = None
CRPad = None
FFPad = None
LFPad = None
TabPad = None
DataBits = 8
LinePRotocol = ASynchronous
PARIty = None
StopBits = 1
UseDCDout = ( OnConnection, NoToggle )
UseDTRin = Ignore
```

Figure 3-6 Port Configuration Log

```
BReakAction = ( InBand )
DataForward = None
ECHOData = OFF
ECHOMask = ( AlphaNum, CR, Term, Punct )
EOM = Disabled
FlowControlFrom = Xon_Xoff
FlowControlTo = Xon_Xoff
IdleTimer = 1
XOFF = ^S
XON = ^Q

CONFIGURATION FOR host
AccessGroup=( 1 )
AUtodisconnect = 15
BUffersize = 82
DeVice = ( Host, Glass )

BAud = 9600
BSPad = None
CRPad = None
FFPad = None
LFPad = None
TabPad = None
DataBits = 8
DUplex = Full
LinePRotocol = ASynchronous
PARIty = None
StopBits = 1
UseDCDout = ( AlwaysAssert, NoToggle )
UseDTRin = Ignore

BReakAction = ( InBand )
DataForward = None
ECHOData = OFF
ECHOMask = ( AlphaNum, CR, Term, Punct )
EOM = Disabled
FlowControlFrom = Xon_Xoff
FlowControlTo = Xon_Xoff
IdleTimer = 1
XOFF = ^S
XON = ^Q
```

Figure 3-6 Port Configuration Log (continued)

```
CONFIGURATION FOR term

AccessGroup = ( 1 )
AccessWord = ( 1 )
BUffersize = 82
DeVice = ( Terminal, Glass )
InterAction = ( Verbose, Echo, MacroEcho, BroadcastON, NoLFInsert )
InitMacro = ""
MaxSessions = 2
PRIvilege = User

BAud = 9600
BSPad = None
CRPad = None
FFPad = None
LFPad = None
TabPad = None
DataBits = 8
DUplex = Full
LinePRotocol = ASynchronous
PARIty = None
StopBits = 1
UseDCDout = ( AlwaysAssert, NoToggle )
UseDTRin = Ignore

BReakAction = ( InBand )
BReakChar = Disabled
DataForward = None
ECHOData = OFF
ECHOMask = ( AlphaNum, CR, Term, Punct )
ECMChar = ^^
EOM = Disabled
FlowControlFrom = Xon_Xoff
FlowControlTo = Xon_Xoff
IdleTimer = 2
LFInsertion = None
MOde = Transparent
XOFF = ^S
XON = ^Q

ERase = ^H
LineERase = ^U
LocalEDiting = ( DataEditing, CmdEditing )
ReprintLine = ^R
VERBatim = ^V
WordERase = ^W
```

Figure 3-6 Port Configuration Log (continued)

CS/1 SITE MANAGEMENT FORM
(Page 1 of 2)

HARDWARE

Serial #_____ Ethernet/IP Addresses:
Date Installed:_____ _____
Location:_____ _____
Service Record:_____
_____
_____

Slot	Board	PROMs	Rev	Notes
A	_____	_____	_____	_____
B	EC/2	M__EDL_____	_____	_____
C	MCPU	M__MMON_____	_____	_____
D	FDC	n/a	_____	_____
E	_____	_____	_____	_____
F	_____	_____	_____	_____
G	_____	_____	_____	_____
H	_____	_____	_____	_____

SOFTWARE

SW/_____
Date Installed:_____ Date Backed up:_____

CLEARINGHOUSE/INTERNET NAMES

Server name:_____
Other names:_____=_____
_____=_____ _____=_____
_____=_____ _____=_____

ROTARIES

!128=_____ !128=_____
!129=_____ !129=_____
!130=_____ !130=_____
!131=_____ !131=_____

Figure 3-7 CS/1 Site Management Form

CS/1 SITE MANAGEMENT FORM (Page 2)

PORT CONFIGURATION

Port	Resource	Configuration	Name	Initmacro
!0				
!1				
!2				
!3				
!4				
!5				
!6				
!7				
!8				
!9				
!10				
!11				
!12				
!13				
!14				
!15				
!16				
!17				
!18				
!19				
!20				
!21				
!22				
!23				
!24				
!25				
!26				
!27				
!28				
!29				
!30				
!31				

Figure 3-7 CS/1 Site Management Form (continued)

CS/100 SITE MANAGEMENT FORM

HARDWARE

Serial #_____ Ethernet/IP Addresses:
Date Installed:_____ _____
Location:_____ _____
PROMs: T__MMON_____ T__ASYN_____
Service Record:_____
_____
_____

SOFTWARE

SW/_____
Date Installed:_____ Date Backed up:_____

CLEARINGHOUSE/INTERNET NAMES

Server name:_____
Other names:_____=_____
_____=_____ _____=_____
_____=_____ _____=_____

ROTARIES

!128=_____ !130=_____
!129=_____ !131=_____

PORT CONFIGURATION

Port	Resource	Configuration	Name	Initmacro
!0				
!1				
!2				
!3				
!4				
!5				
!6				
!7				
!8				
!9				
!10				
!11				
!12				
!13				

Figure 3-8 CS/100 Site Management Form

CS/200 SITE MANAGEMENT FORM

HARDWARE

Serial #_____ Ethernet Address:
Date Installed:_____ %_____
Location:_____
PROM: C__MMON_____
Service Record:_____
_____
_____

FIRMWARE CONFIGURATION

Monitor port #_____
Reboot option: Boot monitor___ Upload then boot___ Reboot only___

SOFTWARE

SW/200-A Version:_____
Date Installed:_____ Date Backed up:_____

CLEARINGHOUSE NAMES

Server name:_____
Other names:_____=_____
_____=_____ _____=_____
_____=_____ _____=_____

ROTARIES

!128=_____ !130=_____
!129=_____ !131=_____

PORT CONFIGURATION

Port	Resource	Configuration	Name	Initmacro
!0				
!1				
!2				
!3				
!4				
!5				
!6				
!7				
!8				
!9				

Figure 3-9 CS/200 Site Management Form

IVECS SITE MANAGEMENT FORM
(Page 1 of 2)

HARDWARE

Serial #_____ Ethernet Address:
Date Installed:_____ %_____
VAX Name/Model:_____ #DMFs Emulated:_____
PROMs: U1__MMON_____ DMF-A_____

Service Record:_____
_____
_____

SOFTWARE

SW/_____
Date Installed on NCS:_____ Date Backed up:_____

CLEARINGHOUSE/INTERNET NAMES

Server name:_____

Other names:_____=_____
_____=_____ _____=_____
_____=_____ _____=_____

ROTARIES

!128=_____ !132=_____
!129=_____ !133=_____
!130=_____ !134=_____
!131=_____ !135=_____

Figure 3-10 IVECS Site Management Form

IVECS SITE MANAGEMENT FORM (Page 2)

VIRTUAL PORT CONFIGURATION

Port	Configuration	Port	Configuration
!0		!32	
!1		!33	
!2		!34	
!3		!35	
!4		!36	
!5		!37	
!6		!38	
!7		!39	
!8		!40	
!9		!41	
!10		!42	
!11		!43	
!12		!44	
!13		!45	
!14		!46	
!15		!47	
!16		!48	
!17		!59	
!18		!60	
!19		!51	
!20		!52	
!21		!53	
!22		!54	
!23		!55	
!24		!56	
!25		!57	
!26		!58	
!27		!59	
!28		!60	
!29		!61	
!30		!62	
!31		!63	

Figure 3-10 IVECS Site Management Form (continued)

GS/1 SITE MANAGEMENT FORM

HARDWARE

Serial #_____ Ethernet Address:
Date Installed:_____ %_____
Location:_____
Service Record:_____
_____
_____

Slot	Board	PROMs	Rev	Notes
A	_____	_____	_____	_____
B	EC/2	M__EDL_____	_____	_____
C	MCPU	M__MMON_____	_____	_____
D	FDC	n/a	_____	_____
E	_____	_____	_____	_____
F	_____	_____	_____	_____
G	_____	_____	_____	_____
H	_____	_____	_____	_____

SOFTWARE

SW/_____
Date Installed:_____ Date Backed up:_____

CLEARINGHOUSE/INTERNET NAMES

Server name:_____
Other names:_____=_____
_____=_____ _____=_____
_____=_____ _____=_____

ROTARIES

!128=_____ !132=_____
!129=_____ !133=_____
!130=_____ !134=_____
!131=_____ !135=_____

Figure 3-11 GS/1 Site Management Form

GS/1 SITE MANAGEMENT FORM (Page 2)

VIRTUAL PORT CONFIGURATION

Port	Configuration	Line	Port	Configuration	Line
!0			!24		
!1			!25		
!2			!26		
!3			!27		
!4			!28		
!5			!29		
!6			!30		
!7			!31		
!8			!32		
!9			!33		
!10			!34		
!11			!35		
!12			!36		
!13			!37		
!14			!38		
!15			!39		
!16			!40		
!17			!41		
!18			!42		
!19			!43		
!20			!44		
!21			!45		
!22			!46		
!23			!47		

LINE ADDRESSES

Line	Address	Characteristics
0		
1		
2		
3		
4		
5		
6		
7		

LINE MAPPING

Port No.s	Line No.	Line Location

Figure 3-11 GS/1 Site Management Form (continued)

GS/3 SITE MANAGEMENT FORM

HARDWARE

Serial #_____ Ethernet Address:
Date Installed:_____ %_____
Location:_____
Service Record:_____

Slot	Board	PROMs	Rev	Notes
A				
B	EC/2	M__EDL_____		
C	MCPU	M__MMON_____		
D	FDC	n/a		
E				
F				
G				
H				

SOFTWARE

SW/_____
Date Installed:_____ Date Backed up:_____

CLEARINGHOUSE/INTERNET NAMES

Server name:_____
Other names:_____=_____
_____=_____ _____=_____
_____=_____ _____=_____

LOCAL NETWORK ADDRESS:_____

LINE CHARACTERISTICS

Line	Baud	Clock Source		Remote Network ID
0	____	Xmit:_____	Rcv:_____	_____
1	____	Xmit:_____	Rcv:_____	_____
2	____	Xmit:_____	Rcv:_____	_____
3	____	Xmit:_____	Rcv:_____	_____
4	____	Xmit:_____	Rcv:_____	_____
5	____	Xmit:_____	Rcv:_____	_____
6	____	Xmit:_____	Rcv:_____	_____
7	____	Xmit:_____	Rcv:_____	_____

Figure 3-12 GS/3 Site Management Form

GS/4 SITE MANAGEMENT FORM

HARDWARE

Serial #_____ Ethernet Address:
Date Installed:_____ %_____
Location:_____

Service Record:_____
_____
_____

Slot	Board	PROMs	Rev	Notes
A	_____	_____	_____	_____
B	EC/2	M__EDL_____	_____	_____
C	MCPU	M__MMON_____	_____	_____
D	FDC	n/a	_____	_____
E	_____	_____	_____	_____
F	_____	_____	_____	_____
G	_____	_____	_____	_____
H	EC/2	M__EDL_____	_____	_____

SOFTWARE

SW/_____
Date Installed:_____ Date Backed up:_____

CLEARINGHOUSE/INTERNET NAMES

Server name:_____
Other names:_____=_____
_____=_____ _____=_____
_____=_____ _____=_____

NETWORK ADDRESSES

Local: _____
Remote: _____

Figure 3-13 GS/4 Site Management Form

GS/6 SITE MANAGEMENT FORM

HARDWARE

Serial #_____ Ethernet Address:
Date Installed:_____ %_____
Location:_____
Service Record:_____

Slot	Board	PROMs	Rev	Notes
A				
B	EC/2	M__EDL_____		
C	MCPU	M__MMON_____		
D	FDC	n/a		
E				
F				
G				
H	HSM-MDM			

SOFTWARE

SW/_____
Date Installed:_____ Date Backed up:_____

CLEARINGHOUSE/INTERNET NAMES

Server name:_____
Other names:_____=_____
_____=_____ _____=_____
_____=_____ _____=_____

LOCAL NETWORK ADDRESSES

Local Network Address:_____
Local Link Address:_____

REMOTE NETWORK ADDRESSES

Network Address	Link Address

Figure 3-14 GS/6 Site Management Form

NCS/150 SITE MANAGEMENT FORM
(Page 1 of 2)

HARDWARE

Serial #_____
Date Installed:_____
Location:_____
PROMs: T_MMON_____
T_ASYN_____
Service Record:_____
_____
_____

Ethernet/IP Addresses:
_____
_____

SOFTWARE

SW/_____
Date Installed:_____

Date Backed up:_____

CLEARINGHOUSE/INTERNET NAMES

Server name:_____

PORT CONFIGURATION

!0 BAud:_____ DataBits:_____ FlowControl:_____
PARIty:_____ StopBits:_____

!1 BAud:_____ DataBits:_____ FlowControl:_____
PARIty:_____ StopBits:_____

Figure 3-15 NCS/150 Site Management Form

NCS/150 SITE MANAGEMENT FORM (Page 2)

BOUND SERVERS

System	Ethernet Address	Internet Address (if applicable)	Name	Model/File
0	%			
1	%			
2	%			
3	%			
4	%			
5	%			
6	%			
7	%			
8	%			
9	%			
10	%			
11	%			
12	%			
13	%			
14	%			
15	%			
16	%			
17	%			
18	%			
19	%			
20	%			
21	%			
22	%			
23	%			
24	%			
25	%			
26	%			
27	%			
28	%			
29	%			
30	%			
31	%			
32	%			
33	%			
34	%			
35	%			
36	%			
37	%			
38	%			
39	%			

Figure 3-15 NCS/150 Site Management Form (continued)

NCS/1 SITE MANAGEMENT FORM

HARDWARE

Serial #_____ Ethernet/IP Addresses:
Date Installed:_____ _____
Location:_____ _____
Service Record:_____
_____
_____

SOFTWARE

SW/_____
Date Installed:_____ Date Backed up:_____

CLEARINGHOUSE/INTERNET NAMES

Server name:_____

PORT CONFIGURATION

ttya Attached device:_____ Baud:_____
ttyb Attached device:_____ Baud:_____

ttys0 Baud:_____ ttys2 Baud:_____
ttys1 Baud:_____ ttys3 Baud:_____

Figure 3-16 NCS/1 Site Management Form

4.0 NETWORK OPERATION

This section describes the documentation that the network manager should maintain and provides procedures for preventive maintenance and troubleshooting.

4.1 Network Management Documentation

The network manager should maintain current, accurate, complete documentation concerning all aspects of the network. Documentation that is maintained on-line should be printed periodically, so that the hardcopy is available in case of network service interruption.

Table 4-1 lists the network management documents described elsewhere in this manual.

Table 4-1
Network Management Documents

Document	*On-line or Hardcopy*	*Section*
Network map	hardcopy	2.8
Site management forms (1 per server)	hardcopy	3.5
Clearinghouse/internet name directory	on-line	3.5
Port configuration log	on-line	3.5
Network problem report	hardcopy	4.6

In addition to the documents listed in Table 4-1, the following documents have been found to be useful:

- Operation log: Many problems occur when connectors or transceivers are changed or installed. The problem can often be isolated by matching symptoms with the most recent log entries.
- Hardcopies: Macros, named configurations, and clearinghouse names with the associated addresses. Maintaining hardcopies of TDR graphs is suggested, as described in Section 2.2.1.
- Hardware list: Servers, repeaters, and transceivers, and spare hardware such as servers, boards, power supplies, fans, and cables. The list should include each element's location or be keyed to the Network Map. Also include each element's Ethernet addresses, serial numbers, and revision levels of boards and PROMs, as applicable.
- Statistics snapshot: As a basis of comparison, busiest sample and 24-hour average statistics for each server on the network or for a sample of servers should be displayed and recorded weekly. The NCS/1 can be used to print hardcopies or maintain an on-line record of these weekly statistics snapshots.
- Log of reported problems and solutions: Can be studied to identify trends and referred to for solutions to future problems.

The network manager should also maintain current backup software for each server. Label each backup diskette or tape cartridge with the date of creation and version level.

4.2 Network Management Reports

Bridge servers maintain network management reports that record statistics regarding, for example, connection requests, error counts, and security statistics. This section describes these reports. Most servers maintain six reports. The first four reports list performance statistics for the following intervals:

- The busiest sample
- The busiest minute
- Averages for a specified hour
- Averages for the prior 24-hour period

The NCS/150 and NCS/1 also show statistics for the most recent week and for the period since the NCS was last booted. For information on these reports, refer to the appropriate *NCS Installation and Operation Guide* (reference [7] or [8]).

The fifth report summarizes all of the above statistics for a specified single port. The sixth report shows which ports have accessed higher privilege levels or devices outside of their own groups and how many times an incorrect password was given for these actions.

The network management reports for the current reporting period are obtained using the SHow command. The *Connection Service User's Guide* (reference [10]) describes command format and syntax of the SHow command.

Figure 4-1 shows the periods covered by the various reports. The busiest samples and minutes statistics are zeroed every midnight, so they cover the period from the most recent midnight to the current moment. The 24-hour average report (SHow STATistics Day) includes the 24 hours from midnight-to-midnight of the preceding day. Security statistics are recorded and accumulate from the time of the most recent power-on or reset up to the current moment.

For the hour average report, if the specified hour is earlier than the current hour, the resulting report lists statistics gathered for the specified hour during the current day; if the specified hour is later than the current hour, the resulting report lists statistics from the corresponding hour during the previous day. For example, if a report is requested at 4:00 p.m. specifying statistics for 6:00 p.m. (entered as "18"), the resulting report lists statistics for the hour from 6:00 p.m. to 7:00 p.m. the previous day.

All servers retain busiest minutes, busiest sample, hour average, and 24-hour average statistics for up to 24 hours starting at the time of the most recent power-on or system reset. Statistics gathered between midnight of one day and a power-on or reset the following day are discarded, and statistics gathered earlier than the most recent midnight are overwritten as new information is gathered.

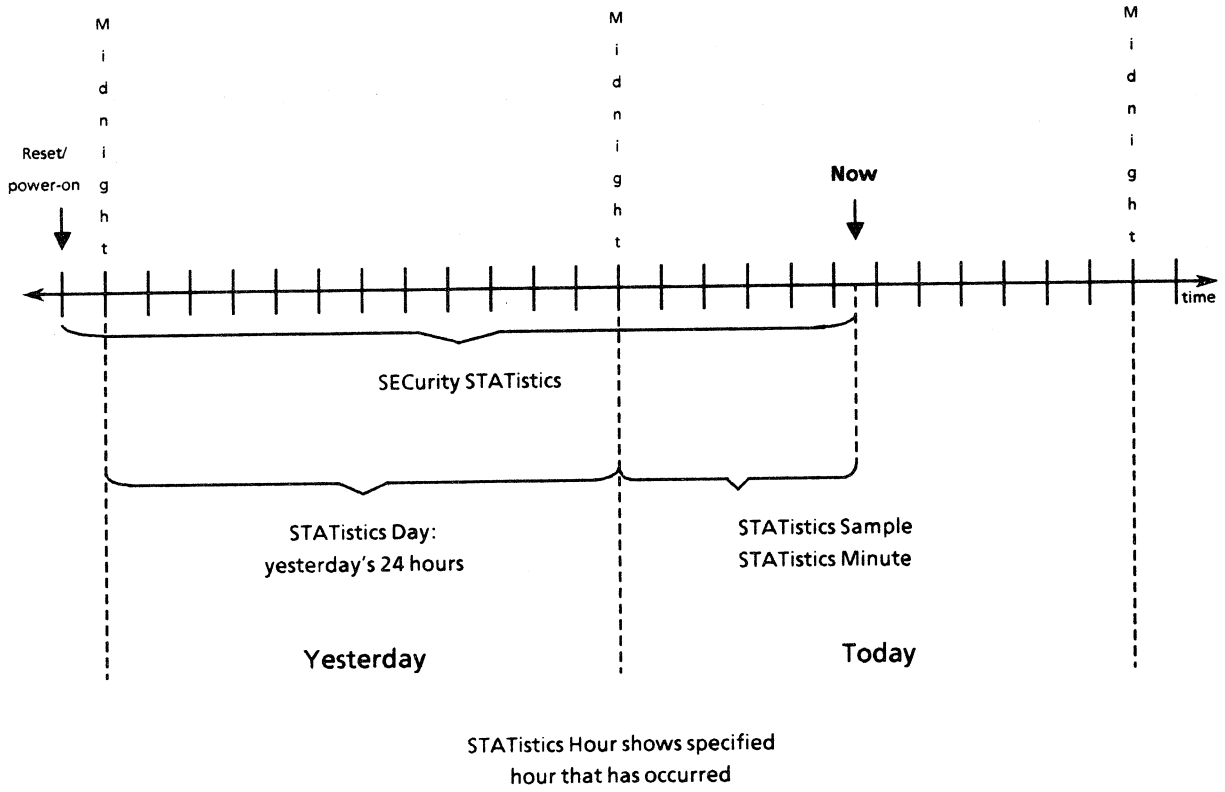


Figure 4-1 Network Management Reports Timeline

To establish a basis of comparison, busiest sample and 24-hour average statistics for each server on the network or for a sample of servers should be displayed and recorded weekly. The NCS/1 can be used to print hardcopies or maintain an on-line record of these weekly statistics snapshots.

Statistics reports on various servers may differ slightly from those shown in this section. For example, reports on the CS/200 do not include disk access errors or statistics for the monitor port; reports on the NCS/1 include Ethernet utilization during the reporting period.

**** NOTES ****

Statistics are available for all physical ports and for all CS/1-HSM, CS/1-SNA, and IVECS virtual ports. For CS/1-X.25 and CS/100-488 virtual ports, and for any virtual ports defined on servers that normally provide only physical ports, only the security statistics report described in Section 4.2.6 is available.

The physical port numbers on a GS/1 are 0, 1, 8, and 9, and on a GS/3 are 0, 1, 8, 9, 15, 16, 24, and 25. Reference [10] defines physical ports and virtual ports.

For the CS/1-X.25 and GS/1, the word "session" refers to an X.25 logical channel, not to a virtual circuit. Thus the listed maximum number of sessions never exceeds the aggregate maximum number of logical channels specified in Sysgen (default 20 per line). The word "call" in this context refers to the creation of a logical channel.

**** NOTE ****

For the GS/3 Interconnection Service, the word "session" refers to activity on a physical line, rather than to a virtual circuit. Thus the listed maximum number of sessions never exceeds the number of lines attached to the GS/3. The word "call" in this context is applicable only to an outgoing call placed by a switched-line modem.

All of the examples in the following subsections include an address field in the command. If the address is omitted, the address of the local server is assumed. Only a Global Network Manager may display statistics for a remote server.

The reports use the following abbreviations:

2LON	packet too long
2SHT	packet too short
AcuDskEr	accumulated disk access errors
ALN	alignment error
BUF	buffer (shared memory) usage
BYTE/S	bytes per second
BootReq	bootstrap requests
BUF	server's buffer usage
CALL/D	call requests per day
CALL/H	call requests per hour
CALL/M	call requests per minute
ChgGrp	port accessed resource in a different group
CHReq	clearinghouse requests
COLL	packet collisions
CPU	server's main processor (MP or MCPU) usage
CRC	packet receive error
DskAcc	disk accesses
DskErr	disk access errors
DskReq	disk requests
ERR	errors
ERR/D	errors per day
ERR/H	errors per hour
ERR/M	errors per minute
ERR/W	errors per week
ERROR	accumulated errors
FilReq	file requests
MAX	SN
MxPr	maximum privilege level reached
PKT/S	packets per second
SetPr	SET PRIVilege command executed successfully
Unsc	unsuccessful command

4.2.1 Busiest Samples of the Day Report

This report summarizes the busiest intervals since the most recent midnight, as shown in Figure 4-1. The length of the interval may be set at the time of system generation to a value in the range 2 to 10 seconds, inclusive. The default value is 4 seconds.

To display this report, use the following command:

```
SHow (<address>) STATistics Sample
```

For example, the following command displays the busiest sample statistics of a remote server with the Ethernet address %080002000018:

```
sh (%080002000018) stat s
```

This report is not available on the NCS/150 or NCS/1. On the NCS/1, a similar report is displayed by entering the following command:

```
SHow STATisticS Current
```

Figure 4-2 shows an example of the Busiest Samples report.

The report is grouped into three areas. The first area lists statistics for the overall server, including the highest percentage of CPU and buffer use, the highest number of simultaneous sessions, the highest number of data packets transmitted/received per second, and the highest number of bytes transmitted/received per second. The report lists the times (in the format "hhmm") at which each maximum occurred and includes a count of disk access errors. The disk error count is a cumulative count for the current day.

The second area of the report lists statistics for the I/O interface portion of the server and includes a per-port report of the highest sample of simultaneous sessions, highest number of packets per second, highest sample of bytes per second, and highest sample of line access errors in one second. This area of the report does not list the times of each maximum. If a CS/1 contains different kinds of interface boards (e.g., both an SIO-A board and an SIO-SM board), this part of the report is broken down into separate listings for the SIO-A ports and the SIO-SM ports.

The third area of the report lists statistics for the Ethernet interface portion of the server. The statistics include the highest sample of packets per second and bytes per second transmitted to/from the Ethernet by this Communications Server and a breakdown of Ethernet errors. The Ethernet errors are listed in five categories: CRC, alignment, packet-too-short, packet-too-long, and collision errors. The itemized error list represents the cumulative count for the reporting period, not a maximum. The Ethernet port number is the network identification number. In a network that is not interconnected with other networks, this number is usually 0.

```
BUSIEST SAMPLES OF THE DAY ----------------------

TOTAL CPU(%)  BUF(%)  MAX#SN  PKT/S  BYTE/S  AcuDskEr
VALUE 75      40      12      150    70K     0
TIME  1005    1030    1015    1005   1005

PORT MAX#SN PKT/S BYTE/S ERR   PORT MAX#SN PKT/S BYTE/S ERR
0    4      40    520     0     1    1      4     100     0
2    2      3     90      0     3    1      50    5000    0
4    0      0     0       0     5    0      0     0       0
6    0      0     0       0     7    0      0     0       0

Ethernet PORT PKT/S BYTE/S ERROR: CRC ALN 2SHT 2LON COLL
         0    100   6000          8   6   0    0    24
```

Figure 4-2 Busiest Samples of the Day Report

The statistics for the busiest sample (and busiest minutes) may be set to zero using the ZeroStats command, providing a starting point for analysis of the report.

Accumulated Ethernet statistics should be monitored carefully for tracking of overall network traffic. Section 4.2.7 gives guidelines for interpreting network management reports.

4.2.2 Busiest Minutes of the Day Report

This report summarizes server performance during the busiest one-minute intervals since the most recent midnight, as shown in Figure 4-1. To display this report, use the following command:

```
SHow (<address>) STATistics Minute
```

For example, the following command displays the busiest minutes statistics of a remote CS/1-TCP with the internet address 192.9.200.1:

```
sh (192.9.200.1) stat m
```

Figure 4-3 contains an example of the Busiest Minutes report.

This report is similar to the Busiest Samples report, except that the busiest minutes report indicates the number of calls per minute rather than the number of simultaneous sessions. A call is a request for a connection.

All Ethernet errors listed represent the maximum, not a cumulative count. For each statistic in the report, the number is the maximum reached during any of the minutes of the current 24-hour period. Each statistic does not necessarily cover the same minute.

```
BUSIEST MINUTES OF THE DAY --------------------

TOTAL CPU(%)  BUF(%)  CALL/M  PKT/S  BYTE/S
VALUE 75      40      12      120    60K
TIME  1005    1030    1015    1005   1005

PORT CALL/M PKT/S BYTE/S ERR/M  PORT CALL/M PKT/S BYTE/S ERR/M
0    4      5     100    0      1    1      16    300    0
2    2      10    120    0      3    1      4     105    0
4    0      0     0      0      5    0      0     0      0
6    0      0     0      0      7    0      0     0      0

Ethernet PORT PKT/S BYTE/S ERR/M: CRC ALN 2SHT 2LON COLL
         0    100   6000          1   1   0    0    1
```

Figure 4-3 Busiest Minutes of the Day Report

The statistics for the busiest minutes (and busiest sample) may be set to zero using the ZeroStats command, providing a starting point for analysis of the report.

Accumulated Ethernet statistics should be monitored carefully for tracking of overall network traffic. Section 4.2.7 gives guidelines for interpreting network management reports.

4.2.3 Hour Average Report

This report shows the average network load for the specified one-hour interval. The hour is entered as a number in the range 0 to 23, inclusive.

On networks with an NCS, the date and time of all servers on the network is automatically synchronized to the NCS's date and time. On networks with no NCS, when a server is powered on or reset its date and time is set to 16:00:00 on December 31, 1969. This time is used as the basis for the 24-hour cycle unless the SET DATE command is used to set the system clock to the current date and time.

To display this report, use the following command:

```
SHow (<address>) STATistics <h>
```

For example, the following command displays statistics for the hour from noon to 1:00 for a remote server with the Ethernet address %0800020001FF:

```
sh (%0800020001FF) stat 12
```

On an NCS/1, statistics for the previous hour only may be displayed. The following command is used:

```
SHow STATisticS Hour
```

Figure 4-4 contains an example of the Hour Average report.

Like the Busiest Minutes report, the Hour Average report groups information into three areas: the overall server, the I/O interface, and the Ethernet interface for the reporting interval (in this case, a specified hour).

This report is useful for pinpointing when a network disturbance occurred.

The Ethernet portion of the report lists the errors for the hour of the report, not a cumulative total or the maximums.

```
HOUR AVERAGE FROM 12:00 to 12:59 ------------------

TOTAL CPU(%)  BUF(%)  CALL/H  PKT/S  BYTE/S
VALUE 75      40      12      120    60K

PORT CALL/H PKT/S BYTE/S ERR/H  PORT CALL/H PKT/S BYTE/S ERR/H
0    4      4     10     0      1    1      4     10     0
2    1      2     140    0      3    1      3     120    0
4    1      5     200    0      5    0      0     0      0
6    3      4     80     0      7    2      4     11     0

Ethernet PORT PKT/S BYTE/S ERR/H: CRC ALN 2SHT 2LON COLL
         0    100   6000          0   0   0    0    1
```

Figure 4-4 Hour Average Report

Accumulated Ethernet statistics should be monitored carefully for tracking of overall network traffic. Section 4.2.7 gives guidelines for interpreting network management reports.

4.2.4 24-Hour Average Report

This report summarizes the average network load for the prior day, as shown in Figure 4-1. To display this report, use the following command:

```
SHow (<address>) STATistics Day
```

For example, the following command displays the day statistics for the server on which the command is entered:

```
sh stat d
```

Figure 4-5 illustrates an example of the Yesterday's 24-Hour Average report.

Like the Busiest Minutes and Hour Average reports, the 24-Hour Average report groups information into three areas: the overall server, the I/O interface, and the Ethernet interface.

```
YESTERDAY'S 24 HOUR AVERAGE ----------------

TOTAL CPU(%)  BUF(%)  CALL/D  PKT/S  BYTE/S
VALUE 75      40      120     40     980

PORT CALL/D PKT/S BYTE/S ERR/D  PORT CALL/D PKT/S BYTE/S ERR/D
0    4      4     10     0      1    10     4     10     0
2    2      4     10     0      3    10     4     10     0
4    0      0     0      0      5    2      4     11     0
6    3      4     8      0      7    10     2     20     0

Ethernet PORT PKT/S BYTE/S ERR/D  CRC ALN 2SHT 2LON COLL
         0    100   6000          4   4   0    0    8
```

Figure 4-5 Yesterday's 24-Hour Average Report

Accumulated Ethernet statistics should be monitored carefully for tracking of overall network traffic. Section 4.2.7 gives guidelines for interpreting network management reports.

4.2.5 Port Statistics Report

This report combines the output of the 24-Hour Average, Busiest Minutes, Busiest Samples, and Hour Average reports for a single specified port.

To display this report, use the following command:

```
SHow (<address>) STATistics
```

For example, the following command displays the statistics of port 3 of a remote server with the Ethernet address %080002000020:

```
sh (%080002000020!3) stat
```

This report is not available on Gateway Servers, NCS/150s, or NCS/1s.

Figure 4-6 contains an example of the Port Statistics report.

The first area of the report lists the Daily Average, Busiest Minutes, and Busiest Samples statistics for the specified port. The second area of the report lists the port's Hour Average statistics for every hour of the past 24 hours. Because of limited screen size, errors are summarized rather than itemized.

This report is useful for pinpointing an unusual event on a server or port.

```
PORT #3 STATISTICS REPORT: --------------------

DAILY AVERAGE:      CALL/D      PKT/S       BYTE/S       ERROR/D
                    10          10          120          0
BUSIEST MINUTE:     CALL/M      PKT/S       BYTE/S       ERROR/M
                    3           70          2000         0
BUSIEST SAMPLE:     MAX#SN      PKT/S       BYTE/S       ERROR
                    2           80          2400         0

HOUR CALL/H PKT/S BYTE/S ERR/H   HOUR CALL/H PKT/S BYTE/S ERR/H
0    0      0    0      0        1    0      0    0      0
2    0      0    0      0        3    0      0    0      0
4    0      0    0      0        5    0      0    0      0
6    0      0    0      0        7    0      0    0      0
8    3      10   800    0        9    1      30   700    0
10   0      20   100    0        11   0      20   108    0
12   1      10   200    0        13   2      30   120    0
14   1      30   500    0        15   1      2    100    0
16   0      2    70     0        17   1      2    80     0
18   0      0    0      0        19   0      0    0      0
20   0      0    0      0        21   0      0    0      0
22   0      0    0      0        23   0      0    0      0
```

Figure 4-6 Port Statistics Report

4.2.6 Security Statistics Report

This report summarizes security activity on the Communications Server since the last system boot. For each port on the system, the report lists the maximum privilege level reached, the number of times a SET PRIVilege command was executed successfully, the number of times a SET PRIVilege command failed because the user entered the wrong password, the number of times the port accessed a resource belonging to a different access group, and the number of times a request for access was denied because the user entered the wrong access password.

To display this report, use the following command:

```
SHow (<address>) SECuritySTATistics
```

For example, the following command displays the security statistics of a remote server with the Ethernet address %080002000018:

```
sh (%080002000018) secstat
```

Only a Global Network Manager can display this report. This report is not available on the following servers:

all TCP servers
GS/3
GS/4
IVECS
NCS/1
NCS/150

Figure 4-7 contains an example of the Security Statistics report. The *Connection Service User's Guide* (reference [10]) describes privilege levels and access control.

If the number of unsuccessful attempts in either category reaches one thousand, the system denies all subsequent requests from the port for a change of that type.

The most common error made when entering passwords is to use lower case where upper case is required or vice versa.

This report should be examined regularly on servers that are attached to modems and can be accessed from a remote network.

SECURITY STATISTICS

Port	MxPr	SetPr	Unsc	ChgGrp	Unsc	Port	MxPr	SetPr	Unsc	ChgGrp	Unsc
! 0	USER	0	0	0	0	! 1	USER	0	0	0	0
! 2	LNM	2	0	0	0	! 3	USER	0	0	0	0
! 4	USER	0	0	0	0	! 5	USER	0	0	0	0
! 6	USER	0	0	0	0	! 7	GNM	4	0	1	0

Figure 4-7 Security Statistics Report

4.2.7 Interpreting Network Management Statistics

Ethernet statistics should be monitored carefully for tracking of overall network traffic. The statistics for the busiest sample and busiest minutes may be set to zero using the ZeroStats command, providing a starting point for analysis of these reports.

Use the following guidelines to interpret network management report:

- Table 4-2 lists guidelines for interpreting CPU and BUFfer usage in the busiest sample, busiest minutes, hour average, and 24-hour average reports.

Table 4-2 Interpreting CPU and BUFfer Usage

Report	*CPU usage*	*BUFfer usage*
Busiest Sample	up to 80% is normal; can be 100% without adverse affects	up to 80% is normal; 100% indicates overload--call Bridge
Busiest Minutes	100% indicates overload--call Bridge*	up to 75% is normal; 100% indicates overload--call Bridge
Hour Average	up to 70% is normal; 90% indicates overload--call Bridge*	up to 75% is normal; 100% indicates overload--call Bridge
24-Hour Average	70% may indicate overload--call Bridge*	up to 45% is normal; 70% may indicate overload--call Bridge

* 100% CPU usage on a CS/1-HSM is normal.

- Error rates on fiber optic networks tend to be higher than those on coaxial cable networks. This is normal.
- For the 24-hour average, a problem may be indicated if the number of packets-too-short or packets-too-long persistently exceeds 1000 per day.
- For the hour average, accumulated PORT errors may indicate cable shielding problems or the wrong interface type.
- The number of CRC and alignment errors could each be as high as 10 without indicating a problem.
- If the number of accumulated disk errors (AcuDskEr) is persistently above 0, a problem with the diskette or drive is indicated. Clean the disk drive head and replace the system diskette. If the problem persists, the drive may have to be replaced.

- Persistent parity errors (ERR) may indicate a problem with the hardware at the terminal or server end of the connection. A port with improper parity parameter settings would generate an extremely high number of errors; this problem would probably be indicated by an unusable terminal before being noticed in a network management report.
- The network should not generate any packet-too-long errors. If the server consistently detects packet-too-long errors, the device that is generating the bad packets is deviating from network protocol standards.
- The number of CRC, alignment, and packet-too-short errors is a function of the number of stations and the traffic load on the network. The network runs smoothly as long as the total of these three error types remains below 10 errors per minute.
- The number of collisions is a function of the number of stations and the traffic load on the network. On a network with a single cable segment, the collision rate can reach 60 collisions per minute before network performance is noticeably affected. On a large network with multiple segments, performance may be affected if collision rates rise above 25 collisions per minute.

  A problem is indicated if the number of collisions suddenly increases markedly.
- Appearance of a negative number in any statistics reports indicates an extremely large number of errors (over 32,000) and warrants immediate investigation and corrective action.

The statistics shown in the busiest samples report are particularly useful when compared with the following statistics:

- The accumulated Ethernet statistics on other Communications Servers. This comparison is useful for problem isolation: a wide discrepancy among different servers on the same network may point to a network interface problem.
- Ethernet statistics in the other reports for the same server. If the accumulated Ethernet errors are high, the other reports can help pinpoint when the network disturbance occurred.

Excessive or unusual error rates are most often caused by one or more of the following problems:

- Loose terminator or loose barrel connector
- Improperly installed transceiver
- Electromagnetic interference, i.e., high-power source close to some part of the network
- Network improperly grounded
- Faulty transceiver or repeater
- Transceiver or repeater positioned closer than 2.5 meters to another transceiver or repeater on the network
- Use of transceivers or transceiver eliminators not tested and approved by Bridge (Table 2-2 lists transceivers tested by Bridge)

4.3 NCS Audit Trail

The audit trail is a record of session and error statistics. Any Communications Server, including one not booted from an NCS, can be configured to output its audit trail to an NCS using the AUditServerAddr parameter described in Appendix B. On the NCS/1, audit trail data can be plotted for easy interpretation.

The network manager should monitor and interpret the audit trail to discover error conditions. The network manager should investigate the cause of the following record types in the audit trail:

BC	Boot completed	PE	Password errors
BR	Boot requested	RW	Read/write error
EA	Ethernet alarm	SD	Server dropped
EE	Ethernet errors	SE	Excessive SIO errors
EO	Error overflow	SI	Server inactive
ER	Excessive retransmission		

If these errors are sent to an NCS/1, they appear automatically in the Diagnostics window.

Increased occurrence of Connection Failed (CF) record types with a Busy (BU) explanatory code and Connection Queued (CQ) record types indicates a need for additional servers.

For detailed information on the NCS/150 or NCS/1 audit trail, refer to the appropriate *NCS Installation and Operation Guide*.

4.4 Preventive Maintenance

One of the network manager's goals should be to detect potential network problems before they affect users. Following the recommendations in this section will help the network manager achieve that goal.

Bridge recommends the following procedures for preventive maintenance:

1. Display the network map daily, preferably at the beginning of each day, as a quick indicator of server problems.
2. Observe the environmental requirements listed in the appropriate *Planning and Installation Guide* for each server. Temperatures outside the recommended range can impair system reliability and cause diskette access errors.
3. Keep each server's top cover closed (except when actually adding or replacing boards) to ensure proper cooling of the server.
4. When adding or replacing boards, handle the boards carefully. Avoid touching the gold edge area, since body oils can affect the conductivity of the surface. Lint-free cleaning products, such as Texwipe Gold-wipes, are available for cleaning the gold area.
5. On all Series/1 products, clean the air intake filter periodically by scrubbing it with a stiff brush to remove accumulated dust and lint. The filter is located inside the enclosure, between the front panel and the cardcage.
6. Keep the area around the servers clean. Avoid accumulated dust, especially around the air intake slots.
7. In case of a system crash on servers with internal disk drives, an immediate memory dump may aid in diagnosing the problem. The network manager should keep two formatted diskettes available for this purpose. Memory dumps from diskless servers are not currently available. The procedures for obtaining memory dumps are described in Appendix C.
8. On the NCS/1, clean the tape drive head using a head cleaning tape cartridge.

For units with disk drives, the following measures are also recommended:

1. Before powering off or resetting the unit, be sure the disk activity LED on the unit front panel is not lit. Remove the diskette from the disk drive before powering the unit on or off.
2. Handle the diskette carefully. Always hold the diskette by its protective cover or by the label area; never touch the exposed areas of the diskette itself.
3. To avoid excessive diskette wear, change the system diskette every three months. Reference [10] describes the procedure for copying diskettes.

4. When the system diskette is changed, clean the disk head using a head cleaning diskette (e.g., Inmac 7157). A head cleaning diskette is available as an option from Bridge Communications, Inc., as part of the Installation Support Tool Kit (designated CS/1-INTK or CS/100-INTK). To clean the heads, follow these steps:

   a. Apply the solvent supplied with the kit to the head cleaning diskette through the slot where the heads will contact the cleaning diskette. Saturate the cleaning diskette with the solvent.

**** CAUTION ****

Do not use a fluorocarbon-based solvent; it will damage the heads. Use only alcohol-based solvents.

   b. Immediately insert the cleaning diskette in the drive and close the drive door.

   c. Press the Reset switch and wait for the Disk Activity LED to go out.

      Press the Reset switch three more times, each time waiting for the Disk Activity LED to go out.

In addition, follow the recommended preventive maintenance measures described in the *Planning and Installation Guides.*

4.5 Troubleshooting

This section describes how to troubleshoot common network problems. If a problem is observed, first read the troubleshooting flowchart in Section 4.5.2. If a problem cannot be solved by following the flowchart, find the title of a subsection following the chart that best describes the observed symptoms and follow the steps listed there. Contact Bridge or an authorized service representative for help with any problem that cannot be corrected by following the procedures described here.

If a user reports a problem, ask the user to explain the symptoms in as much detail as possible. Ask the following questions:

- What port is the user on? Refer to your network and personnel maps, described in Section 2.8.
- What keys did the user press, in what order?
- Can the user describe specific symptoms? For example, "When I turn my terminal on, the keyboard lights don't come on." or "When I turned my terminal on, the welcome message never appeared."
- What was the user doing when the problem occurred? For example, turning the terminal on, connecting to a host, trying to print, switching from word processing to accounting, and so on.
- What application, if any, was involved?

The answers to these questions should indicate whether the problem involves components of the LAN or whether it involves hardware or software outside the LAN. If the problem is network-related, determine what portion of the LAN is affected. For example, the problem might be limited to the following parts of the network:

- One port or a group of ports on a server
- A single server
- All servers of a given type (for example, all CS/1-HSMs)
- All servers attached to an individual transceiver eliminator
- All servers attached to a single network segment
- The entire network

All problems and the steps taken to correct them should be recorded in the problem log or on-line file, in as much detail as possible.

4.5.1 Troubleshooting Tools and Utilities

The troubleshooting tools available from Bridge include the software packet generator, hardware packet generator, installation tool kits, and most crash cart components.

Modem with Dedicated Telephone Line

Bridge recommends installing a modem with a dedicated telephone line and Communications Server port. This facilitates remote diagnostics of any network problems by Bridge Technical Support personnel.

Installation Tool Kits

The CS/1 and CS/100 Installation Tool Kits (designated CS/1-INTK and CS/100-INTK, respectively) include diagnostic tools useful to validate and troubleshoot Communications Servers. The kits include diskettes, testing software, loopback fixtures for testing SIO modules, and documentation that describes network validation, troubleshooting disk drives, and other procedures.

Crash Cart

A crash cart is essentially a LAN on wheels. The crash cart is used to replace a problem component temporarily to help pinpoint the cause of a given problem. For example, if a user's terminal is dead, the network manager might use the crash cart terminal and SIO cables in turn to determine whether the problem is in the user's terminal or SIO cable.

The components of the crash cart must be known to be in good condition and in working order. Each element should be tested and successfully operated on the network before being added to the cart. The cart should include the following items as a minimum:

- Complete and up-to-date set of Bridge manuals
- Terminal with cable
- One or more SIO cables of each type used in the installation
- Several transceiver cables
- Communications Server with an internal disk drive
- Good copies of current software
- Good transceiver or transceiver eliminator
- Some spare parts or spare boards
- Loopback cable
- Cable installation tool kit (designated CBL-CITK)
- Spare nuts, bolts, screws, and so on
- Time Domain Reflectometer (TDR)

Software Packet Generator

The Packet Generation software, described in Section 2.7, can be used to test the network-to-server and server-to-device connections. Documentation accompanies the software packet generator.

Hardware Packet Generator

The hardware packet generator (designated ACC-HWPKT), which is attached directly to a transceiver, loads the network with packets of varying lengths. The packets include various types of errors, depending on the EPROMs installed on the generator. The hardware packet generator may be used to simulate the activity of a full-sized network and to test transceivers and cabling independent of the servers. Documentation accompanies the hardware packet generator.

Miscellaneous Tools

The following tools are useful for troubleshooting:

- Soldering iron
- X-ACTO knife
- Digital multi-meter
- Serial line analyzer
- Cable rework kit, including crimper, stripper, pin extractor, and a supply of pins
- Breakout boxes (RS-232-C or appropriate version)
- Two universal flat cables with male and female connectors on both ends

4.5.2 Troubleshooting Flowcharts

The troubleshooting flowcharts in Figures 4-8 through 4-14 can be used to correct common problems. Use Figure 4-8 as a directory to the other flowcharts. The flowcharts assume that the server's initial startup and checkout, described in the server's *Planning and Installation Guide,* was successfully performed. The flowcharts also assume that the user will go on to the next step if a given procedure does not correct the problem.

If a problem cannot be solved by following a flowchart, find the title of one of the following subsections that best describes the observed symptoms and follow the steps listed there.

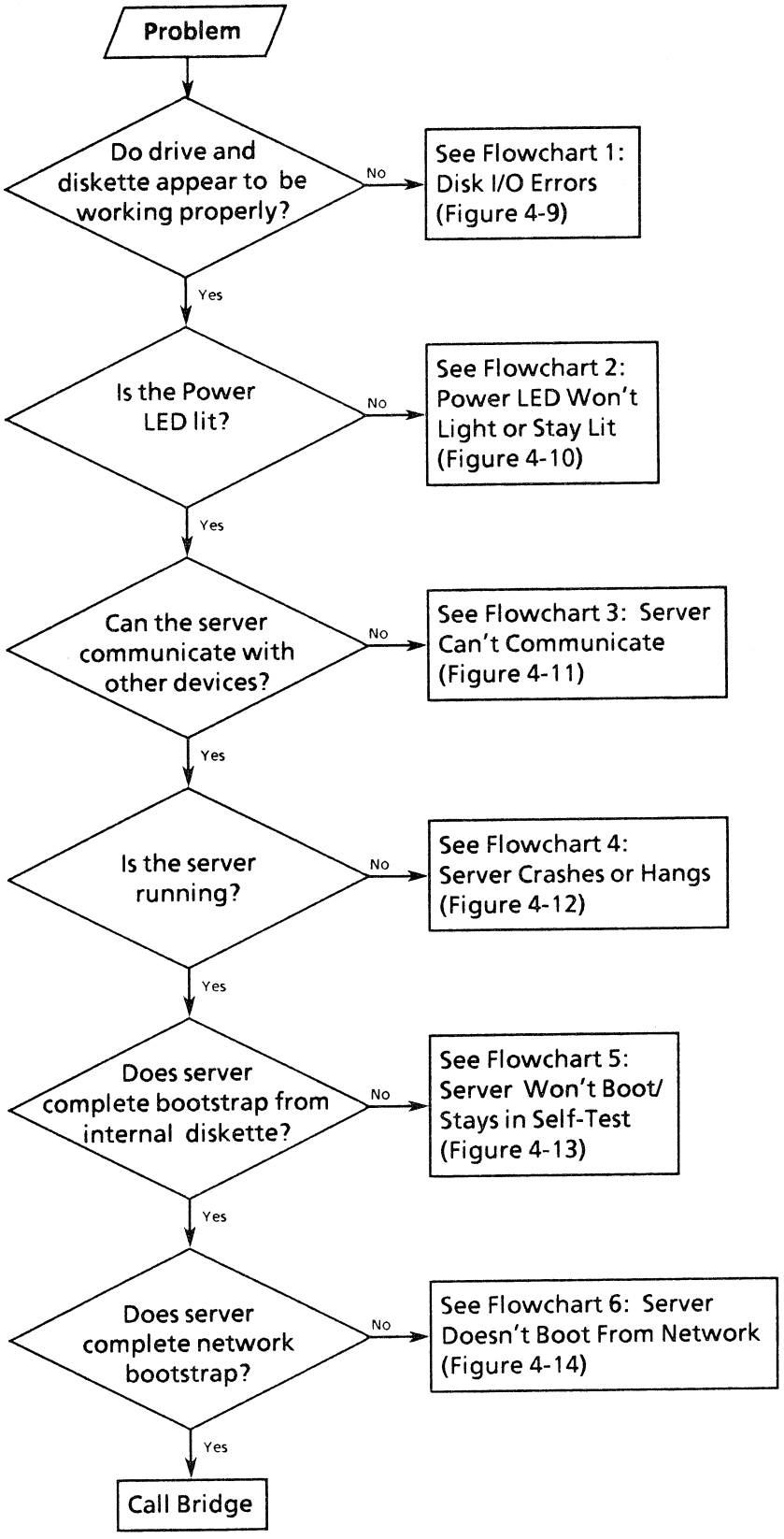


Figure 4-8 Flowchart Directory

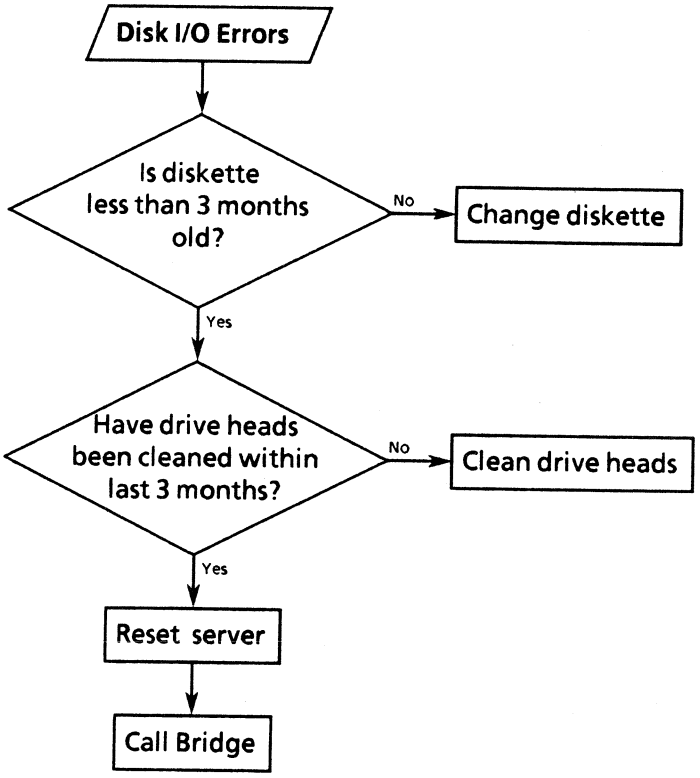


Figure 4-9
Flowchart 1: Disk I/O Errors

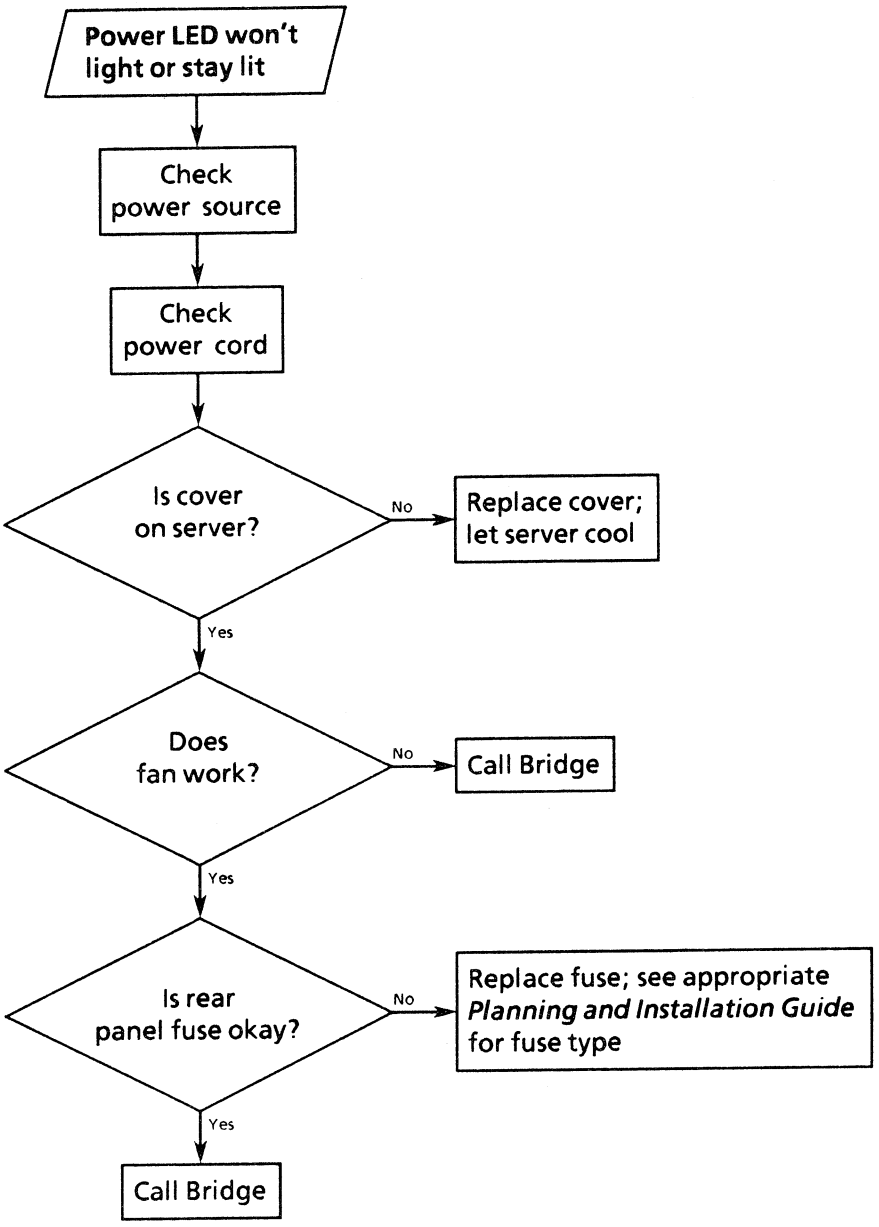


Figure 4-10
Flowchart 2: Power LED Won't Light or Stay Lit

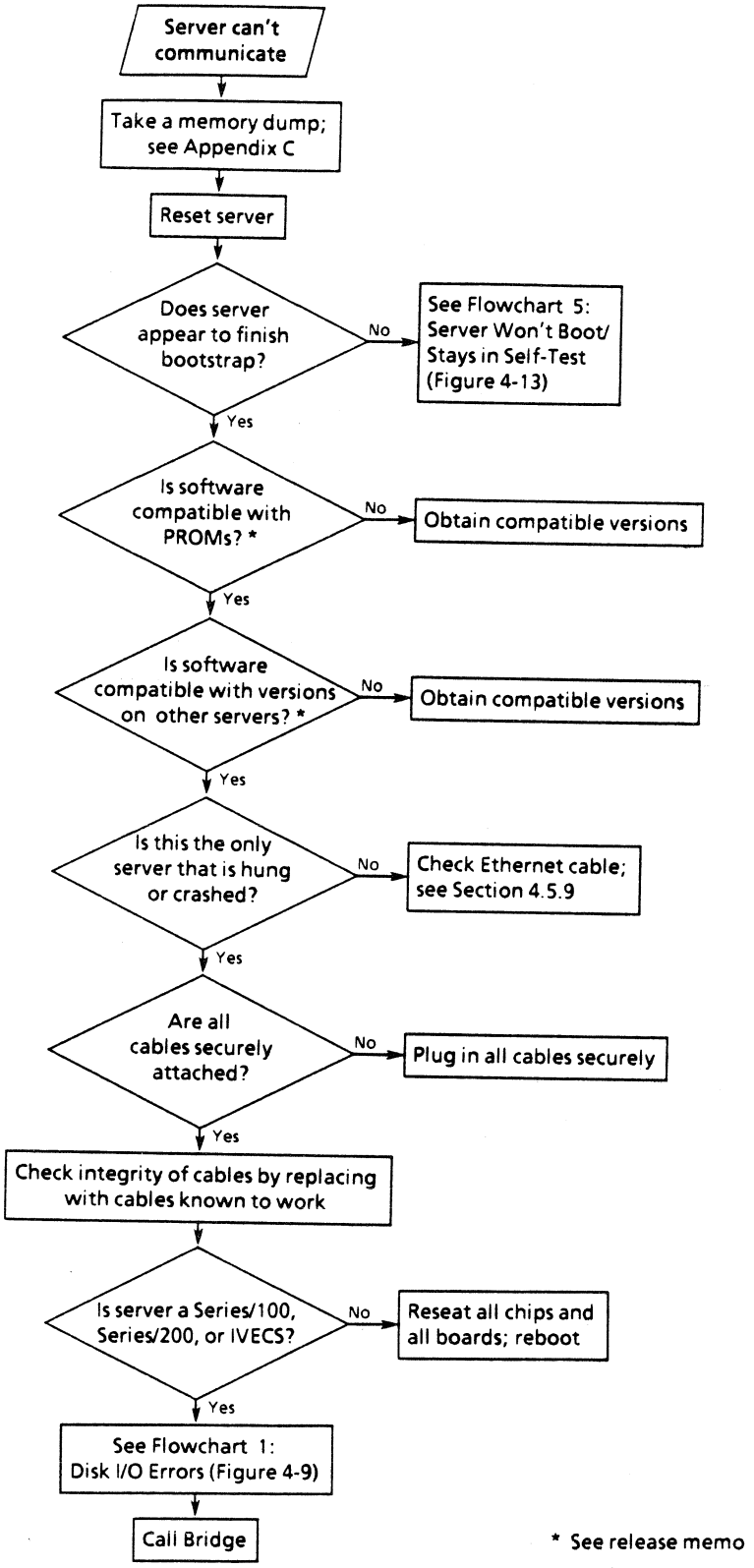


Figure 4-11
Flowchart 3: Server Can't Communicate

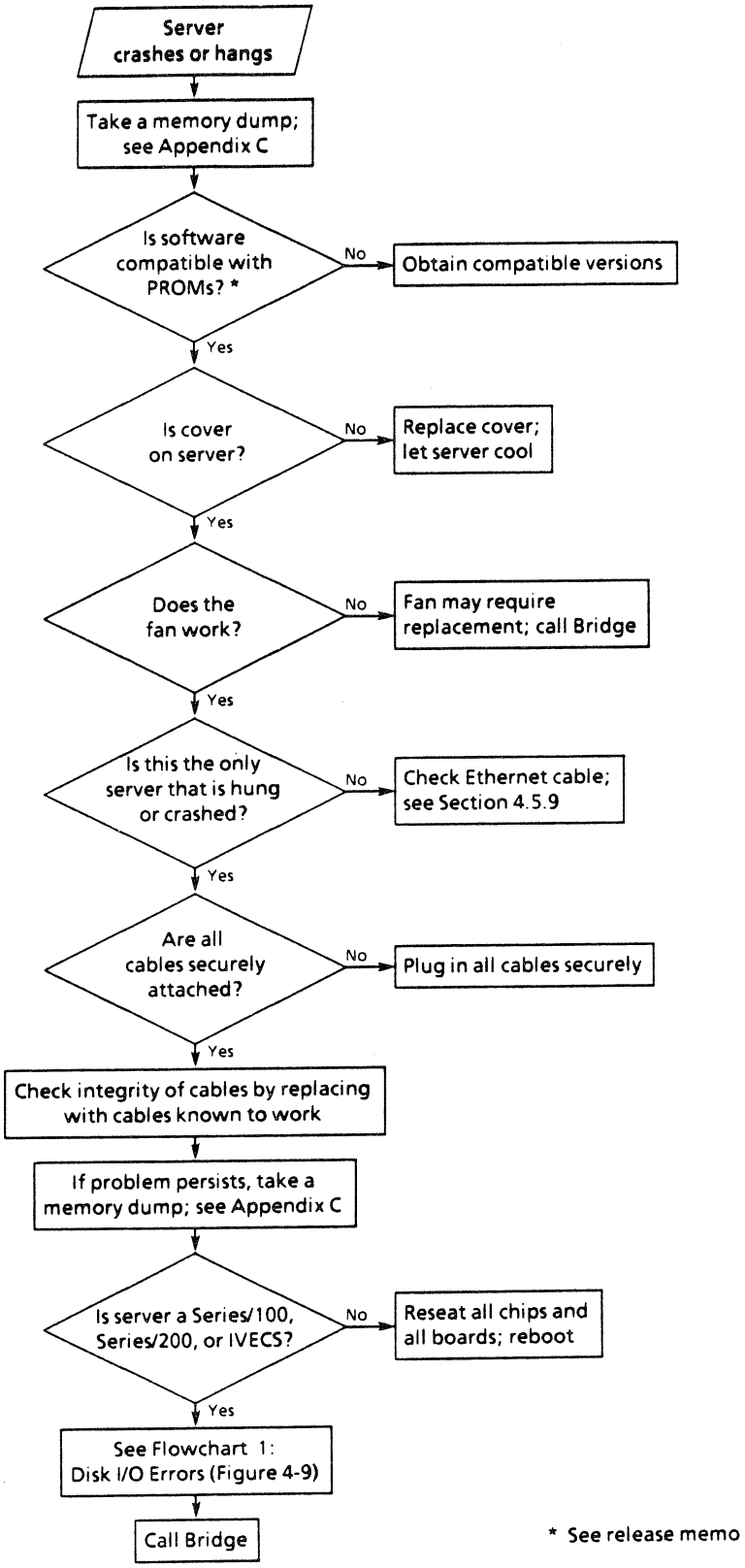


Figure 4-12
Flowchart 4: Server Crashes or Hangs

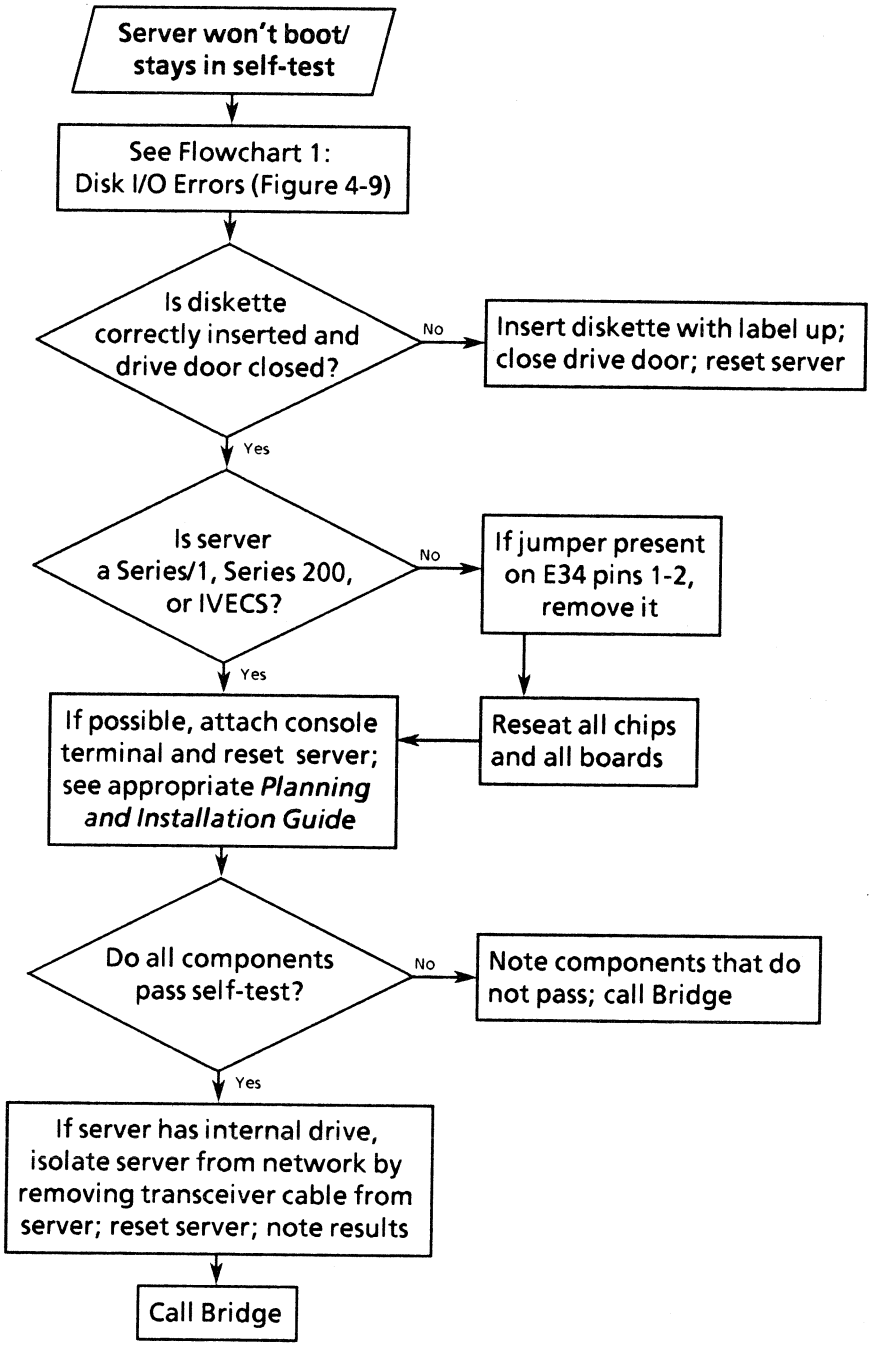
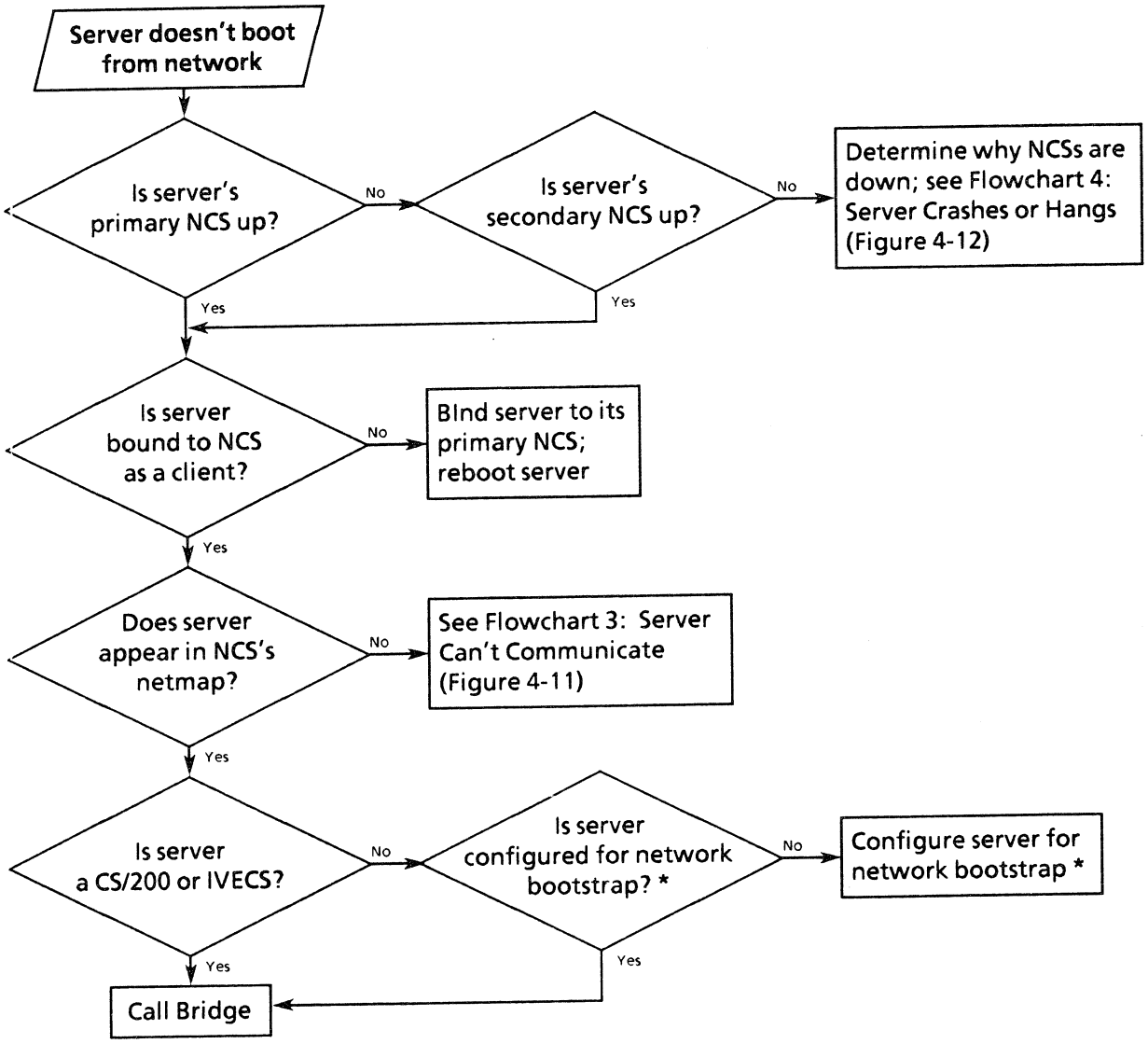


Figure 4-13
Flowchart 5: Server Won't Boot/Stays in Self-Test



* See appropriate *Planning and Installation Guide*

Figure 4-14
Flowchart 6: Server Doesn't Boot from Network

4.5.3 User Does Not Receive a Connection Service Prompt

If a single user does not receive a connection service prompt, follow these steps:

- The user may have inadvertently turned on flow control by pressing <CTRL-S>. Ask the user to enter <CTRL-Q>. If the terminal still does not respond, ask the user to turn the terminal off, wait at least ten seconds, and then turn it on again.
- The user may have inadvertently turned down the intensity. Ask the user to check the intensity knob.
- Check the status of the server to which the user's terminal is attached by issuing a SHow NetMAP command on another server. If the server's Ethernet address does not appear in the netmap, refer to Section 4.5.7.
- Making a connection to some devices, such as to a host connected to a CS/1-X.25, changes several session parameters. If the user may have made such a connection, the port should be placed in Listen mode and then in Command mode to reestablish the port's default parameters as its session parameters. The SHow command, described in reference [10], may be used to compare the port's default and session parameters.
- Access the server to which the user's terminal is attached in remote mode and execute a command that requires information from the remote server. For example, enter

```
SHow ADDRess
```

  a. If the command is successful, then the server is running. Place the user's port in Listening mode by using the Listen command, where the address is the user's port number:

```
Listen (<address>)
```

     Ask the user to press the return key. The server welcome message and prompt should appear.

  b. If the message "Timeout Failure" appears in response to the command, then the server to which the user's terminal is attached is down. (Or, if the server to which the user's terminal is attached is accessed across a Gateway Server, the Gateway Server might be down.) Reboot the server.

- Check that the SIO cable is attached to the correct port on the terminal.
- Switch the terminal's SIO cable with another SIO cable known to be in good working order.
- Check the setup parameters of the user's terminal. Users may inadvertently change a setup parameter, resulting in a flow control or communication problem between the terminal and the server.

4.5.4 User Cannot Access Device or Application

If a single user receives a Communications Server prompt, but cannot access a given device or application, check the following:

- The server attached to the specified device; follow the steps listed in Section 4.5.3
- That the specified application is up and running
- That the destination device is working
- Whether access groups are preventing the user from accessing the device or application; access groups are described in Section 3.2

4.5.5 Problems Reported by Several Users on the Same Server

If several users, all on the same server, report problems, follow these suggestions:

- Check the server to which the users' terminals are attached.
- If the users' physical ports are on the same board in the server, a hardware problem may exist. On Series/1 servers, all of the ports in the same vertical column on the back of the server are on the same board. On Series/100 and Series/200 servers, all of the ports on the same horizontal row on the back of the server are on the same board. On a Series/1 server, the affected SIO board may require replacement. For all other servers, call Bridge or an authorized service representative.
- Check the server's Packet Received LED. If it is lit constantly, check the server's transceiver and transceiver cable.
- If the users report an apparently sluggish response, the cause may be a noisy cable that is causing frequent transitions on the RS-232-C handshake lines (e.g., DCD, CTS), resulting in frequent interrupts on the SIO processor. To determine whether these lines are causing the problem, insert an RS-232-C jumper box between the server and the device cable, with only data lines connected and handshake lines jumpered high. If response picks up, then the lines should be permanently removed from the cable or, if they are required for the attached device, the cable shielding should be improved.
- Plugging an SIO cable attached to a Communications Server into the parallel printer port of an IBM or IBM-compatible personal computer may crash the server. If IBM-compatible personal computers are present, check the ports to which the SIO cables are attached.

4.5.6 Problems Reported by Several Users on Different Servers

If several users on different servers report problems, follow these suggestions:

- Question the users to identify a server or other resource being used by all of them. Perhaps each user was connected to the same host, and the host's Communications Server has developed a problem, or all the users were accessing resources across a Gateway Server that has gone down. Identify the server being used in common by the users reporting the problem, and address that server.
- Check each involved server individually by following the steps listed in Section 4.5.3.

- Check the servers' transceivers or transceiver eliminators.
- Check cable repeaters, if any.

4.5.7 Netmap Indicates Missing or Only One Server

If the SHow NetMAP command displays an incomplete list, indicates an inactive node, or lists only the server on which the command is entered, follow these steps:

- Issue the SHow NetMAP command on a terminal attached to a port on a second server. If the netmap shows the addresses of all the servers on the network except the first server, then the problem probably is the first server's connection to the Ethernet cable. Follow the steps outlined below, checking for the appearance of the first server in the netmap after each step:

  a. Check that the transceiver cable is securely attached to the transceiver and to the server.

  b. Loosen the transceiver from its tap and then retighten it until it is snug. Do not overtighten. This allows the transceiver probe to reseat, reestablishing its contact with the Ethernet cable. Section 2.2 describes installing taps and transceivers.

  c. Remove the transceiver and tap, and clean out the tap. Inspect the transceiver probe. Reinstall the tap and transceiver. Section 2.2 describes installing taps and transceivers.

  d. Remove the transceiver, plug the tap, and reinstall the transceiver with a new tap in a different location. Section 2.2.4 describes reinstalling transceivers.

- If the above suggestions are ineffective, then the first server probably has a hardware problem:

  For Series/1 servers (except the NCS/1): replace the Ethernet Transceiver Interface board and the Ethernet Shared Buffer board or, on later versions, the Ethernet Controller board. Test the server after replacing each board.

  For all other servers: Call Bridge Communications, Inc., or an authorized service representative for additional support.

4.5.8 Problems Making a Connection Between Two Server Types

If a connection between two different types of servers fails, follow these suggestions:

- Check for software version incompatibility. Section 5.4 describes compatibility.
- If an updated version of software was recently installed on a server, see if the problem is caused by the new software by rebooting the server with the old software. If PROMs have also been changed, check the compatibility of the old software with the new PROMs before attempting to run the old software. Section 5.4 describes compatibility.

**** NOTE ****

Bridge recommends running new software on only one server for the first 48 hours.

4.5.9 Network-wide Problems

If the entire network is not functioning correctly, follow these suggestions:

- If an NCS/1 is available, check the Diagnostics window and the audit trail for Ethernet Alarm records. Reference [7] describes the NCS/1.
- Check that the terminators have not been loosened or damaged.
- If an updated version of software was recently installed, see if the problem is caused by the new software by rebooting the server(s) with the old software. For servers that boot from an NCS, reinstall the previous version of software on the NCS and then reboot its client servers. If PROMs have also been changed, check the compatibility of the old software with the new PROMs before attempting to run the old software. Section 5.4 describes compatibility.
- If a new hardware component was recently installed, see if the problem is related to that component by powering it off or removing it from the network.
- Check the cable using Time Domain Reflectometry. The cable may be shorted, or may have been damaged in some way. If the cable has been damaged in one place so that it cannot operate, the entire cable, including portions attached by in-line connectors, cannot operate because the damaged portion affects wave transmission on the entire length of cable, as shown in Figure 4-15.

  If in-line connectors have been used in the cable, the affected portion of the cable can be isolated by removing the connectors, attaching a terminator onto each end of the cable, and testing each portion of the network. After the problem is corrected, the connectors may be reinstalled.

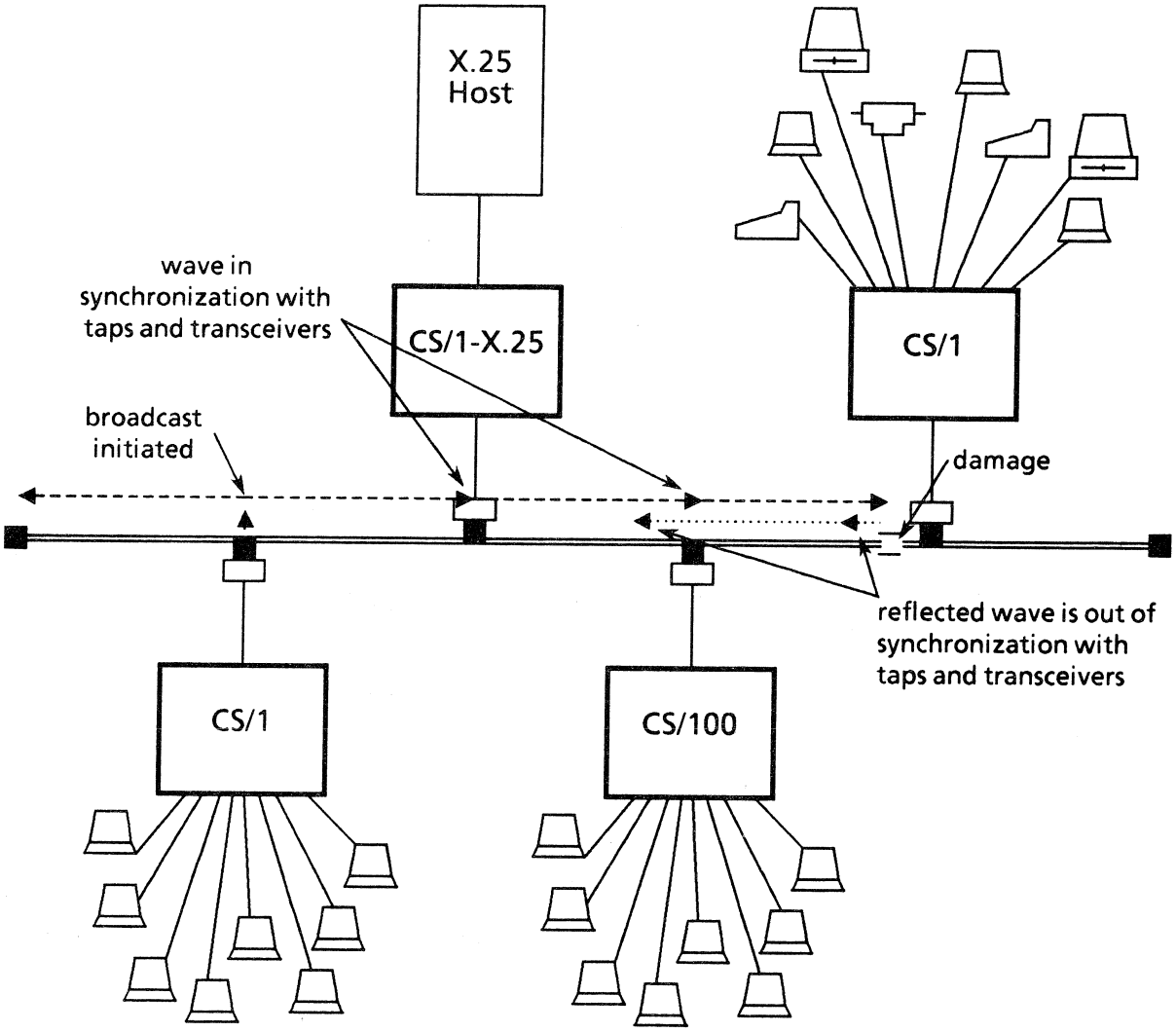


Figure 4-15 Wave Transmission on Coaxial Cable

4.5.10 Problems that Repeatedly Occur at the Same Time of Day

Problems that occur at the same time of day are usually caused by environmental or power conditions. Consider activities that might affect power supply or environment, such as:

- Air-conditioning startup
- Carpeting static
- Electric or solar lighting changes
- Heat from sunshine through a window
- Startup of manufacturing equipment
- Vacuum cleaner
- Extremely heavy network activity

4.5.11 Printer Problems

If a printer attached to a Communications Server port is not operating properly, follow the troubleshooting procedures recommended by the printer manufacturer. In addition, check the following:

- Make sure that the cable connections at both ends are secure.
- Make sure that the cable used to attach the printer conforms to the manufacturer's specifications, and that no additional wires are present.
- If the printer output is garbled, check the printer switch settings for correct baud rate, parity, and flow control.
- Check the configuration of the printer port, particularly the DeVice and Baud parameters.

4.5.12 Troubleshooting Macros

Use the following guidelines to correct the problem when a macro does not execute as expected.

- 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.
- Do not use the RESume command in a macro except as the last line of the macro.
- Do not use the Connect command in a macro unless it is the last line of the macro or it includes the ECM argument.
- Because macros are limited in length to 256 bytes, it is best to use the minimum unambiguous abbreviation of commands and parameters in macros that may approach this limit.
- Do not use the REMOTE command in a macro since there is no way to escape remote mode from within the macro.
- A macro may include a DO command to call another macro, but it should not call itself or another macro that calls it, because this will result in an endless loop.
- When debugging a macro on the NCS/1, editing the macro to set interaction to macroecho may be useful.
- After a Connect command, it is usually necessary to Pause for several seconds before Transmitting to allow time for the system to respond to the connection request. For example:

```
connect host ecm
pause 2
transmit "HELLO^M"
```

4.5.13 Disk Drive Problems

If repeated problems occur on a given disk drive, follow these steps:

- Verify that the drive heads have been cleaned, as described in Section 4.4.
- Verify that the system diskette is replaced every three months, as described in Section 4.4.
- Test the drive by following these steps:

  a. Make five copies of the system diskette using the COpy command.

  b. If more than one copy does not verify correctly on the first pass, repeat the preceding step using a different system diskette.

  c. If more than one copy from the different system diskette does not verify correctly on the first pass, contact Bridge Communications, Inc.

4.6 Network Operation Control Documents

Figure 4-16 shows a network problem report. This report is particularly useful for less experienced network management personnel, who can use it to define a problem clearly before attempting to correct it. The report includes space for recording serial numbers of replacement equipment.

NETWORK PROBLEM REPORT

Form #_____

Request Date: _____ Time: _____
Completion Date: _____ Time: _____

Reported by: _____ Report taken by: _____

User: _____ Address: _____

Host/device: _____
CH/Internet Name: _____ Address: _____

Problem Description: _____

Equipment Replaced? Yes No
Serial number of replacement: _____
Status of original: _____

Progress: _____

Comments: _____

Hours to correct: _____
Cost to correct: _____
Downtime: _____

Figure 4-16 Network Problem Report

5.0 NETWORK PLANNING

This section describes guidelines and procedures for adding servers, for segmenting the network with a GS/4, for providing redundancy, and for ensuring network system compatibility.

5.1 Adding Servers

Bridge servers can easily support a device attached to each of the server's ports because the servers operate efficiently at maximum capacity. For this reason, new servers usually need to be added to the network only when additional ports are required.

An exception to this may occur if devices that use more than one bandwidth are included in the network. In this case, servers should be added if the following indicators are noticed:

- In the network management reports, consistent 100% buffer utilization and 100% CPU utilization
- In the NCS audit trail, frequent occurrence of Connection Failed (CF) record types with a Busy (BU) explanatory code and Connection Queued (CQ) record types
- Persistent slowdown in response time over the network

Some installations where users frequently use multiple sessions may require extra servers. Additional servers can also be used to expand clearinghouse name and macro storage capacity. For example, if the maximum number of clearinghouse names have been defined on one NCS, another NCS can be added to store additional names.

5.2 Segmenting Networks with GS/4s

A GS/4 is used to connect two segments of a network. The GS/4 is described in detail in the *Series/1 Planning and Installation Guide* (reference [3]).

Splitting a network with a GS/4 offers several advantages. If the Ethernet cable is damaged or develops some other problem, its failure affects the entire network. Splitting the cable into two cables connected by a GS/4 eliminates this central point of potential failure.

Splitting the network decreases cable utilization on each segment. If cable utilization, as plotted on the NCS/1, approaches 80%, the network manager should consider splitting the network with a GS/4.

In addition, the GS/4 performs other functions:

- Decouples the cable system, both from the electrical and traffic point of view
- Completely regenerates packets
- Decreases the number of collisions and alignment and CRC errors
- Filters traffic: each segment of the network sees only the traffic bound for the servers on that segment
- Decreases amount of traffic on each segment: Routine broadcasts, such as those used by all servers to create and maintain the network map, contribute to the amount of traffic on any segment. Some low performance nodes, such as an IBM PC running EtherTerm, may be adversely affected by these routine broadcasts. Decreasing the number of servers on a segment reduces the traffic resulting from routine broadcasts.

To determine where to split the network, isolate the current traffic groups in the network. When the network is split, traffic within each segment should be maximized with 80 percent or more of the traffic occurring within that group, and traffic from segment to segment should be minimized. The members of the traffic groups should be in close proximity to one another, or at least contiguous.

For example, in Figure 5-1, the administration area includes Host A, the host accessed most of the time by most of the users in that area. The users on the rest of the network are not in close proximity to each other, and they access both Host B and Host C. The administration area clearly constitutes a traffic group that could be split into its own Ethernet, with access to the rest of the network provided by a GS/4.

The GS/4 can also be used in mixed media applications and to connect several buildings, with a backbone cable attached to several segments via GS/4s. The backbone is often a fiber optic cable. Figure 5-2 shows an example of this use of a GS/4.

Terminal and host servers should not be separated by GS/4s. This would defeat the purpose of segmentation with GS/4s, because all of the traffic between the terminals and hosts would have to go through the GS/4. If the traffic on the network is balanced, with the majority of users routinely accessing all hosts on the network, a GS/4 is not necessary except to extend the network or for a mixed media application.

Ethernet cable runs efficiently up to 80 percent of capacity. Ethernet cable utilization is included in the NCS/1 statistics reports and can be plotted graphically.

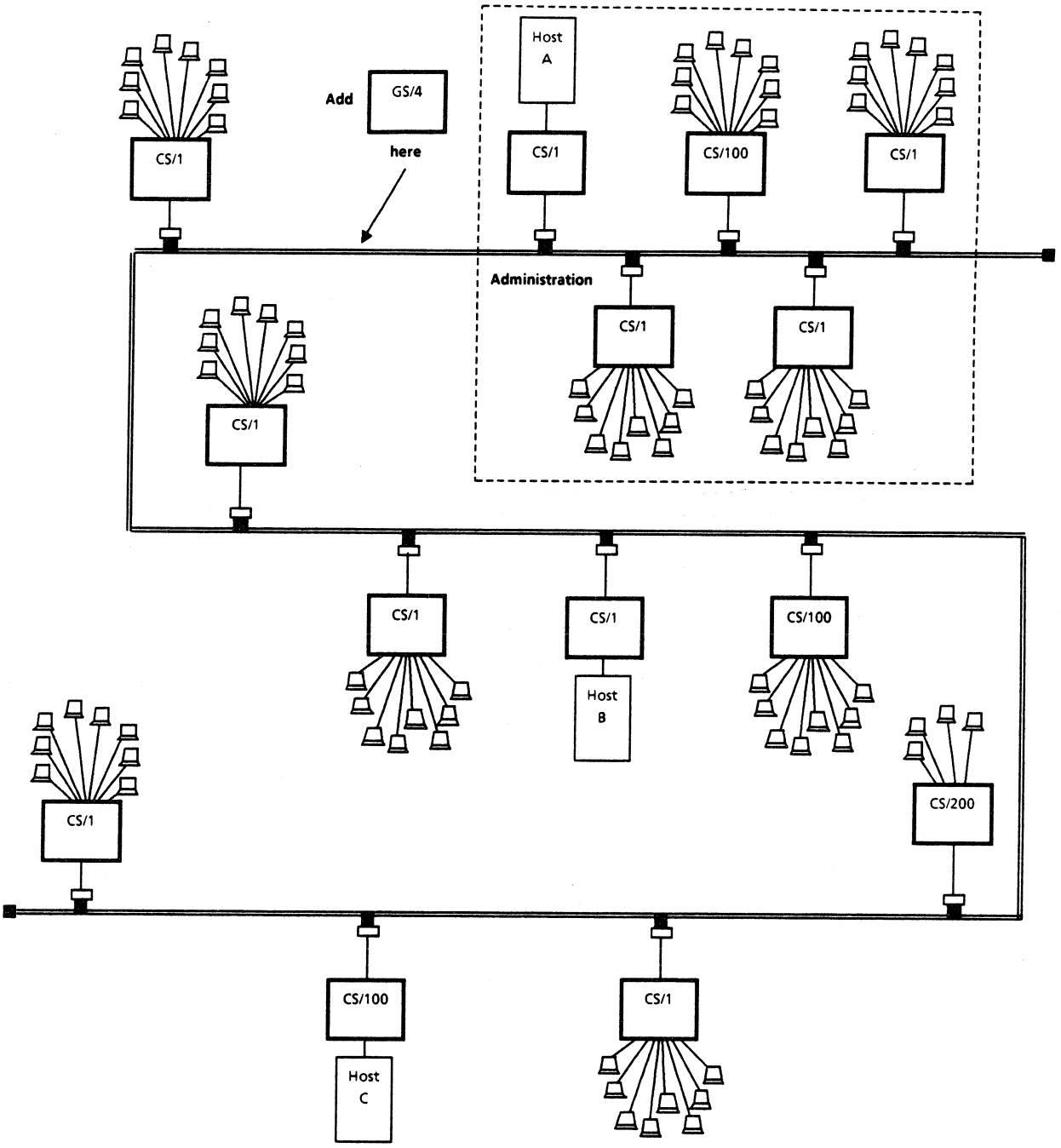


Figure 5-1 Splitting a Network with a GS/4

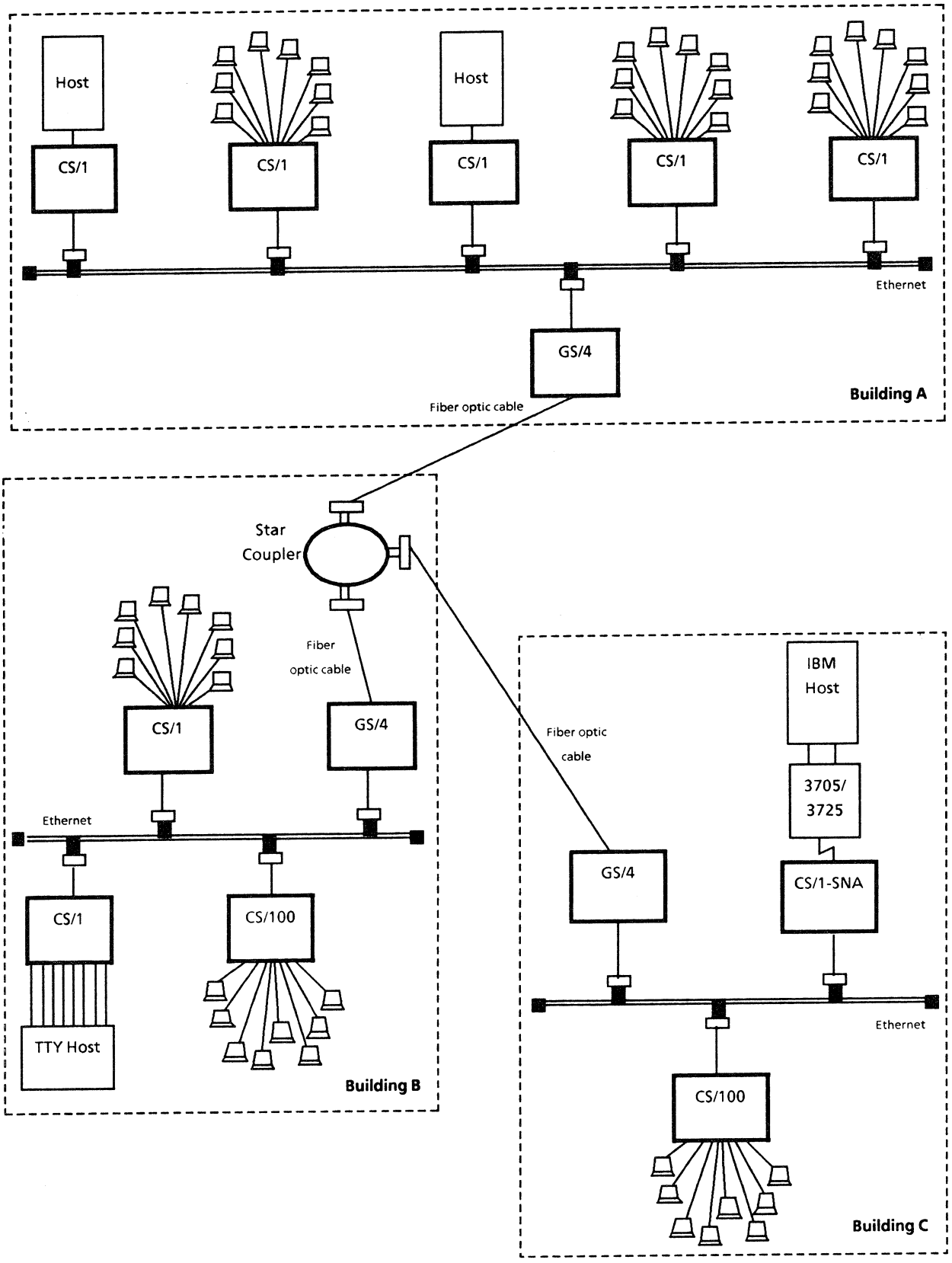


Figure 5-2 GS/4s Linking Segments to a Backbone Cable

5.3 Redundancy

Bridge Communications, Inc., recommends attaching more than one Communications Server to key system resources. All Communications Servers attached to a given resource should remain operational at all times. If one of the Communications Servers is taken out of service, users can access a given resource through the other Communications Server without interruption.

Keeping spare servers or parts on-site provides additional assurance that any interruption in service can be minimized. Bridge recommends 1 percent sparing, i.e., for every 100 units, spare parts for one unit should be maintained. On small networks, spares may be impractical; however, spares should be maintained for any server that is vital to network operation.

To prevent system downtime due to failure of a single NCS, Bridge Communications, Inc., recommends that each installation that uses NCSs include at least two of them. The primary NCS supports the Communications Servers, and the secondary NCS acts as a backup.

This arrangement simplifies network maintenance, because all configuration information is stored on the primary NCS, with backups on the secondary NCS, instead of being stored on multiple Communications Servers all over the network. The network manager simply backs up the primary NCS to the secondary NCS whenever the network configuration changes.

5.4 Compatibility

The network manager must ensure that compatibility among Bridge software, firmware, and hardware is maintained:

- Read every release memo. The release memos describe in detail the current version's compatibility (or incompatibility) with other versions. This information is not readily available from any other source.
- Before installing a new release, determine the versions of existing components or software and verify their compatibility with the new release.

APPENDIX A

SYSTEM GENERATION

This appendix describes the CS/1, CS/100, and Gateway Server system generation.

The procedures are executed from the monitor, via the system console terminal or NCS/1 console. For information on the console terminal and on accessing the monitor, refer to the appropriate *Planning and Installation Guide*. For information on executing system generation on the NCS/1, refer to the *NCS/1 Installation and Operation Guide* (reference [7]).

The system generation procedure is used to adjust system generation parameters to meet the needs of a specific installation. System generation parameters typically need to be set only once for each server. The results of the system generation are recorded on the system disk, which should be backed up afterward.

System generation may be required or optional depending on the type of server, the type of software, and whether the server boots from an NCS. Restrictions and requirements are summarized in Table A-1 and described below.

Table A-1 System Generation Requirements

Server	*System Generation*
CS/1-A	Not required *
CS/1-BSC running standard software	Not required *
CS/1-SDLC	Not required *
CS/1 that boots from an NCS/1	Not required *
CS/1 that boots from an NCS/150	Not required *
CS/1-TCP that boots from an NCS/150-TCP	Not required *
CS/1-BSC running SPMUX software	Required
CS/1-HSM	Required
CS/1-SNA	Required
CS/1-TCP	Required
CS/1-X.25	Required
CS/100-A/BSC	Not required *
CS/100 that boots from an NCS/1	Not required *
CS/100 that boots from an NCS/150	Not required *
CS/100-TCP that boots from an NCS/150-TCP	Not required *
CS/100-488	Not available
CS/100-TCP	Required
CS/200	Not available
Gateway Servers (all types)	Required
IVECS	Not available
NCS/1	Not required
NCS/150	Not required
NCS/150 running TCP protocols	Required

* System generation may be required for custom software or a nonstandard installation.

For Communications Servers, system generation may not be necessary; the following list outlines restrictions and requirements:

- **The CS/1-A, the standard CS/1-BSC, and the CS/1-SDLC** are shipped with a set of default parameters designed for standard software on a 32-port system. System generation is required only on a system with custom software or special installation-dependent requirements; refer to Section A.2.

- **A CS/1 or CS/100 that boots from an NCS/1** does not require system generation in standard installations. If system generation is required for custom software or a non-standard installation, the procedure must be performed on the NCS/1 (reference [7] describes copying to the NCS/1). The sysgenned software is used by all CS/1s or CS/100s bound to that software file.
- **A CS/1 or CS/100 that boots from an NCS/150** does not require system generation in standard installations. If system generation is required for custom software or a nonstandard installation, the procedure must be performed on a CS/1 or CS/100 with an internal disk drive, and the changes must be copied onto the NCS/150 diskette (reference [8] describes copying to the NCS/150 diskette). The sysgenned software is used by all CS/1s or CS/100s supported by the NCS/150, not just by the CS/1 or CS/100 on which Sysgen was run.
- **A CS/1-TCP or CS/100-TCP that boots from an NCS/150-TCP** does not require system generation in standard installations; the server's internet address is specified when the server is bound to its NCS. If system generation is required for custom software or a nonstandard installation, the procedure must be performed on a CS/1-TCP or CS/100-TCP with an internal disk drive, and the changes must be copied onto the NCS/150-TCP diskette (reference [8] describes copying to the NCS diskette). The sysgenned software is used by all CS/1-TCPs or CS/100-TCPs supported by the NCS, not just by the CS/1-TCP or CS/100-TCP on which Sysgen was run.
- **The CS/1-BSC running SPMUX software** is shipped with default parameters for 32 UTS terminals mapped into 3 DCP ports. System generation is always required; refer to Section A.3.
- **The CS/1-HSM** is shipped with default parameters for one multiplexed line to a DEC host. System generation is always required; refer to Section A.4.
- **The CS/1-SNA** is shipped with default parameters for one line to an SNA communications processor. System generation is always required; refer to Section A.5.
- **The CS/1-TCP and CS/100-TCP** are shipped with a set of default parameters designed for standard software on a 32-port CS/1-TCP or 14-port CS/100-TCP. For servers that boot from an internal diskette, system generation is required to specify the server's internet address. Refer to Section A.6.
- **The CS/1-X.25** is shipped with default parameters for one X.25 line. System generation is always required; refer to Section A.7.
- **The CS/100-A/BSC** is shipped with a set of default parameters designed for the standard software on a 14-port system. System generation is required only on a system with custom software or special installation-dependent requirements; refer to Section A.2.
- **The CS/100-488** never requires system generation.
- **The CS/200** is shipped with a set of default parameters designed for the standard software on a 10-port system. System generation is not currently available.
- **The IVECS** is shipped with default parameters for one multiplexed line to a DEC host. System generation is not currently available.

All Gateway Servers require system generation as follows:

- **For the GS/1,** to specify the network address of the Ethernet to which the GS/1 is connected, the addresses and characteristics of the lines connecting the GS/1 to the X.25 networks, and the network addresses and access line addresses of the remote networks. Refer to Section A.8.
- **For the GS/3 Interconnection Service,** to specify the network address of the Ethernet to which the GS/3 is connected, the addresses and characteristics of the lines attached to the GS/3, and the network addresses and access line numbers of all remote Ethernet networks. Refer to Section A.9.
- **For the GS/4 Interconnection Service,** to specify the local and remote network addresses. Refer to Section A.10.
- **For the GS/6 Interconnection Service,** to specify the local network address and the remote network and link addresses. Refer to Section A.11.

**** NOTE ****

Once a diskette has been configured for a particular Gateway Server, the diskette must not be used in any other server, since the address information on the diskette applies only to a single Gateway Server.

For an NCS/150 that supports Communications Servers running TCP protocols, system generation is always required; refer to the *NCS/150 Installation and Operation Guide* (reference [8]). The NCS/1 and an NCS/150 that supports Communications Servers running XNS protocols never require system generation.

A.1 Running the Sysgen Program

The Sysgen program is a simple, menu-based utility for displaying and altering the system generation parameters and saving the changes.

The Sysgen program may be performed only on a server with an internal disk drive or on an NCS/1. On a Communications or Gateway Server, Sysgen may be executed only immediately after a power-on or reset; the program does not execute properly if communications software has been running prior to the execution of Sysgen. The system diskette must be in place in the disk drive when Sysgen is executed.

For all Series/1 products (e.g., CS/1, GS/4) except the NCS/1, the procedures are executed from the MCPU monitor, via the system console terminal. Boot the system software diskette and then enter the Sysgen command. To run Sysgen on an NCS/1, the NCS/1 Sysgen utility is used; follow the instructions in reference [7].

For Series/100 products (e.g., CS/100, NCS/150), the procedures are performed through the utilities diskette, via the system console terminal. First boot the utilities diskette. After the system is booted and an angle-bracket prompt (>) appears on the terminal attached to port 0, remove the utilities diskette from the disk drive and replace it with the system diskette. Then enter the Sysgen command.

**** NOTE ****

> On a CS/100-BSC, if a character-synchronous terminal is attached to port 0, that terminal must be disconnected and an asynchronous terminal must be connected in its place.

After booting the appropriate software, enter the Sysgen command:

```
gn
```

The main Sysgen menu is displayed:

```
1.  View/Alter Module Parameters

2.  Save Parameters

3.  Exit to Monitor

Enter selection:
```

Enter the number of the desired option, then press the return key.

The system generation parameters are divided into seven or eight groups, depending on the server type. When the View/Alter option is chosen from the main Sysgen menu, the program displays a list of all parameter groups. The following example shows the typical View/Alter menu for the CS/1-A and CS/100-A; the View/Alter menu for other server models may differ.

```
1. Kernel Parameters
2. IDP Parameters
3. SPP Parameters
4. User Interface Parameters
5. Virtual Terminal Parameters
6. Statistics Monitor Parameters
7. Clearinghouse Parameters
```

Most system generation parameters are set to default values appropriate for standard installations, and need not be altered by the customer. However, all possible parameters appear in the Sysgen menus in order to allow alterations necessary in custom installations and during software development. Detailed descriptions of all parameters not described in this guide are available in the *Software Technical Reference Manual* (reference [2]).

**** NOTE ****

Sysgen parameters should be altered only by someone with a thorough understanding of the system software.

To select a parameter type, enter the number of the group, then press the return key. Depending on the group chosen, the program displays a menu of parameters, a menu of additional menus, or a hybrid menu of both parameters and additional menus.

To change a parameter, locate the menu that lists that parameter and its value, and then enter the number of the parameter. The resulting prompt may include a list of limits that apply to the parameter value. To enter a new value, respond to the prompt by typing the new value (in hexadecimal, if the value is numeric), then press the return key. To leave the value unchanged, simply press the return key.

Throughout the Sysgen program, pressing the escape key returns the program to the menu at the next higher level.

**** NOTE ****

For terminals that do not have an escape key, the character <CTRL-[> may be used to send an escape character to the program.

For descriptions of individual parameters that must be set on various models of server, refer to Sections A.2 through A.11.

After system generation is complete, and before the modified system generation parameters can take effect, the values must be saved on the system diskette or, on the NCS/1, in the appropriate system file and the system must be booted from the updated software. To save the new values, first press the escape key as many times as necessary to return to the main Sysgen menu. Then select option 2 (Save Parameters) from the main menu.

Sysgen requests confirmation before writing over the old system configuration parameters. First verify that the diskette is in place in the disk drive. Then respond to the confirmation prompt with a lower case "y" to save the new values or a lower case "n" to return to the menu without writing to the disk.

A written record of parameters that are changed should be maintained. The Site Management Forms, described in Section 3.5, may be used for these notes.

A.2 Setting CS/1-A/BSC/SDLC and CS/100-A/BSC Parameter Values

In most installations, unless the CS/1-A/BSC/SDLC or CS/100-A/BSC is running custom software or unless special installation-dependent requirements exist, no system generation parameters should be changed except those in options 4 and 7 (User Interface Parameters and Clearinghouse Parameters, respectively).

To review the default values of these parameters, first select option 1 (View/Alter Parameters) from the Sysgen main menu, and then select either option 4 or option 7 from the Module Select Menu.

The User Interface Parameters may be used to alter the default privilege levels required to execute Connection Service commands.

**** NOTE ****

Do not establish any privilege level other than User for the SET command. Otherwise, no one will be able to access higher privilege levels, which can be done only through the SET command.

Giving a User privilege level to commands that can change stored names, macros, rotaries, or default configurations (e.g., Name, UNDefine, ROtary, SETDefault) is not recommended.

The single parameter in the Clearinghouse menu may be used to specify whether the Communications Server distinguishes between lower and upper case in clearinghouse names.

A.3 Setting CS/1-BSC SPMUX Parameter Values

In an SPMUX environment, two types of CS/1 are present. The standard CS/1-BSC interfaces the DCP host front-end processor to the Ethernet; the CS/1-BSC running SPMUX software interfaces UTS terminals to the Ethernet. System generation must be performed on both types of CS/1, on the DCP, and on each UTS terminal in the network.

The network manager must ensure that both the CS/1-BSC running SPMUX software and the DCP are configured with the same mapping of terminal addresses to DCP ports; in addition, the network manager must ensure that the UTS terminals are individually configured with the same addresses. For detailed information, refer to the release memo accompanying the SPMUX software diskette.

For the CS/1-BSC on the DCP side, only one system generation parameter might need to be altered.

This alteration improves performance, but is not mandatory. The decision should be made based on whether the system is to be booted from an NCS. If the parameter is changed, the system probably will not be able to boot from the NCS, but will have to boot from an onboard disk drive.

To make this alteration, select option 5 from the View/Alter menu, then select option 3 from the Virtual Terminal parameters menu; change the depth of the VT-to-agent mailbox from 1 to 2. Increasing the value of this parameter may affect MCPU buffer allocation; contact Bridge Communications, Inc., or an authorized service representative for detailed information.

For the CS/1-BSC running SPMUX software, option 8 of the View/Alter menu is used to define the address mapping between the UTS terminals and the DCP host ports.

When option 8 is selected, the system displays a list of two submenus:

- The View/Modify Terminal Addresses menu (option 1) maps CS/1 ports to UTS terminal RID/SID addresses and maps the RID/SID addresses to groups representing DCP ports. By default, 32 terminals are mapped into three DCP ports (12 each to groups 1 and 2, and 8 to group 3).

  To alter the RID/SID address or group assignment for a CS/1 port, enter the port number of the affected port. The system will prompt for the RID, the SID, and the group. All values must be specified in hexadecimal; each RID/SID address in a group must be unique.

  Each UTS terminal consists of two logical screen devices. The SID specified by the user is assigned to the terminal's first screen, and the CS/1 automatically assigns the next higher SID number to the terminal's second screen. Therefore, the SID portion of any terminal address must be greater than the SID of the previous terminal in the list by at least two, or two logical devices will have duplicate addresses. If the addresses are not unique, the system will not function.

- The View/Modify Host Port Addresses menu (option 2) maps terminal group numbers to the Ethernet addresses of the corresponding DCP ports. The default mapping sets all DCP port numbers to zero and contains no valid Ethernet addresses; the addresses and the DCP port numbers must be specified for each CS/1-BSC running SPMUX software.

  To map terminal groups to DCP ports, enter the group number associated with the terminals to be multiplexed on a DCP line. The CS/1 then prompts for the Ethernet address and the port number of the associated DCP port.

  No two terminal groups may be assigned to the same Ethernet address and port number.

A.4 Setting CS/1-HSM Parameter Values

The system generation procedure for the CS/1-HSM includes both mandatory and optional parameters. To review the default values of these parameters, first select option 1 (View/Alter Parameters) from the main Sysgen menu, and then select option 5 (Virtual Terminal Parameters) from the Module Select Menu.

On the CS/1-HSM, the list of Virtual Terminal parameters includes several parameters specifically applicable to the HSM configuration. The parameters are listed twice, once for each possible HSM board in the unit.

- The Base Port ID parameters specify (in hexadecimal) the lowest number in the range of virtual port numbers accessed through each board. If two HSM boards are present, a base port ID must be specified for each board; if only one HSM board is present, the base port ID must be specified for that board, and the second base port ID must be set to zero. Virtual port numbers must be in the range 32 to 95 (decimal).

- The Number of Ports parameters specify (in hexadecimal) how many virtual ports are assigned to each board. By default, 64 virtual ports are assigned to a single HSM board. If two HSM boards are present, this parameter is mandatory. In this case, the number of ports specified on each board must correspond to the unit count specified when the HAC boards were installed. For example, if a unit count of 6 was specified on the first HAC and a unit count of 2 was specified on the second HAC, then 48 ports must be specified for the first HSM board and 16 ports must be specified for the second HSM.

  Reference [3] describes HAC board installation.

- The Break Char parameters determine how breaks are sent to the host. If this parameter is set to 0, the CS/1-HSM sends the host a null character with a framing error when a break signal is received from the terminal. If this parameter is set to a value in the range 0x1 through 0xFF, the CS/1-HSM sends the host the specified ASCII character when a break signal is received from the terminal.

  If the CS/1-HSM is connected to a VAX running VMS, this parameter should be set to 0x19 (<CTRL-Y>).

The remaining parameters in the menu should not be altered unless the CS/1-HSM is running custom software.

A.5 Setting CS/1-SNA Parameter Values

Option 8 of the View/Alter menu on the CS/1-SNA applies specifically to the CS/1-SNA, and is used to define the interface between the CS/1-SNA and the host's communications processor.

The default values of many parameters are factory set to standard values, and need not be specified unless a different value is required; other parameters have no factory default and must be specified.

The network manager or host system administrator must also run the host system generation procedure to specify appropriate values on the host side. For further information on SNA host system generation, see reference [9].

For the CS/1-SNA, the option 8 menu consists of a list of 11 parameters and submenus that define the SDLC protocol interface and three submenus that define the SNA protocol interface.

The SDLC protocol interface is defined by the following parameters and submenus:

- The Station Address parameter specifies the SDLC station address of the CS/1-SNA. The parameter value must be in the range 0x0 through 0xFF, and must match the address specified by the host. The default value is 0xC1.
- The SDLC Window Size parameter specifies the maximum permitted number of outstanding unacknowledged SDLC frames. This value must match the window size specified by the host. The default value is 7.
- The Maximum SDLC Frame Size parameter specifies the maximum size, in bytes, of an SDLC frame. The size includes the SDLC header, the transmission header (TH), the request/response header (RH), and the request/response unit (RU). The value must match the maximum frame size specified by the host. The default value is 0x10B (decimal 267). Increasing the value of this parameter may affect MCPU buffer allocation; contact Bridge Communications, Inc., or an authorized service representative for detailed information.
- The Number of Devices parameter specifies the maximum number of Logical Units (LUs) supported by the CS/1-SNA. The value must be equal to or less than the maximum number of LUs specified by the host. The parameter value must be in the range 0x1 through 0x18; the default value is 0x10.
- The Exchange ID parameter specifies the value of the third field of the CS/1-SNA's Exchange ID. An Exchange ID is a 12-digit hexadecimal number that identifies the terminal cluster to the host. The ID consists of three fields; only the third field can be specified. The first field (4 digits) identifies the physical unit type; PU type 2 (0x0200) is the only value currently supported. The second field (3 digits) specifies that the CS/1-SNA emulates a 3274 cluster controller (0x017). The third field (5 digits) is a unique ID assigned to this CS/1-SNA. The entire Exchange ID must match the ID specified for the CS/1-SNA by the host. This parameter need not be specified if the CS/1-SNA is directly connected to the 37x5; it is applicable only to switched or leased lines.
- The Baud Rate parameter determines the speed of the link between the CS/1-SNA and the host. The CS/1-SNA supports speeds from 110 baud to 64K baud; the default is 4800 baud. This parameter is applicable only if the receive clock and transmit clock are set to internal.

- The Duplex parameter determines whether the link is full duplex or half duplex. If the parameter is set to Full, the SIO board provides a Bell 212-type interface. If the parameter is set to Half, the SIO board provides a Bell 208-type interface.

  This parameter is affected by the setting of the Line Mode parameter (see Table A-2). The default is half duplex for switched lines and full duplex for leased lines and direct connections. To override the default combination, first set Line Mode appropriately, and then set Duplex to the desired value.

- The Interface Type parameter determines whether the CS/1-SNA functions as a DTE or as a DCE. This parameter is affected by the setting of the Line Mode parameter (see Table A-2). The default value is DTE for switched or leased lines and DCE for direct connection. If the parameter is set to DCE, the connector cable must be a synchronous host cable rather than the standard synchronous modem cable. To override the default combination, first set Line Mode appropriately, and then set Interface Type to the desired value.

- The Sense DCD parameter determines the function of the DCD line (pin 8) on the RS-232 interface. The parameter value is affected by the setting of the Line Mode parameter (see Table A-2) and the parameter function is affected by the settings of the Duplex and Interface Type parameters (see Table A-3).

  The default value of the Sense DCD parameter is ON for switched lines and OFF for direct connections and leased lines. To override the default combination, first set Line Mode appropriately, and then set Sense DCD to the desired value.

- The Mark Idle parameter determines whether an idle line is in mark state (ON) or sync state (OFF). This parameter is affected by the setting of the Line Mode parameter (see Table A-2). The default value is ON for switched lines, leased lines, and direct connections. To override the default combination, first set Line Mode appropriately, and then set Mark Idle to OFF.

- The Line Mode parameter determines whether the line is a switched line, a leased line, or a direct connection. The default value is switched line. Changing the value of this parameter automatically changes the values of the Duplex, Interface Type, Sense DCD, and Mark Idle parameters. The effect of Line Mode on these other parameters is illustrated in Table A-2.

The SNA protocol interface is defined by selecting the following three parameters:

- The Negative Response parameter specifies how the CS/1-SNA responds to an activate message from the host. The host may expect no response, or may expect a negative response plus sense code 8004 (illegal destination address field). The default value is no response.

- The Device Types parameter determines the device type of each logical unit (LU) specified in the Number of Devices parameter. The possible device types are Screen and Printer. By default, devices 2 and 3 are printer LUs and the remainder are screen LUs. The menu has 24 fields; if fewer than 24 devices are specified by the Number of Devices parameter, the program automatically sets the device type of any LU not present to Disabled.

- The Default Printer parameter may be used to associate a printer LU with one or more screen LUs. For each LU defined as a screen by the Device Types parameter, the user may specify an associated printer. A single printer LU may be associated with more than one screen LU. By default, printer 2 is associated with screen 0, and printer 3 is associated with screen 1.

Table A-2 Effect of Line Mode on Other Parameters

	Switched Line	*Leased Line*	*Direct Connect*
Duplex	Half	Full	Full
Interface Type	DTE *	DTE *	DCE **
Sense DCD	ON	OFF	OFF
Mark Idle	ON	ON	ON

* Requires use of synchronous modem cable (CBL-SM-25).
** Requires use of synchronous host cable (CBL-SH-25).

Table A-3 Interaction Among Sense DCD, Duplex, and Interface Type Parameters

Case	*Sense DCD*	*Duplex*	*Interface Type*	*Result*
1	ON	Full	DTE	The SIO firmware uses DCD to place the receiver in and out of hunt phase. DCD is on pin 8 on an SIO-SM board and on pin 20 on an SIO-ST board or a CS/100.
2	ON	Full	DCE	The SIO firmware uses RTS to place the receiver in and out of hunt phase. RTS is on pin 5 on an SIO-SM board and on pin 4 on an SIO-ST board or a CS/100.
3	ON	Half	DTE	The SIO firmware uses DCD to place the receiver in and out of hunt phase. DCD is also used to condition transmission; when DCD is true, transmission is inhibited. In this configuration, the DCE device must toggle DCD. DCD is on pin 8 on an SIO-SM board and on pin 20 on an SIO-ST board or a CS/100.
4	ON	Half	DCE	The SIO firmware uses RTS to place the receiver in and out of hunt phase. RTS is also used to condition transmission; when RTS is true, transmission is inhibited. In this configuration, the DCE device must toggle RTS. RTS is on pin 5 on a SIO-SM board and on pin 4 on an SIO-ST board or a CS/100.
5	OFF	Full	DTE	The SIO firmware ignores DCD. DCD is on pin 8 on an SIO-SM board and on pin 20 on an SIO-ST board or a CS/100.
6	OFF	Full	DCE	The SIO firmware ignores RTS. CTS is constant. RTS is on pin 5 on an SIO-SM board and on pin 4 on an SIO-ST board or a CS/100. CTS is on pin 4 on an SIO-SM board and on pin 5 on an SIO-ST board or a CS/100.
7	OFF	Half	DTE	RTS is toggled by the SIO firmware at line turnaround points and transmission waits for CTS. RTS is on pin 4 on an SIO-SM board and on pin 5 on an SIO-ST board or a CS/100.
8	OFF	Half	DCE	DCD is toggled by the SIO firmware at line turnaround points. RTS is on pin 20 on an SIO-SM board and on pin 8 on an SIO-ST board or a CS/100.

A.6 Setting CS/1-TCP and CS/100-TCP Parameter Values

Three options of the View/Alter menu apply specifically to servers running TCP/IP protocols:

```
3.  IP Parameters
4.  TCP Parameters
8.  Service Listener Port List
```

Option 3 is used to specify the internet address assigned to the server; this is the only mandatory portion of CS/1-TCP sysgen. Option 4 is used to specify the maximum number of retransmissions. Option 8 is used to add a service listener port. These options are described below. The other options are the same as those for the CS/1-A running XNS protocols.

Option 3 (IP Parameters) is used to assign the server's internet address and optionally modify it with a subnet mask.

- Select option 3 of the IP Parameters submenu to assign an internet address to the server. An internet address must be assigned.

  The network portion of the address must be the same for all TCP servers on the same network, and the host portion of the address must be unique for each TCP server on the network.

  The conventions for specifying TCP/IP internet addresses are described in reference [10].

- Select option 4 of the IP Parameters submenu to enter the server subnet mask. The server subnet mask is optional, and need be established only if the network includes subnets.

  An internet address consists of 32 bits divided into four 8-bit subfields. Normally these fields are divided between the network and host fields as described in reference [10]. Some TCP/IP networks, however, extend the network field with an additional field called the subnet field, which is used to indicate a particular physical segment. The subnet field is formed by taking the leading bits from the host field. The entire address still has 32 bits.

  The subnet mask is a 32-bit number; each bit of the mask that coincides with the network field must be set. For example, 126.000.000.000 is a class A internet address. To extend this network number by a subnet field that would provide for up to 16 subnets requires a 4-bit subnet field. The binary representation of this subnet mask is as follows, where the first field (11111111) masks the network field of the internet address, and the second field (11110000) extends the network field by four bits:

  (11111111).(11110000).(00000000).(00000000)

  The decimal representation of this binary number is:

  255.240.000.000

  Determine the binary representation of the subnet mask necessary to provide the desired number of subnets, and convert it to decimal. When prompted, enter the decimal representation of the subnet mask and press the return key.

Option 4 (TCP Parameters) is optionally used to specify maximum retransmissions. Do not change the user-to-TCP or IP-to-TCP data mailbox depth.

Option 8 (Service Listener Port List) is optionally used to add or delete a service listener port. The Telnet service listener port (option 1) and Rlogin service listener port (option 2) are provided by default and cannot be changed. The last option may be used to add or delete other user-defined services as necessary. The assigned service listener ports can be found in the RFC 943 document.

Up to eight service ports, in addition to Telnet and Rlogin, are allowed in this menu. These service ports can be used to export the TCP interface to a serial line. The host could bind a process to that line to accept incoming data units from the active side of the particular service and generate appropriate responses for the service protocol.

Service ports are available only on the passive end of a connection. The remote service cannot be selected when making a connection from a terminal attached to a CS/1-TCP; only the Telnet service is available.

A.7 Setting CS/1-X.25 Parameter Values

Three options of the View/Alter menu are applicable to the CS/1-X.25: option 5 (Virtual Terminal Parameters), option 8 (X.25 Parameters), and option 9 (X.25 Address Configuration).

Option 5 of the View/Alter menu on the CS/1-X.25 contains a submenu. Option 2 of this submenu is used to map virtual ports to lines.

The default mapping distributes 48 virtual ports evenly among eight lines. If the system has only one line, all 48 virtual ports should be assigned to that line. If the system has multiple lines of different speeds to a single X.25 host, the mapping can be used to distribute the load by assigning more virtual ports to the faster line(s). Or, if each line is connected to a different host, more virtual ports can be assigned to the host that typically has higher traffic loads.

The lines are numbered 0 through 7, arranged as shown in Table A-4.

Table A-4
CS/1-X.25 Line Numbers

Line Number	*Board Number*	*Port Number*
0	1	0
1	1	1
2	2	0
3	2	1
4	3	0
5	3	1
6	4	0
7	4	1

Option 8 of the View/Alter menu on the CS/1-X.25 is used to define the interface between the CS/1-X.25 and the X.25 host.

The parameters are requirements of the X.25 interface, and must be specified for each physical line attached to the CS/1-X.25. The default values of many of the parameters are factory set to values appropriate for a Telenet-compatible host; obtain the appropriate values from the X.25 host documentation.

The option 8 menu lists three submenus: Line Parameters, X.25 Level 2 Parameters, and X.25 Level 3 Parameters. To display the current value of a parameter or to change a parameter in any of these categories, select the appropriate submenu. The system first prompts for the number of the physical line to which the parameters apply, then displays the selected submenu.

The Line parameter determines the address and physical characteristics of each line, and must be specified once per line:

- The Baud Rate parameter specifies the speed of the synchronous line connected to the CS/1. The default line speed for all lines is 4800 baud.

**** NOTE ****

If two lines connected to the same SIO board are of different speeds, the higher-speed line must be connected to port 0 and the lower-speed line must be connected to port 1.

The X.25 Level 2 parameters are as follows:

- The X.25 Level 2 Window Size parameter specifies the X.25 variable K, which represents the maximum number of outstanding unacknowledged packets permitted at Level 2. The value specified must be in the range 1 through 7; the default value is 7.
- The T1 Timer parameter specifies the value (in milliseconds) of the Level 2 retransmission timer. The value of this parameter depends on the requirements of the X.25 interface; the default value is 3000 milliseconds.
- The T3 Timer parameter specifies the value (in milliseconds) of the X.25 Link Initialization timer. The value of this parameter depends on the requirements of the X.25 interface; the default value is 90000 milliseconds.
- The Number of Retries parameter specifies the value of the X.25 variable N2, which determines how many retries are permitted after the T1 timer elapses. The value of this parameter depends on the requirements of the X.25 interface; the default value is 20, counting both the original transmission and subsequent retransmissions.

The X.25 Level 3 parameters are as follows:

- The DTE or DCE parameter determines whether the CS/1-X.25 functions as a DTE or a DCE. The default value is DCE.
- The X.25 Level 3 Packet Size parameter specifies the maximum packet size permitted by the X.25 interface. The value of this parameter depends on the requirements of the X.25 interface; typical sizes are 128 bytes, 256 bytes, 512 bytes, and 1024 bytes. The default value is 128 bytes. Increasing the value of the Packet Size parameter may affect MCPU buffer allocation; contact Bridge Communications, Inc., or an authorized service representative for detailed information.

  The CS/1-X.25 also uses the value of the Level 3 Packet Size parameter to obtain the value of the X.25 variable N1 (the maximum number of bytes per frame). The value of N1 is calculated as the Level 3 Packet Size plus two bytes of HDLC header and three bytes of X.25 Level 3 header.
- The X.25 Level 3 Window Size parameter specifies the maximum number of outstanding unacknowledged packets permitted at Level 3. The range of permitted values is 1 through 7; the default value is 2.
- The Take Reverse Charge Call parameter determines whether the CS/1-X.25 allows reverse charge X.25 calls from the host to the Ethernet. By default, reverse charge calls are accepted.

- The Make Reverse Charge Call parameter determines whether all calls from the CS/1-X.25 to the host are reverse charged. By default, calls are not reverse charged.
- The Incoming Calls Barred parameter determines whether incoming calls (i.e., from the host to the Ethernet) are accepted or refused. By default, incoming calls are accepted.
- The Outgoing Calls Barred parameter determines whether outgoing calls (i.e., from the Ethernet to the host) are accepted or refused. By default, outgoing calls are accepted.
- The Number of Clear Request Retries parameter specifies the maximum number of times a clear request may be retransmitted. The range of permitted values is 1 through 10; the default value is 3.
- The Number of Reset Request Retries parameter specifies the maximum number of times a reset request may be retransmitted. The range of permitted values is 1 through 10; the default value is 4.
- The Number of Logical Channels parameter specifies the maximum number of logical channels permitted per physical line. The value of this parameter depends on the requirements of the X.25 interface; the default maximum is 20.
- The Beginning of SVC Channel Number parameter specifies both the Logical Channel Group Number (LCGN) and the number of the first logical channel on the line. The value specified must be in the range 001 through 7FF, in the format "xyy", where "x" represents the LCGN and "yy" represents the number of the first logical channel on the line. If "x" is omitted, the LCGN defaults to 0; if the parameter is not specified at all, both LCGN and first logical channel number default to 1.
- The T10, T11, T12, and T13 parameters specify the values (in milliseconds) of the X.25 Level 3 DCE timers. The values of these parameters depend on the requirements of the X.25 interface; Table A-5 lists the default values.
- The T20, T21, T22, and T23 parameters specify the values (in milliseconds) of the X.25 Level 3 DTE timers. The values of these parameters depend on the requirements of the X.25 interface; Table A-5 lists the default values.

Table A-5 X.25 Level 3 DCE and DTE Timer Values

Timer Name	*Default Value**
T10	60000
T11	180000
T12	60000
T13	60000
T20	180000
T21	200000
T22	180000
T23	180000

* Expressed in milliseconds.

Option 9 of the View/Alter menu on the CS/1-X.25 is used to define the X.25 address of each physical line attached to the CS/1-X.25.

A.8 GS/1 System Generation

The GS/1 system generation parameters include Connection Service parameters, Interconnection Service parameters, and parameters that are identical to the CS/1 Connection Service modules. System generation is required to set the Connection and Interconnection Service parameters.

The GS/1 provides a network-layer Interconnection Service. The service uses the medium of an X.25 network to transmit packets between two networks that both use the IDP protocol. The GS/1 also provides automatic call setup services if the server is connected with the X.25 network through dedicated lines. For more information, see references [1] and [14].

The GS/1 must be configured with three types of information; the following subsections describe how to sysgen each type:

- **Internetwork configuration--Local network parameters:** the network address of the Ethernet to which the server is attached and the X.25 address of each line connecting the GS/1 with an X.25 network.

  The GS/1 uses the Ethernet network address when communicating with devices on remote Ethernets.

  The GS/1 uses the local X.25 line addresses when it sends packets from the Ethernet device that originates the connection to the X.25 network that carries the transmission. The GS/1 specifies the address of the line on which the data is sent as the source of the transmission, for the benefit of the receiving device on the X.25 network. Answering packets are sent to the X.25 line address specified in the original transmission. The X.25 network controller tracks the addresses of all devices on the network and routes packets directly to the destination lines.

  The GS/1 does not refer to the X.25 addresses of its own lines before accepting transmissions; it processes any packet routed by the X.25 network controller to one of its lines. However, when the GS/1 receives a transmission from a device on the X.25 network that is not already part of an active session, the GS/1 compares the destination address of the packet with the address of the line on which the packet was received. If the addresses do not match, the GS/1 automatically treats the packet as a Connection Service connection request and interprets the destination address as a clearinghouse name. To implement the pass-through service, assign the line a different address from the address used by the X.25 network for that line. Reference [10] describes the X.25 pass-through service in more detail.

  Internetwork configuration--Remote network parameters: The network addresses of all accessible remote Ethernets and the X.25 addresses of the lines leading to their GS/1s. Sysgen of this information is mandatory for the GS/1 Interconnection Service; it is optional for GS/1s running the Connection Service only.

- **Line characteristics:** the physical and network characteristics of each line connecting the GS/1 with an X.25 network.

  The GS/1 uses the line characteristics to interact correctly on the physical level with the attached devices.

- **Line mapping and user interface status:** the mapping between virtual port numbers and physical line numbers and the status of the Connection Service interface on each line (incoming call service parameters).

  The GS/1 uses the port-to-line mapping to route connections from the Ethernet side of the circuit to the X.25 side of the circuit. If all lines attached to the GS/1 are connected to the same X.25 network, the port-to-line mapping is usually not important. If different lines are connected to different X.25 networks, however, the port-to-line mapping can be used to facilitate rotaries for connection routing and to allocate ports as needed for different applications on different lines.

  The GS/1 uses the incoming call service parameter to enable or disable the user interface on each line. If the interface is disabled on a line, that line can be used only with the connection pass-through service, described in reference [10], and for connections from the Ethernet network to the X.25 network.

A.8.1 Internetwork Configuration

The local and remote network parameters are configured through the Internetwork Configuration module, option 9 on the Module Select menu.

To set the parameters, choose option 9 from the Module Select menu. The system responds with a two-option menu:

```
1. Local network parameters

2. Remote network parameters
```

To set the local network parameters, choose option 1 from the Internetwork Configuration menu. The system responds with a nine-option menu:

```
1. Local network address

2. Line 0 X.25 address

3. Line 1 X.25 address

4. Line 2 X.25 address

5. Line 3 X.25 address

6. Line 4 X.25 address

7. Line 5 X.25 address

8. Line 6 X.25 address

9. Line 7 X.25 address
```

Each line leading to an X.25 PDN is assigned an X.25 address by the PDN to which it is attached. X.25 addresses contain up to 15 decimal digits. The first 4 digits represent the Data Network Identification Code (DNIC). The next 6 to 8 digits (usually 8 for U.S. networks) represent the host address; and the last 2 to 4 digits (usually 2 for U.S. networks) represent a subhost address or port number. Not all fields appear in every installation; an individual X.25 address can be much shorter than 15 digits. Trailing zeros can be omitted.

For a private line (i.e., a line not connected to an X.25 network), enter the letter "p" instead of an X.25 address.

To set the remote network parameters, choose option 2 from the Internetwork Configuration menu. The system responds with the following:

```
1. Add remote network
```

The GS/1 Interconnection Service uses the X.25 line addresses and the remote Ethernet addresses to select the appropriate lines on which to send packets destined for remote networks. Each line leading from the GS/1 is assigned a single X.25 address by the X.25 network to which the line is connected. Each X.25 address is associated with a single Ethernet network address. When the GS/1 Interconnection Service receives a packet destined for a remote Ethernet, it sends it out on the line associated with that Ethernet.

A.8.2 Line Characteristics

The physical and network characteristics of the lines are specified through the X.25 Parameters module, option 8 on the Module Select menu.

The appropriate settings of most X.25 parameters depend on the requirements of the X.25 network to which the server is attached. These parameters are described here very briefly. For detailed information, see references [17] and [18]. The default values shipped with a new system are set to be compatible with Telenet; if a different X.25 PDN is used, contact an agent of the PDN for the appropriate values.

The X.25 parameters module is divided into three parts: physical parameters, X.25 Level 2 parameters, and X.25 Level 3 parameters. The values for each parameter type are defined for one line number at a time.

Physical Parameters

The baud rate parameter specifies the speed of the synchronous line connected to the GS/1. The default speed for all lines is 4800 baud.

**** NOTE ****

If two lines connected to the same SIO board are of different speeds, the higher-speed line must be connected to port 0 and the lower-speed line must be connected to port 1.

X.25 Level 2 Parameters

- The X.25 variable K specifies the X.25 Level 2 window size, which represents the maximum number of outstanding unacknowledged packets permitted at Level 2. The value specified must be in the range 1 through 7; the default value is 7.

- The T1 timer specifies the value (in milliseconds) of the Level 2 retransmission timer. The value of this parameter depends on the requirements of the X.25 PDN; the default value is 3000 milliseconds.
- The T3 timer specifies the value (in milliseconds) of the X.25 Link Initialization timer. The value of this parameter depends on the requirements of the X.25 PDN; the default value is 90000 milliseconds.
- The X.25 variable N2 specifies the number of retries permitted after the T1 timer elapses. The value of this parameter depends on the requirements of the X.25 PDN; the default value is 20, counting both the original transmission and subsequent retransmissions.

X.25 Level 3 Parameters

- The DTE/DCE parameter specifies the type of connector on the server end of the cable. For interaction with a DCE device (e.g., a modem), the DTE/DCE parameter should be set to 0 (DTE). For interaction with a DTE device, the parameter should be set to 1 (DCE). The default value is 1.
- The X.25 Level 3 packet size parameter specifies the maximum packet size permitted by the X.25 network. The value of this parameter depends on the requirements of the X.25 PDN; typical sizes are 128 bytes, 256 bytes, 512 bytes, and 1024 bytes. The default value is 128 bytes. Increasing the value of the packet size can affect MCPU buffer allocation; contact Bridge Communications, Inc., or an authorized service representative for detailed information.

  The GS/1 also uses the value of the Level 3 packet size parameter to obtain the value of the X.25 variable N1 (the maximum number of bytes per frame). The value of N1 is calculated as the Level 3 packet size plus two bytes of HDLC header and three bytes of X.25 Level 3 header.
- The X.25 Level 3 window size parameter specifies the maximum number of outstanding unacknowledged packets permitted at Level 3. The range of permitted values is 1 through 7; the default value is 2.
- The take reverse-charged calls parameter specifies whether or not the line accepts reverse-charged calls. The default of 1 accepts reverse-charged calls.
- The make reverse-charged calls parameter specifies whether or not the line reverses the charges when making a call. The default of 0 does not reverse the charges.
- The incoming calls barred parameter specifies whether or not incoming calls are allowed. The default of 0 allows incoming calls.
- The outgoing calls barred parameter specifies whether or not outgoing calls can be made. The default of 0 allows outgoing calls.
- The number of clear request retries parameter specifies the maximum number of times a clear request may be retransmitted. The range of permitted values is 1 through 10; the default value is 3.
- The number of reset request retries parameter specifies the maximum number of times a reset request may be retransmitted. The range of permitted values is 1 through 10; the default value is 4.

- The number of logical channels parameter specifies the maximum number of logical channels permitted per physical line. The value of this parameter depends on the requirements of the X.25 PDN; the default maximum is 20.
- The beginning SVC channel number parameter specifies the lowest number in the LCN subrange. The value must be in the range 1 through 7FF. The default value is 1.
- The T10, T11, T12, and T13 parameters specify the values (in milliseconds) of the X.25 Level 3 DCE timers. The values of these parameters depend on the requirements of the X.25 PDN; Table A-5 lists the default values.
- The T20, T21, T22, and T23 parameters specify the values (in milliseconds) of the X.25 Level 3 DTE timers. The values of these parameters depend on the requirements of the X.25 PDN; Table A-5 lists the default values.

A.8.3 Line Mapping and User Interface Status

The line mapping table determines which virtual port numbers are used for communicating with which X.25 networks when the GS/1 provides connections from devices on an Ethernet network to devices on one or more X.25 networks.

The incoming call service parameters determine whether or not the Connection Service interface is available on each line.

The mapping and incoming call service parameters are established through the Virtual Terminal parameter module, option 5 on the Module Select menu. The Virtual Terminal submenu contains eight options:

```
1. Maximum number of sessions

2. Mailbox depth to SPP

3. Mailbox depth to agent

4. MORE-Bit disabled or enabled

5. Autolisten timer

6. Use PEP/BTP

7. X.25 incoming call service

8. Virtual port to physical line mapping
```

In most standard installations, the default settings of the first six parameters are appropriate. Option 1 merely determines the maximum number of simultaneous sessions available to a single virtual port. Option 4 should be set to disabled if connections will be made to the GS/1 from CS/1s running software version 1.6500 or earlier. Before changing any other of the first six parameters, refer to the *Software Technical Reference Manual* for more information.

The default settings of the X.25 incoming call service parameters make the Connection Service interface available on all lines. To suppress the interface on one or more lines, first choose option 7 from the Virtual Terminal submenu, then choose the menu option for the line number to be changed. Set the parameter to 0 to disable the Connection Service interface or to 1 to enable it.

To alter the port-to-physical-line mapping table, choose option 8 from the Virtual Terminal submenu. On a GS/1 with four SIO boards supporting two lines each, the default mapping table is often appropriate. Table A-6 lists the default mapping between virtual ports and line numbers.

On a GS/1 with fewer than four lines, or in an application in which the load on one or more lines is much greater than on other lines, some adjustment of the port-to-line mapping may be appropriate.

Table A-6 Default Mapping Between Port Numbers and Lines on the GS/1

Port Numbers	*Line Number*	*Line Location*
0 - 5	0	Connector 0, SIO board 1
6 - 11	1	Connector 1, SIO board 1
12 - 17	2	Connector 0, SIO board 2
18 - 23	3	Connector 1, SIO board 2
24 - 29	4	Connector 0, SIO board 3
30 - 35	5	Connector 1, SIO board 3
36 - 41	6	Connector 0, SIO board 4
42 - 47	7	Connector 1, SIO board 4

A.8.4 Other GS/1 Parameters

The GS/1 Module Select menu includes a number of parameter modules identical to the CS/1 Connection Service modules:

Kernel parameters
IDP parameters
SPP parameters
User Interface parameters
Statistics Monitoring parameter
Clearinghouse parameter

In most installations, none of these parameters needs to be altered.

The User Interface parameters are primarily concerned with privilege levels necessary for various Connection Service commands. This module has no meaning for the GS/1 Interconnection Service.

The Clearinghouse parameter determines whether or not the GS/1 distinguishes between upper and lower case in clearinghouse names. The Statistics Monitoring parameter specifies the sampling interval used for the Busiest Sample network management report (see Section 4.2 for a description of the network management reports).

The parameters in the other modules should be set only for custom applications and only by someone with a thorough understanding of the internal system software. These parameters are described only briefly within the Sysgen program; for more detailed descriptions, see the *Software Technical Reference Manual.*

A.9 GS/3 System Generation

The GS/3 system generation parameters include Interconnection Service parameters only.

The GS/3 provides a network-layer Interconnection Service. The service routes packets between two networks that both use the IDP protocol and takes care of all call setup and load balancing in between.

Automatic call setup requires a leased line between the server and the remote GS/3. On a switched line, the user must dial manually.

To support the Interconnection Service, a GS/3 must be configured with two kinds of information:

- The network number of the Ethernet to which the GS/3 is directly connected.

  The GS/3 uses this number to identify itself when communicating with remote Ethernets.

- The network numbers of all remote Ethernet networks and the line numbers and physical characteristics of the lines connecting the GS/3 with those networks.

  The GS/3 uses the list of remote Ethernet numbers and the associated line numbers to create a routing table for sending packets to the remote networks. Reference [3] describes routing tables.

If the GS/3 has multiple lines to a single remote Ethernet, the GS/3 monitors response time and reliability on each line, automatically switching packets to different lines when necessary. If a line remains idle for the time interval used by the reliability checking algorithm, the server sends a probe packet to test the line. If no acknowledgement is received, the GS/3 removes the line from the routing table until subsequent probes show that it is operational.

The initial routing table is established through option 6, Internetwork Configuration, on the main Module Select menu. These parameters must be set for every GS/3.

The Internetwork Configuration submenu contains three options:

```
1. Local network address

2. Line configuration

3. Line map display
```

The local Ethernet network number must be set first. The conventions for entering Ethernet numbers are described in Section A.8.1.

To set the parameters for the lines attached to the server's SIO boards, choose option 2 from the Internetwork Configuration submenu. The system first prompts for a line number in the range 0 through 7. For reference, Table A-7 lists the eight possible lines, their locations, and their port numbers. (The port numbers are used only in the network statistics reports described in Section 4.0.)

Table A-7 GS/3 Line Numbers

Line Number	*Location*	*Port Number*
0	Connector 0, SIO board 1	0
1	Connector 1, SIO board 1	1
2	Connector 0, SIO board 2	8
3	Connector 1, SIO board 2	9
4	Connector 0, SIO board 3	16
5	Connector 1, SIO board 3	17
6	Connector 0, SIO board 4	24
7	Connector 1, SIO board 4	25

For each line number, the system prompts for three parameters:

1. `Baud rate`
2. `Clock selection`
3. `Network ID of remote Ethernet`

The default baud rate for all lines is 4800. Reset this parameter for each line that operates at a different baud rate.

When entering the network number of the remote Ethernet for each line, follow the conventions for entering the local Ethernet number described in Section A.8.1. The system does not accept a remote network address that is identical to the address already specified for the local address.

To review the settings of all lines, choose the third option from the Internetwork Configuration menu.

When all the required information has been entered, first press the escape key as often as necessary to return to the main Sysgen menu and then select the save option to save the information on the diskette.

A.10 GS/4 System Generation

To support the Interconnection Service, a GS/4 must be configured with two kinds of information:

- The network address of the local network.
- The network address of the remote network.

Both of these addresses are configured through the Internetwork Configuration parameter module, option 7 on the Module Select menu.

To specify the addresses, first select option 7 of the Module Select menu. The program displays the Internetwork Configuration menu:

```
1. EBA network address

2. SBA-E network address
```

Option 1, "EBA Network Address", is used to establish the network address of the local network that is attached to the transceiver connector labeled "EBA" on the GS/4.

Option 2, "SBA-E Network Address", is used to establish the network address of the remote network that is attached to the transceiver connector labeled "SBA-E" on the GS/4.

The sources of these addresses and the conventions for entering them are described in Section A.8.1.

A.11 GS/6 System Generation

To support the Interconnection Service, a GS/6 must be configured with three kinds of information:

- The local network address.
- The local link address.
- Remote network parameters, including the remote network address and the remote link address. The remote network parameters must be specified for each remote GS/6 that will be accessed via the broadband network by the GS/6 on which Sysgen is run.

This information is configured through the Internetwork Configuration parameter module, option 7 on the Module Select menu.

First select option 7 of the Module Select menu. The program displays the Internetwork Configuration menu:

```
1. Local network address

2. Local link address

3. Remote network parameters
```

Option 1, "Local network address", is used to establish the network address of the local Ethernet network.

The sources of these addresses and the conventions for entering them are described in Section A.8.1.

Option 2, "Local link address", is used to establish the local link addresses. The local link address is the address of the GS/6 on the broadband network. The local link address may be selected independently of the individual network addresses and must be entered in the range 01 to FF hexadecimal.

Option 3, "Remote network parameters", consists of the following submenu:

```
1. Add remote network
```

When this option is selected, the Sysgen program prompts for the remote network address and the remote link address. Select this option and specify the appropriate addresses for each remote GS/6 that will be accessed via the broadband network by the GS/6 on which Sysgen is run.

The sources of these addresses and the conventions for entering them are described in Section A.8.1.

APPENDIX B

PORT CONFIGURATION

This appendix describes the port configuration parameters and provides sample configurations for devices of various types. The information is grouped into the following sections:

- Section B.1 describes the configuration parameters applicable to asynchronous ports and provides sample configurations appropriate for various asynchronous devices.
- Section B.2 describes the configuration parameters applicable to character-synchronous ports and provides sample configurations appropriate for various character-synchronous devices.
- Section B.3 describes the configuration parameters applicable to bit-synchronous devices and provides sample configurations appropriate for various bit-synchronous devices.
- Section B.4 describes the configuration parameters applicable to ports on the CS/1-X.25.
- Section B.5 describes the configuration parameters applicable to the IVECS.
- Section B.6 describes the configuration parameters applicable to the CS/1-HSM, the CS/1-SNA, and the CS/100-488.
- Section B.7 describes the configuration parameters applicable to Gateway Servers.

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 parameters, 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 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, CS/100-488, and IVECS, only default parameter tables can be altered, and only a limited number of parameters apply.

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 B-1 illustrates the effects of these commands. Reference [10] 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 SET-Default 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 (the parameters are listed in Section B.2). 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 <^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.

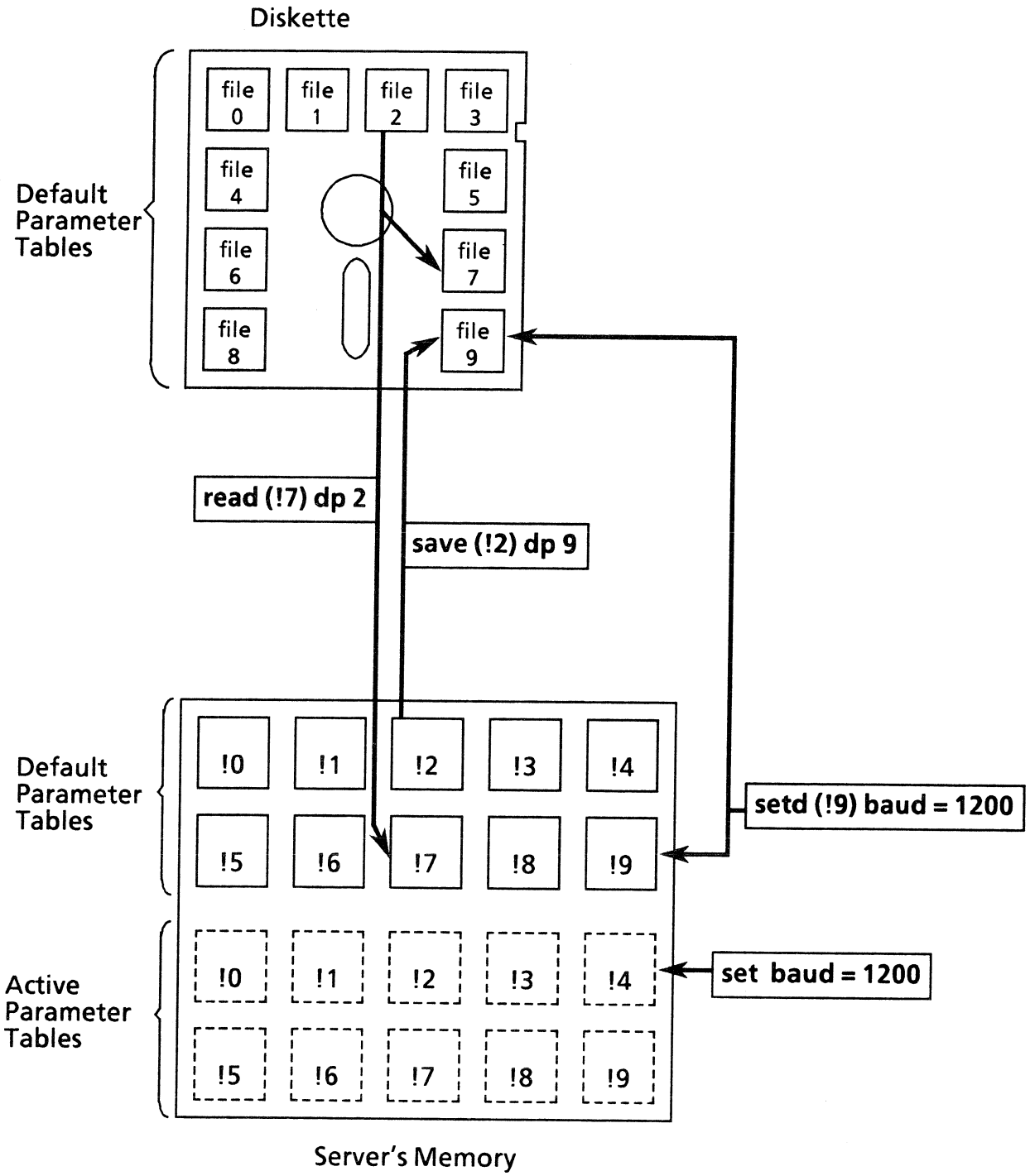


Figure B-1 Effects of the ReaD, SAve, SET, and SETDefault Commands

B.1 Asynchronous Server Configuration Parameters

Table B-1 lists all asynchronous port parameters alphabetically and gives the section number of each description. Upper case characters represent the minimum unambiguous abbreviation of each parameter. All of the parameters apply to ports on a CS/1-A, CS/100-A, and CS/200. For ports on TCP servers, all of the parameters apply except AccessGroup, AccessWord, DOmain, and Organization.

Table B-1
Asynchronous Configuration Parameter Summary

Parameter	*Section*	*Parameter*	*Section*
AccessGroup *	B.1.1	GlobalPassWord	B.1.5
AccessWord *	B.1.1	GroupxPasswd	B.1.5
AUditServerAddr	B.1.5	IdleTimer	B.1.3
AUToDisconnect	B.1.1	InitMacro	B.1.1
BAud	B.1.2	InterAction	B.1.1
BootServerAddr	B.1.5	LFDelay	B.1.2
BReakAction	B.1.3	LFInsertion	B.1.3
BReakChar	B.1.3	LFPad	B.1.2
BSDelay	B.1.2	LineERAse	B.1.4
BSPad	B.1.2	LinePRotocol	B.1.2
BUffersize	B.1.1	LocalEDiting	B.1.4
CONNectAudit	B.1.5	LocalPassWord	B.1.5
CRDelay	B.1.2	LongBReakAction	B.1.3
CRPad	B.1.2	MaxSessions	B.1.1
DataBits	B.1.2	MOde	B.1.3
DataForward	B.1.3	NMPrompt	B.1.5
DATE	B.1.5	Organization *	B.1.5
DeVice	B.1.1	PARIty	B.1.2
DIsconnectAction	B.1.3	PRIvilege	B.1.1
DOmain *	B.1.5	PROMPt	B.1.5
DUplex	B.1.2	ReprintLine	B.1.4
ECHOData	B.1.3	StopBits	B.1.2
ECHOMask	B.1.3	TabDelay	B.1.2
ECMChar	B.1.3	TabPad	B.1.2
EOM	B.1.3	UseDCDout	B.1.2
ERAse	B.1.4	UseDTRin	B.1.2
ERRorAudit	B.1.5	VERBatim	B.1.4
FFDelay	B.1.2	WelcomeString	B.1.5
FFPad	B.1.2	WordERAse	B.1.4
FlowControlFrom	B.1.3	XOFF	B.1.3
FlowControlTo	B.1.3	XON	B.1.3
FlushVC	B.1.3		

* Not applicable to TCP servers.

B.1.1 Asynchronous Port Transmission Parameters

This section describes the asynchronous port transmission parameters, usually set by the network manager for each port. The parameters and their permitted values are listed in Table B-2. Except for the PRIvilege parameter, these parameters apply to both asynchronous and synchronous ports.

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 B-2 Asynchronous Port Transmission Parameters

Parameter	*Permitted Values*
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)
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)
MaxSessions	<number> (1-8 sessions)
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 3.2. 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 B.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 **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 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.

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 the CS/1, 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, the default values are Host for ports 8 and 9, and Terminal and Glass for ports 0 through 7.

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 and the DEFine command are described in reference [10].

**** 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" (reference [10] provides further information).

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. This pair of values also determine whether broadcast messages are preceded by a header indicating the port number of the sender of the message. Reference [10] lists all error messages and their corresponding error numbers. 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.

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 (reference [10] 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.

B.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 B-3.

Table B-3 Asynchronous Port Physical Parameters

Parameter	*Permitted Values*
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
PARIty	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.

- On the CS/1 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 of one of the numeric values listed in Table B-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 may be set. 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 a CS/1-A or a CS/100-A, 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 CS/1 SIO board and ports 8 and 9 on the CS/100).

  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 the CS/1-A, CS/100-A, CS/200, and IVECS. Only some ports on other Communications Server types support this option. Refer to the appropriate *Planning and 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 B-2; Table B-12 lists recommended settings of the UseDCDout parameter for use with various devices (both figure and table are in Section B.1.9).

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 the CS/1-A, CS/100-A, CS/200, and IVECS. Only some ports on other CS/1 types support this option; refer to the appropriate *Planning and 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 B.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 unit 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 both terminal and 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.

B.1.3 Asynchronous Session Transmission Parameters

Table B-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 B-4 Asynchronous Session Transmission Parameters

Parameter	*Permitted Values*
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>

* 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. Both a negative and a positive response will work, but no response at all will make 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 B.7.6 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 lower case 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 B.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 *Planning and Installation Guide* for the mapping between these lines and EIA connector pins, and to Section B.1.2 for a description of the UseDTRin parameter. This value must not be selected if UseDTRin is set to Ignore.

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 **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 COntrol; 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>.

B.1.4 Session Editing Parameters

Table B-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 B-5 Editing Parameters

Parameter	*Permitted Values*
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.

B.1.5 Global Parameters

Table B-6 lists the configuration parameters that determine the welcome message, date, prompts, passwords, and NCS audit trail functions. 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 B-6 Global Parameters

Parameter	*Permitted Values*
AUditServerAddr	<address>
BootServerAddr *	<address>
CONNectAudit	OFF | ON
DATE	<yy/mm/dd hh:mm[:ss]> <mm/dd/yy hh:mm[:ss]>
DOmain **	<string>
ERRorAudit	OFF | ON
GlobalPassWord	<string>
GroupxPasswd ***	<string>
LocalPassWord	<string>
NMPrompt	<string>
Organization **	<string>
PROMPt	<string>
WelcomeString	<string>

* Can be set with SET only, not SETDefault.
** 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. References [7] and [8] describe 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). References [7] and [8] describe 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). References [7] and [8] describe 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 B-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 **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, valid only on servers bound to an NCS, 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). References [7] and [8] describe 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 3.2. 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 **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 lower case followed by a crosshatch symbol (#) and a space. For example, on the CS/1, the default prompt is "cs/1# ".

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 **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 ^J". Reference [10] describes the conventions for entering string text.

B.1.6 Sample Asynchronous Configurations

This section contains examples of typical asynchronous port configurations and describes how configuration parameters interact with one another depending on the device type of the port and the nature of the application.

Tables B-7 through B-11 summarize some of the parameters that are critical to the ability of an asynchronous port to function as required by the application or by the connected device. The tables describe five types of applications:

Table B-7 Parameters for a terminal-to-host, line-oriented application (e.g., a user terminal interacting with a command interpreter or line-oriented editor)

Table B-8 Parameters for a terminal-to-host, screen-oriented application (e.g., a user terminal interacting with a screen-oriented editor)

Table B-9 Parameters for a host-to-host file transfer application

Table B-10 Parameters for a host-to-printer file transfer application

Table B-11 Parameters for ports to which dial-in or dial-out modems are attached

Table B-7 Configuration Parameters for Terminal-to-Host, Line-Oriented Applications

Parameter	*Terminal Port Setting*	*Host Port Setting*
DeVice	Terminal	Host
InterAction	Verbose, Echo	n/a
DataForward	ESC, CR, COntrol	None
IdleTimer	Disabled	1
MOde	Scroll	Transparent
ECHOData	ON	OFF
LFInsertion	OutputCrlf, EchoCrlf	n/a
BReakAction	EscDTM	IGnore
BReakChar	(1)	n/a
ECMChar	Disabled (2)	n/a
UseDCDout (3)	AlwaysAssert	OnConnection
UseDTRin (3)	AsDTR	AsDTR

(1) BReakChar is defined only if there is no break key on the terminal.

(2) An ECMChar may be preferable to a break signal if in-band breaks to the host are desired.

(3) See Sections B.1.2 and B.1.9 for more information.

Table B-8 Configuration Parameters for Terminal-to-Host, Screen-Oriented Applications

Parameter	*Terminal Port Setting*	*Host Port Setting*
DeVice	Terminal	Host
InterAction	Verbose, Echo	n/a
DataForward	None	None
IdleTimer	1	1
MOde	Transparent	Transparent
ECHOData	OFF	OFF
LFInsertion	None	n/a
BReakAction	InBand	IGnore
BReakChar	(1)	n/a
ECMChar	<CTRL-^>(2)	n/a
UseDCDout (3)	AlwaysAssert, NoToggle	OnConnection, ToggleonDisc
UseDTRin (3)	AsDTR	AsDTR

(1) BReakChar is defined only if there is no break key on the terminal.
(2) The ECMChar can be any control character not normally transmitted as data.
(3) See Sections B.1.2 and B.1.9 for more information.

Table B-9 Configuration Parameters for Host-to-Host File Transfer Applications

Parameter	*Initiating Host Port Setting*	*Destination Host Port Setting*
DeVice	Terminal (1)	Host
InterAction	Brief, NoEcho	n/a
DataForward	None	None
IdleTimer	60-255 (2)	1
MOde	Transparent	Transparent
ECHOData	OFF	OFF
LFInsertion	None	n/a
BReakAction	InBand	IGnore
BReakChar	(3)	n/a
ECMChar	<CTRL-^>(4)	n/a
UseDCDout (5)	OnConnection	OnConnection
UseDTRin (5)	AsDTR	AsDTR

(1) The initiating host must be configured as a terminal to initiate the connection, unless the network manager form of the Connect command is used to connect the two ports remotely.

(2) The IdleTimer setting is host-dependent.

(3) BReakChar is defined only if the initiating host cannot generate a break signal and needs to signal the other host.

(4) The ECMChar applies only to the initiating host, and can be any control character not normally transmitted. The host should be programmed to wait after issuing an ECMChar for the interval specified by the IdleTimer parameter before sending more characters.

(5) See Sections B.1.2 and B.1.9 for more information.

Table B-10 Configuration Parameters for Host-to-Printer File Transfer Applications

Parameter	*Host Port Setting*	*Printer Port Setting*
DeVice	Terminal (1)	Host
InterAction	Brief, NoEcho	n/a
DataForward	None	None
IdleTimer	60-255 (2)	1
MOde	Transparent	Transparent
ECHOData	OFF	OFF
LFInsertion	None	n/a
BReakAction	InBand	IGnore
BReakChar	Disabled	n/a
ECMChar	<CTRL-^> (3)	n/a
UseDCDout (4)	OnConnection	OnConnection
UseDTRin (4)	AsDTR	AsDTR

(1) The host port must be configured as a terminal to initiate the connection unless the network manager form of the Connect command is used to connect the two hosts remotely.

(2) The IdleTimer setting is host-dependent.

(3) The ECMChar applies only to the initiating host, and can be any control character not normally transmitted. The host should be programmed to wait after issuing an ECMChar for the interval specified by the IdleTimer parameter before sending more characters.

(4) See Sections B.1.2 and B.1.9 for more information.

Table B-11
Configuration Parameters for Modem Ports

Parameter	*Dial-in Modem Setting*	*Dial-out Modem Setting*
DeVice	Terminal	Host
InterAction	Verbose, Echo	n/a
DataForward	None	None
IdleTimer	1	1
MOde	Transparent	Transparent
ECHOData	Off	Off
LFInsertion	None	n/a
BReakAction	InBand	IGnore
BReakChar	(1)	n/a
ECMChar	(1)	n/a
BAud	(2)	(2)
UseDCDout (3)	AlwaysAssert, ToggleonDisc	OnConnection, ToggleonDisc
UseDTRin (3)	AsDTR	AsDCD

(1) BReakChar and ECMChar must be defined if the devices accessing the modem use them.
(2) Set to the same speed as the modem itself.
(3) See Sections B.1.2 and B.1.9 for more information.

B.1.7 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. Refer to Sections B.4 and B.6 for information on configuring the virtual ports on these systems.

On a new unit, some ports are configured for terminal device connections. That is, 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 port other than port 7:

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

Reference [10] describes the SETDefault command. Section B.1.1 describes 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).

B.1.8 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. Reference [10] describes the modes of operation and 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 LinePRotocol 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).

B.1.9 Asynchronous Modem Control Lines

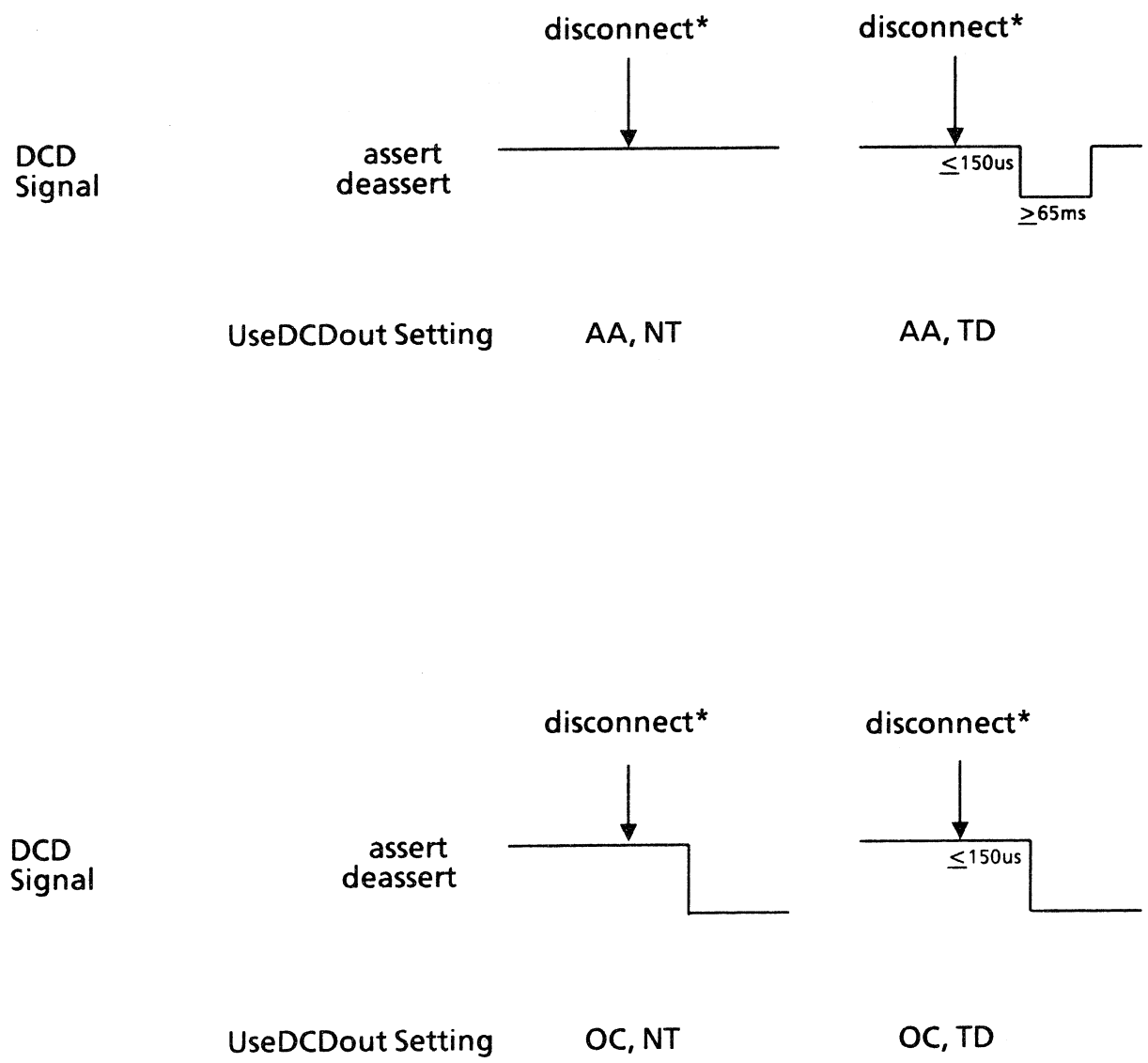
Table B-12 describes the interaction between the hardware modem control lines DTR and DCD and the software configuration parameters UseDTRin and UseDCDout. The information covers terminal ports, host ports, and modem ports, since these lines can be used by devices other than modems. Section B.1.2 describes the UseDTRin and UseDCDout parameters.

Some modems expect a toggle in the DCD signal at disconnect. Figure B-2 illustrates the effect of different UseDCDout parameter settings on the DCD signal at disconnect. Table B-12 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 *Planning and 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 B-2 Effect of UseDCDout Parameter Settings

Table B-12 Recommended Settings of UseDCDout and UseDTRin

Device Type	*UseDCDout Setting*	*UseDTRin Setting*
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

B.2 Character-Synchronous Configuration Parameters

This section describes the port parameters specific to character-synchronous devices.

Since the Connection Service commands are not available directly to a character-synchronous port, parameters for a character-synchronous port are set remotely from an asynchronous terminal port on a different Communications Server on the same Ethernet. On a hybrid CS/1 containing both character-synchronous and asynchronous boards, parameters for a character-synchronous port can be set from a port on an SIO-A board on the same CS/1.

Table B-13 is a summary of all character-synchronous port parameters, listed alphabetically. Upper case characters represent the minimum unambiguous abbreviation of each parameter. All character-synchronous port parameters must be set with the SETDefault command, except those indicated otherwise in the table below.

Table B-13 Character-Synchronous Port Configuration Parameter Summary

Parameter	*Section*	*Parameter*	*Section*
AccessGroup	B.2.1	InitMacro *	B.2.1
AccessWord	B.2.1	InterAction *	B.2.1
AUToDisconnect	B.2.1	INTerfaceType	B.2.2
BAud	B.2.2	LinePRotocol	B.2.2
BinaryData	B.2.2	MaxSessions *	B.2.1
BlockCheck	B.2.2	PARIty	B.2.2
BReakAction	B.2.3	PassCheck	B.2.2
BSCProtocol	B.2.2	PRIvilege *	B.2.1
BUffersize	B.2.1	RECvTimer	B.2.2
CarrierSense	B.2.2	RESpTimer	B.2.2
CharCode	B.2.2	SOH	B.2.2
DataBits	B.2.2	SYN	B.2.2
DeVice	B.2.1	SynCharCount	B.2.2
DLE	B.2.2	UseDSRout	B.2.2
DUplex	B.2.2	UseDTRin	B.2.2
FlowControlFrom	B.2.3	XmitTimer	B.2.2
FlowControlTo	B.2.3		

* May be displayed with SHow, but not set with SETD.

B.2.1 Character-Synchronous Port Transmission Parameters

The port transmission parameters for character-synchronous ports are identical to the port transmission parameters for asynchronous ports. These parameters are described in detail in Section B.1.1.

All character-synchronous port parameters must be specified with the SETDefault command, not the SET command.

B.2.2 Character-Synchronous Port Physical Parameters

This section describes the character-synchronous port physical parameters, usually set by the network manager for each port. The parameters and their possible values are listed in Table B-14.

Definitions of each parameter, explanations of each possible value, and an indication of the default follow the table. If the default value is appropriate, the parameter does not have to be set.

Table B-14 Character-Synchronous Port Physical Parameters

Parameter	*Permitted Values*
BAud	50 | 75 | 110 | 134.5 | 150 | 200 | 300 | 600 | 1200 | 1800 | 2400 | 3600 | 4800 | 7200 | 9600 | 19.2K | 38.4K * | 56K *
BinaryData	OFF | ON
BlockCheck	None | LRC | CRC16 | CCITT16
BSCProtocol	UTS | VIP | MODE4C | BASIC | 3270 | 3780 | HASP | FREE-FORM | SPECIAL
CarrierSense	OFF | ON
CharCode	ASCII | EBCDIC
DataBits	5 | 6 | 7 | 8
DeVice	(Host | Terminal , Paper | Glass)
DLE	<char>
DUplex	Full | Half | RecvOnly | XmitOnly
INTerfaceType	DCE | DTE
LinePRotocol	ASynchronous | BYTESynchronous | BITSynchronous
PARIty	None | Odd | Even
PassCheck	Pass | Strip
RECvTimer	Disabled | <number> (1-255 sixteenths of a second)
RESpTimer	Disabled | <number> (1-255 sixteenths of a second)
SOH	Include | Exclude
SYN	<char>
SyncCharCount	4 | 8 | 12 | 16
UseDSRout	(AlwaysAssert | OnConnection , NoToggle | ToggleonDisc)
UseDTRin	Ignore | AsDTR | AsDCD
XmitTimer	Disabled | <number> (1-255 sixteenths of a second)

* Applies to CS/1 only.

The **BAud** parameter determines the baud rate of the port and applies only if the SIO board is configured for internal clocks. The setting of this parameter is ignored if the SIO board is configured for external clocks. The maximum load per SIO board is two 56K half-duplex ports.

The **BinaryData** parameter specifies whether or not IBM transparent procedures for passing binary data are used. The default value is OFF. When the parameter is set to ON, so that the procedures are used, binary data transmission begins when a DLE.STX or DLE.SOH is detected, and continues until a DLE.ETX, DLE.ETB, or DLE.ITB is detected. A DLE.EOT or DLE.ENQ aborts the block. A DLE.DLE is treated as a binary number. The DLE character is excluded from block check calculations, except for the second DLE of a DLE.DLE sequence detected within binary transmission. When the value of the parameter is OFF, the DLE is included in the block check calculations. The BinaryData parameter should never be set to ON if PARIty is enabled.

The **BlockCheck** parameter specifies the kind of block check character that is generated following a block. The parameter can be set to one of four possible values:

None

Specifies that no block check character is generated or checked.

LRC

Specifies that the ANSI-standard Longitudinal Redundancy Check (LRC) is calculated and appended to the block. If the port is set up for EBCDIC encoding, the LRCs are 8 bits wide with no parity. If the port is set up for ASCII encoding, the LRCs are 7 bits wide, independent of parity. This value is usually appropriate if the ASCII character code is being used.

CRC16

Specifies that the block check character is generated using this polynomial:

$x^{16} + x^{15} + x^{2} + 1$

This value, the default, represents the standard IBM character-synchronous block check character. If this value is set, the DataBits parameter must be set to 8.

CCITT16

Specifies that the block check character is generated using this polynomial:

$x^{16} + x^{12} + x^{5} + 1$

If this value is set, the DataBits parameter must be set to 8.

The **BSCProtocol** parameter defines the control character conventions used at the datalink process. This parameter can be set to one of nine values:

UTS

For compatibility with Sperry character-synchronous Uniscope devices.

VIP

For compatibility with Honeywell character-synchronous VIP devices.

MODE4C

For compatibility with Control Data Corporation standard devices.

BASIC

For compatibility with Burroughs standard devices.

3270

For compatibility with IBM 3270 equipment. This is the default.

3780

For compatibility with IBM 3780 equipment.

HASP

For compatibility with IBM HASP equipment.

FREE-FORM

For use with custom applications. The datalink process monitors only SYN and line-marking characters. When the BSCProtocol parameter is set to FREE-FORM, the BlockCheck parameter must be set to None.

SPECIAL

For use with custom applications. The datalink process follows control character specifications supplied by the user (see the *Software Technical Reference Manual,* reference [2]).

The **CarrierSense** parameter determines whether or not the system uses carrier sensing before line turnaround. The possible values are OFF (the default) and ON. This parameter takes effect only if the port is operating in half-duplex mode, which is standard for character-synchronous communication.

On the CS/100, the effect of the CarrierSense parameter depends on the settings of the DUplex and INTerfaceType parameters. On the CS/1, the effect of the CarrierSense parameter depends both on the settings of the DUplex and INTerfaceType parameters and also on whether the device is connected to an SIO-SM (synchronous modem) or SIO-ST (synchronous terminal) board. Table B-15 shows the interaction among these parameters.

The **CharCode** parameter specifies how data is encoded. The possible values are EBCDIC (the default) and ASCII. The value EBCDIC may be set only if the BSCProtocol parameter is set to 3270, 3780, or HASP. The value ASCII may be set regardless of the BSCProtocol parameter setting.

The **DataBits** parameter specifies the number of databits per byte. The value may be set to 5, 6, 7, or 8. The default is 8.

The **DeVice** parameter specifies whether the device is a host or a terminal. This parameter is identical in function to the DeVice parameter for asynchronous devices; refer to Section B.1.1 for a complete description.

The **DLE** parameter specifies the Data Link Escape (DLE) character. The value can be entered as the numeric value of the DLE character or as a printing character representing the ASCII equivalent of the numeric value of the DLE character. The default (hexadecimal 10) is appropriate in almost all applications. The Communications Server always displays the value of this parameter as the printing character representing the ASCII equivalent of the parameter value. Hexadecimal 10 is displayed as "^P". Reference [10] describes the conventions for entering numbers.

The **DUplex** parameter specifies the type of physical interface provided by the SIO board for the port. If DUplex is set to Full, the SIO board provides a Bell 212-type interface. If DUplex is set to Half (the default), the SIO board provides a Bell 208-type interface. When the parameter is set to either RecvOnly or XmitOnly, the SIO board provides a one-way, Bell 208-type interface.

Table B-15 Interaction Among Carrier Sense, Duplex, and Interface Type Parameters

Case	*Carrier Sense*	*Duplex*	*Interface Type*	*Result*
1	ON	Full	DTE	The SIO firmware uses DCD to place the receiver in and out of hunt phase. DCD is on pin 8 on an SIO-SM board and on pin 20 on an SIO-ST board or a CS/100.
2	ON	Full	DCE	The SIO firmware uses RTS to place the receiver in and out of hunt phase. RTS is on pin 5 on an SIO-SM board and on pin 4 on an SIO-ST board or a CS/100.
3	ON	Half	DTE	The SIO firmware uses DCD to place the receiver in and out of hunt phase. DCD is also used to condition transmission; when DCD is true, transmission is inhibited. In this configuration, the DCE device must toggle DCD. DCD is on pin 8 on an SIO-SM board and on pin 20 on an SIO-ST board or a CS/100.
4	ON	Half	DCE	The SIO firmware uses RTS to place the receiver in and out of hunt phase. RTS is also used to condition transmission; when RTS is true, transmission is inhibited. In this configuration, the DCE device must toggle RTS. RTS is on pin 5 on a SIO-SM board and on pin 4 on an SIO-ST board or a CS/100.
5	OFF	Full	DTE	The SIO firmware ignores DCD. DCD is on pin 8 on an SIO-SM board and on pin 20 on an SIO-ST board or a CS/100.
6 *	OFF	Full	DCE	The SIO firmware ignores RTS. CTS is constant. RTS is on pin 5 on an SIO-SM board and on pin 4 on an SIO-ST board or a CS/100. CTS is on pin 4 on an SIO-SM board and on pin 5 on an SIO-ST board or a CS/100.
7	OFF	Half	DTE	RTS is toggled by the SIO firmware at line turn-around points and transmission waits for CTS. RTS is on pin 4 on an SIO-SM board and on pin 5 on an SIO-ST board or a CS/100.
8	OFF	Half	DCE	DCD is toggled by the SIO firmware at line turn-around points. RTS is on pin 20 on an SIO-SM board and on pin 8 on an SIO-ST board or a CS/100.

* On the CS/1-BSC, this combination is functionally the same as case 1.

The **INTerfaceType** parameter specifies whether the port is acting as a DCE or DTE device. If the parameter is set to DCE, the port sets the CTS signal, allowing transmission, whenever the RTS signal is asserted by the other end of the connection. The port transmits after asserting DCD, without waiting for a response. If the parameter is set to DTE, the port first asserts the RTS signal to the modem and then waits for assertion of the CTS signal from the modem before transmitting. The port begins receiving whenever the DCD signal from the modem is asserted. On the CS/100, the cable connectors are wired as DCE devices. Therefore, the RTS signal to the modem is sent from the CTS pin on the CS/100, the CTS signal from the modem is received at the RTS pin on the CS/100, and the DCD signal from the modem is received at the DTR pin on the CS/100. On a port connected to a terminal or host, this parameter should usually be set to DCE, the default. On a port connected to a modem, this parameter should usually be set to DTE.

The **LinePRotocol** parameter specifies whether asynchronous, character-synchronous, or bit-synchronous transmission is used. The Communications Server automatically sets the value at boot time to either ASynchronous or BYTESynchronous based on the SIO firmware present on the board and on the default value of the LinePRotocol parameter. If synchronous firmware is present, and the default LinePRotocol value is ASynchronous, the value is automatically changed to BYTESynchronous. The network manager should use the SETDefault command to set the value to BITSynchronous for operation with the SDLC pass-through service.

The **PARIty** parameter specifies the local device parity. The possible values are None, Odd, or Even. The default is None. If the BinaryData parameter is set to ON, the PARIty parameter must be set to None.

The **PassCheck** parameter determines how the Communications Server processes the block check character. When it receives a block from an attached device, the Communications Server generates its own block check character and compares it with the block check character received with the block. Whether or not an error is detected, the block is transmitted to the other end of the circuit. The PassCheck parameter determines whether the transmitted block carries the block check character. This parameter can be set to one of two values:

Pass

> Specifies that the block check character generated by the source device is transmitted over the network with the data block. This is the default value and the appropriate value for use with the pass-through service now available for character-synchronous communications.

Strip

> Specifies that the original block check character is stripped from the block before transmission over the network. When the block arrives at the destination Communications Server, the server regenerates the block check character before transmitting the block to the destination device.

The **RECvTimer** parameter sets the reception error recovery timer. This timer aborts block reception and generates a timeout error signal if a block's reception time exceeds the time specified by the parameter. The parameter can be set to Disabled, in which case the timer is always off, or to a number between 1 and 255, representing sixteenths of a second. The default value is 64.

The **RESpTimer** parameter sets the response timer. This timer generates a timeout error signal if the interval between the end of transmission from the Communications Server at one end of a circuit and the beginning of reception at the same server exceeds the setting of the timer. The parameter can be set to Disabled, in which case the timer is always off, or to a number between 1 and 255, representing sixteenths of a second. The RESpTimer parameter is not used by the current Connection Service software. The default value is Disabled.

The **SOH** parameter determines whether the first Start of Header (SOH) or Start of Text (STX) character is included in the block check character calculation. The parameter can be set to either:

Include

Specifies that the character is included in the calculation. This setting is required if the BSCProtocol parameter is set to MODE4C.

Exclude

Specifies that the first SOH or STX character is excluded from the calculation. This setting is the default and is appropriate for all BSCProtocol values except MODE4C.

The **SYN** parameter specifies the SYN character. The value can be entered as the numeric value of the SYN character or as the printing character representing the ASCII equivalent of the numeric value of the SYN character. The Communications Server always displays the value of this parameter as the printing character representing the ASCII equivalent of the parameter value. The default (hexadecimal 32) is usually appropriate if the CharCode parameter is set to EBCDIC. The hexadecimal value 16 is usually appropriate if the CharCode parameter is set to ASCII. The Communications Server displays hexadecimal 32 as "'2'" and displays hexadecimal 16 as "^V". Reference [10] describes the conventions for entering numbers.

The **SyncCharCount** parameter determines the number of SYN characters that precede each block transmitted. The possible value of this parameter is 4, 8, 12, or 16. The default value (4) is appropriate for most installations.

The **UseDSRout** parameter specifies how the Communications Server supplies the DTR signal to the attached device.

On the CS/1, the effect of this parameter varies depending on the interface hardware. On an SIO-ST board, UseDSRout has no effect. On an SIO-SM board, UseDSRout affects the DTR signal from the CS/1 to the modem.

On the CS/100, the effect of this parameter depends on the setting of the port's INTerfaceType parameter. If the INTerfaceType parameter is set to DCE, UseDSRout has no effect. If the INTerfaceType parameter is set to DTE, UseDSRout influences the DTR signal to the modem, which is the DCD signal from the CS/100. Refer to the appropriate *Planning and Installation Guide* for mapping between DSR, DTR, and the EIA connector pins.

One each from two sets of parameter values must be set:

AlwaysAssert | OnConnection

Determines when the DTR signal is asserted.

AlwaysAssert causes the signal to be asserted at all times.

OnConnection (the default) causes the signal to be deasserted as long as no connection is established to the device, and asserted when a connection is made.

NoToggle | ToggleonDisc

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

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

ToggleonDisc causes the signal to be deasserted for at least 200 milliseconds after disconnection. Depending on the other UseDSRout parameter setting, the signal then either changes to asserted or remains deasserted. This value is used when the Communications Server is connected to certain data switch devices.

The action of these parameter settings is illustrated in Figure B-3 in Section B.2.5. For recommended settings of this parameter for use with various devices, see Table B-26 in Section B.2.5.

The **UseDTRin** parameter specifies the response of the Communications Server to the value of the DTR or DSR signal received from the attached device. On the CS/1, the parameter affects system response to the DTR signal for ports on an SIO-ST board, and to the DSR signal for ports on an SIO-SM board. On the CS/100, the effect of the parameter depends on the setting of the INTerfaceType parameter. If INTerfaceType is set to DTE, the UseDTRin parameter has no effect. If INTerfaceType is set to DCE, the parameter affects system response to the DTR signal from the terminal, which is also the DTR signal to the CS/100. Refer to the appropriate *Planning and Installation Guide* for mapping between DSR, DTR, and the EIA connector pins.

For a third-party, pass-through connection or for a permanent virtual circuit, never set this parameter to any value but Ignore, the default. The Communications Server recognizes three possible values:

Ignore

Specifies that the Communications 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.

AsDTR

Specifies that the Communications Server checks the state of the DTR or DSR input signal before establishing a connection to a port. This value is not appropriate for the pass-through Connection Service currently available to character-synchronous ports.

AsDCD

Specifies that the Communications Server does not reject a connection request to the port based on the value of the DTR or DSR input. This value is not appropriate for the pass-through Connection Service currently available to character-synchronous ports.

The **XmitTimer** parameter sets the transmission error recovery timer. This timer aborts block transmission and generates a timeout error signal if the transmission time of a block exceeds the time specified by the XmitTimer parameter. The parameter can be set to Disabled, in which case the timer is always off, or to a number between 1 and 255, representing sixteenths of a second. The default value is 64.

B.2.3 Character-Synchronous Session Transmission Parameters

This section lists the session transmission characteristics for character-synchronous ports.

The parameters and their possible values are listed in Table B-16. Descriptions of each parameter, explanations of the possible values, and an indication of the default follow the table. If the default is acceptable, the parameter does not have to be set.

All character-synchronous port parameters must be specified from a remote port with the SETDefault command, not the SET command.

Table B-16 Character-Synchronous Session Transmission Parameters

Parameter	*Permitted Values*
BReakAction	IGnore | (OutofBand , FlushVC , InBand , EscDTM)
FlowControlFrom	None | CTS_RTS
FlowControlTo	None | CTS_RTS

The **BReakAction** parameter specifies the action taken by the Communications Server when a timeout error occurs. The timeout error can be generated by any one of three timers: the RECvTimer, the RESpTimer, or the XmitTimer. The value IGnore is mutually exclusive with any other value; more than one of the remaining values may be specified. The parameter has five possible values:

IGnore

Specifies no action. This is the default value.

OutofBand

Specifies that an out-of-band break is transmitted to the remote device when a timeout error occurs.

EscDTM

Specifies that the user port changes from Data Transfer mode to Command mode. This value is not currently implemented.

InBand

Specifies that an in-band break is transmitted to the remote device when a timeout error occurs.

FlushVC

Specifies that all packets for this session currently in the circuit are flushed. This value is not currently implemented.

The **FlowControlFrom** parameter specifies the flow control mechanism from the Communications Server to the local device. The Communications Server cannot interrupt transmission once it has started, but it can disallow transmission before it starts. The STX-ETX flow

control protocol established for synchronous transmission is always in effect, regardless of the setting of this parameter. On the CS/1, this parameter applies only to devices attached to an SIO-ST board. On the CS/100, this parameter applies only to ports on which the INTerfaceType parameter is set to DCE. The FlowControlFrom parameter accepts the same values as the FlowControlTo parameter, discussed below. The default value is None.

The **FlowControlTo** parameter specifies the flow control mechanism from the local device to the Communications Server. The local device cannot interrupt transmission once it has started, but it can disallow transmission before it starts. The STX-ETX flow control protocol established for synchronous transmission is always in effect, regardless of the setting of this parameter. On the CS/1, this parameter applies only to devices attached to an SIO-SM board. On the CS/100, this parameter applies only to ports on which the INTerfaceType parameter is set to DTE. The FlowControlTo parameter accepts one of two values:

None

Specifies that no flow control other than STX-ETX is used. This is the default value.

CTS_RTS

Specifies that the hardware control lines CTS and RTS are used. Refer to the appropriate *Planning and Installation Guide* for the mapping between these lines and EIA connector pins.

B.2.4 Sample Character-Synchronous Configurations

This section contains samples of typical port configurations for use with character-synchronous equipment.

Tables B-17 through B-25 summarize some of the parameter settings appropriate for ports connected to various kinds of equipment:

Table B-17 Parameters compatible with remote IBM 3274 equipment.

Table B-18 Parameters compatible with IBM 3780 equipment.

Table B-19 Parameters compatible with IBM HASP equipment.

Table B-20 Parameters compatible with IBM 3270 equipment using the ASCII character set.

Table B-21 Parameters compatible with Honeywell VIP equipment.

Table B-22 Parameters compatible with Sperry UTS equipment using the standard CS/1-BSC pass-through service. These parameters are not applicable if the connection uses the SPMUX multiplexer service.

Table B-23 Parameters compatible with Sperry UTS equipment using the SPMUX multiplexer service. These parameters are applicable for ports to which UTS terminals are attached and for ports to which a DCP host front-end processor is attached.

Table B-24 Parameters compatible with Control Data Corporation MODE4C equipment.

Table B-25 Parameters compatible with Burroughs BASIC equipment.

Table B-17 Configuration Parameters for Remote IBM 3274 Equipment

Parameter	*Setting*
DeVice	Host
BinaryData	OFF
BSCProtocol	3270
BlockCheck	CRC16
CarrierSense	OFF
CharCode	EBCDIC
DataBits	8
DLE	^P (1)
DUplex	Half (2)
INTerfaceType	DCE
PARIty	None
PassCheck	Pass
RECvTimer	64 (3)
RESpTimer	Disabled
SOH	Exclude
SYN	'2' (1)
SyncCharCount	4
UseDSRout	OnConnection, NoToggle (2)
UseDTRin	Ignore
XmitTimer	64 (3)
BReakAction	IGnore
FlowControlFrom	None (3)
FlowControlTo	None (3)

(1) The Connection Service always displays this value as the printing character that represents the ASCII equivalent of the numeric value of the setting.

(2) Varies in different installations.

(3) These settings will allow transmission. Depending on the device's timing characteristics, however, performance may improve with some alteration.

Table B-18 Configuration Parameters for IBM 3780 Equipment

Parameter	*Setting*
DeVice	Host
BinaryData	ON
BSCProtocol	3780
BlockCheck	CRC16
CarrierSense	OFF
CharCode	EBCDIC
DataBits	8
DLE	^P (1)
DUplex	Half (2)
INTerfaceType	DCE
PARIty	None
PassCheck	Pass
RECvTimer	64 (3)
RESpTimer	Disabled
SOH	Exclude
SYN	'2' (1)
SyncCharCount	4
UseDSRout	OnConnection, NoToggle (2)
UseDTRin	Ignore
XmitTimer	64 (3)
BReakAction	IGnore
FlowControlFrom	None (3)
FlowControlTo	None (3)

(1) The Connection Service always displays this value as the printing character that represents the ASCII equivalent of the numeric value of the setting.

(2) Varies in different installations.

(3) These settings will allow transmission. Depending on the device's timing characteristics, however, performance may improve with some alteration.

Table B-19 Configuration Parameters for IBM HASP Equipment

Parameter	*Setting*
DeVice	Host
BinaryData	ON
BSCProtocol	HASP
BlockCheck	CRC16
CarrierSense	OFF
CharCode	EBCDIC
DataBits	8
DLE	^P (1)
DUplex	Half (2)
INTerfaceType	DCE
PARIty	None
PassCheck	Pass
RECvTimer	64 (3)
RESpTimer	Disabled
SOH	Exclude
SYN	'2' (1)
SyncCharCount	4
UseDSRout	OnConnection, NoToggle (2)
UseDTRin	Ignore
XmitTimer	64 (3)
BReakAction	IGnore
FlowControlFrom	None (3)
FlowControlTo	None (3)

(1) The Connection Service always displays this value as the printing character that represents the ASCII equivalent of the numeric value of the setting.

(2) Varies in different installations.

(3) These settings will allow transmission. Depending on the device's timing characteristics, however, performance may improve with some alteration.

Table B-20 Configuration Parameters for IBM 3270 Equipment Using the ASCII Character Set

Parameter	*Setting*
DeVice	Host
BinaryData	OFF
BSCProtocol	3270
BlockCheck	LRC
CarrierSense	OFF
CharCode	ASCII
DataBits	8
DLE	^P (1)
DUplex	Half (2)
INTerfaceType	DCE
PARIty	None
PassCheck	Pass
RECvTimer	64 (3)
RESpTimer	Disabled
SOH	Exclude
SYN	^V (1)
SyncCharCount	4
UseDSRout	OnConnection, NoToggle (2)
UseDTRin	Ignore
XmitTimer	64 (3)
BReakAction	IGnore
FlowControlFrom	None (3)
FlowControlTo	None (3)

(1) The Connection Service always displays this value as the printing character that represents the ASCII equivalent of the numeric value of the setting.
(2) Varies in different installations.
(3) These settings will allow transmission. Depending on the device's timing characteristics, however, performance may improve with some alteration.

Table B-21 Configuration Parameters for Honeywell VIP Equipment

Parameter	*Setting*
DeVice	Host
BinaryData	OFF
BSCProtocol	VIP
BlockCheck	LRC
CarrierSense	OFF
CharCode	ASCII
DataBits	8
DLE	^P (1)
DUplex	Half (2)
INTerfaceType	DCE
PARIty	None
PassCheck	Pass
RECvTimer	64 (3)
RESpTimer	Disabled
SOH	Exclude
SYN	^V (1)
SyncCharCount	4
UseDSRout	OnConnection, NoToggle (2)
UseDTRin	Ignore
XmitTimer	64 (3)
BReakAction	IGnore
FlowControlFrom	None (3)
FlowControlTo	None (3)

(1) The Connection Service always displays this value as the printing character that represents the ASCII equivalent of the numeric value of the setting.

(2) Varies in different installations.

(3) These settings will allow transmission. Depending on the device's timing characteristics, however, performance may improve with some alteration.

Table B-22 Configuration Parameters for Sperry UTS Equipment in a Non-SPMUX Environment

Parameter	*Setting*
DeVice	Host
BinaryData	OFF
BSCProtocol	UTS
BlockCheck	LRC
CarrierSense	OFF
CharCode	ASCII
DataBits	8
DLE	^P (1)
DUplex	Half (2)
INTerfaceType	DCE
PARIty	None
PassCheck	Pass
RECvTimer	64 (3)
RESpTimer	Disabled
SOH	Exclude
SYN	^V (1)
SyncCharCount	4
UseDSRout	OnConnection, NoToggle (2)
UseDTRin	Ignore
XmitTimer	64 (3)
BReakAction	IGnore
FlowControlFrom	None (3)
FlowControlTo	None (3)

(1) The Connection Service always displays this value as the printing character that represents the ASCII equivalent of the numeric value of the setting.
(2) Varies in different installations.
(3) These settings will allow transmission. Depending on the device's timing characteristics, however, performance may improve with some alteration.

Table B-23 Configuration Parameters for Sperry UTS Equipment in an SPMUX Environment

Parameter	*Setting*
DeVice	Host
BinaryData	OFF
BSCProtocol	UTS
BlockCheck	LRC
CarrierSense	ON
CharCode	ASCII
DataBits	8
DLE	^P (1)
DUplex	Half (2)
INTerfaceType	DCE
PARIty	None
PassCheck	Pass
RECvTimer	64 (3)
RESpTimer	Disabled
SOH	Exclude
SYN	^V (1)
SyncCharCount	4
UseDSRout	OnConnection, NoToggle (2)
UseDTRin	AsDTR
XmitTimer	64 (3)
BReakAction	IGnore
FlowControlFrom	None (3)
FlowControlTo	None (3)

(1) The Connection Service always displays this value as the printing character that represents the ASCII equivalent of the numeric value of the setting.

(2) Varies in different installations.

(3) These settings will allow transmission. Depending on the device's timing characteristics, however, performance may improve with some alteration.

Table B-24 Configuration Parameters for Control Data Corporation MODE4C Equipment

Parameter	*Setting*
DeVice	Host
BinaryData	OFF
BSCProtocol	MODE4C
BlockCheck	LRC
CarrierSense	OFF
CharCode	ASCII
DataBits	8
DLE	^P (1)
DUplex	Half (2)
INTerfaceType	DCE
PARIty	None
PassCheck	Pass
RECvTimer	64 (3)
RESpTimer	Disabled
SOH	Exclude
SYN	^V (1)
SyncCharCount	4
UseDSRout	OnConnection, NoToggle (2)
UseDTRin	Ignore
XmitTimer	4 (3)
BReakAction	IGnore
FlowControlFrom	None (3)
FlowControlTo	None (3)

(1) The Connection Service always displays this value as the printing character that represents the ASCII equivalent of the numeric value of the setting.

(2) Varies in different installations.

(3) These settings will allow transmission. Depending on the device's timing characteristics, however, performance may improve with some alteration.

Table B-25 Configuration Parameters for Burroughs BASIC Equipment

Parameter	*Setting*
DeVice	Host
BinaryData	OFF
BSCProtocol	BASIC
BlockCheck	LRC
CarrierSense	OFF
CharCode	ASCII
DataBits	8
DLE	^P (1)
DUplex	Half (2)
INTerfaceType	DCE
PARIty	None
PassCheck	Pass
RECvTimer	64 (3)
RESpTimer	Disabled
SOH	Exclude
SYN	^V (1)
SyncCharCount	4
UseDSRout	OnConnection, NoToggle (2)
UseDTRin	Ignore
XmitTimer	64 (3)
BReakAction	IGnore
FlowControlFrom	None (3)
FlowControlTo	None (3)

(1) The Connection Service always displays this value as the printing character that represents the ASCII equivalent of the numeric value of the setting.

(2) Varies in different installations.

(3) These settings will allow transmission. In some installations, however, system performance may improve with some alteration.

B.2.5 Character-Synchronous Handshake Control Lines

This section describes the effects of configuration parameters on handshake control lines.

The effect of some parameters depends on whether the port is functioning as a DTE or as a DCE. For the CS/100, this is determined by the setting of the port's INTerfaceType parameter; for the CS/1, this is determined both by the INTerfaceType parameter and by the SIO board type.

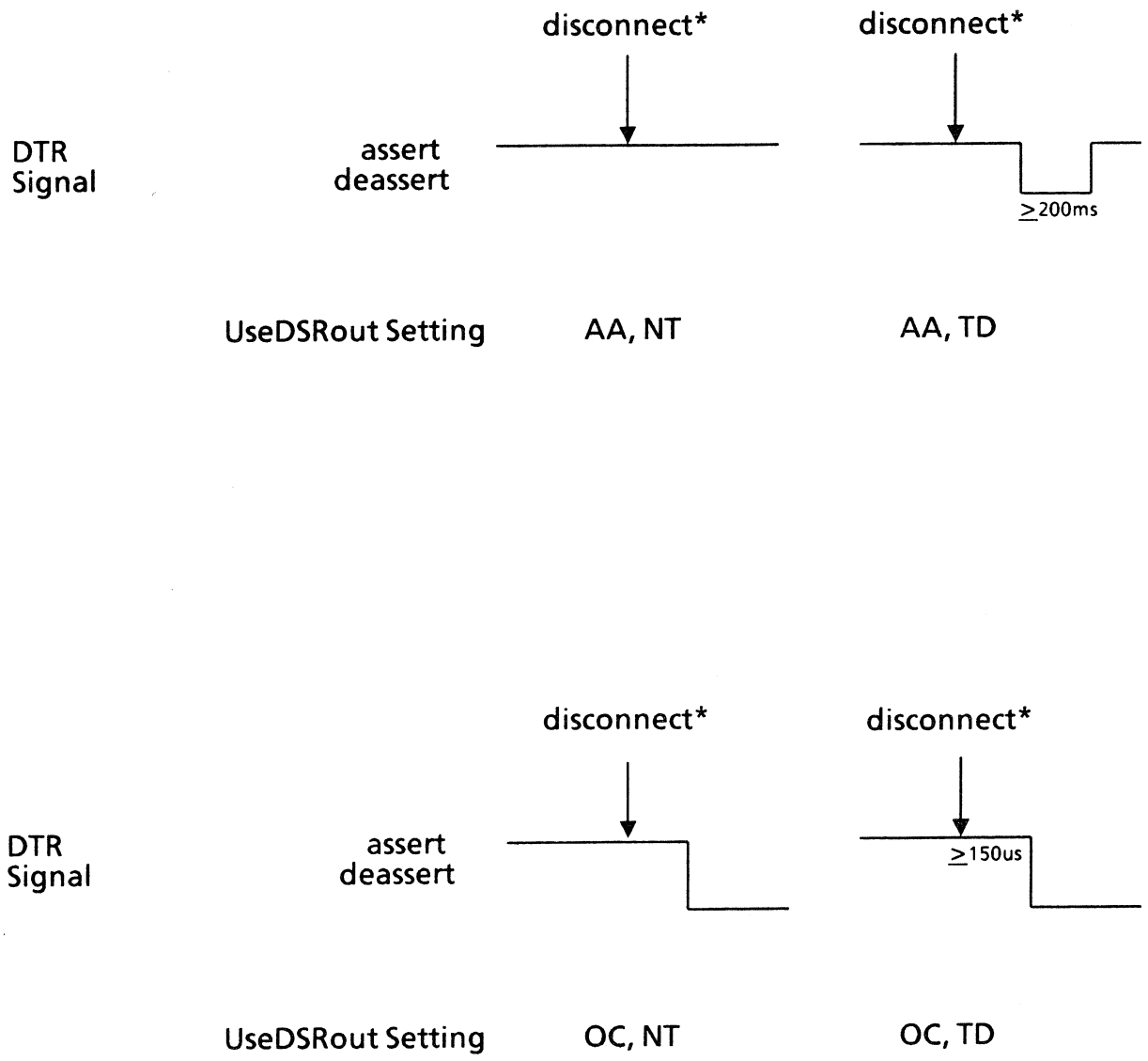
Table B-26 summarizes the differences. The signal names in the table are relative to the modem.

Table B-26 Effect of Parameters Dependent on Board Type and on Interface Type Parameter Setting

Parameter	*SIO-SM DTE Port*	*SIO-SM DCE Port*	*CS/100 * DTE Port*	*CS/100 * or SIO-ST DCE Port*
CarrierSense	sense DCD set RTS	sense RTS set DCD	sense DCD set RTS	sense RTS set DCD
UseDSRout	DTR	DSR	DTR	no effect
UseDTRin	DSR	DTR	no effect	DTR
FlowCtlFrom	not used	used	not used	used
FlowCtlTo	used	not used	used	not used

* The DCD signal from the modem is delivered to the DTR pin on the CS/100; the RTS signal to the modem is delivered from the CTS pin on the CS/100; and the DTR signal to the modem is delivered from the DCD pin on the CS/100.

Figure B-3 illustrates the effect of the different UseDSRout parameter settings on the DTR signal. This parameter has no effect on a port on an SIO-ST board or a CS/100 port configured as a DCE device.



* The disconnect must come from a remote port.

Figure B-3 Effect of UseDSRout Parameter Settings

Table B-27 illustrates the recommended settings of the UseDSRout parameter for use with different kinds of modems. This table assumes that the modem is connected to a port on an SIO-SM board or a CS/100 port configured as a DTE device. For the third-party, pass-through Connection Service currently available for synchronous transmission, always set the UseDTRin parameter to Ignore.

Table B-27
Recommended Settings of UseDSRout

Device Type	*UseDSRout Setting*
Dial-in modem without unattended disconnect	AlwaysAssert, NoToggle
Dial-out modem without unattended disconnect	OnConnection, NoToggle
Dial-in modem with unattended disconnect	AlwaysAssert, ToggleonDisc
Dial-out modem with unattended disconnect	OnConnection, ToggleonDisc

B.3 Bit-Synchronous Configuration Parameters

This section describes the port parameters specific to bit-synchronous transmission. The parameters are appropriate for ports on a CS/1-SDLC.

Since the Connection Service commands are not available directly to a bit-synchronous port, parameters for the port are set remotely from an asynchronous terminal port on a different Communications Server on the Ethernet. On a hybrid CS/1 containing both bit-synchronous and asynchronous boards, parameters for a bit-synchronous port can be set from a port on an SIO-A board on the same CS/1.

The default parameter tables shipped with both character-synchronous and bit-synchronous systems include character-synchronous parameters only. In these parameter tables, the LinePRotocol parameter is settable to either BYTESynchronous or BITSynchronous. Before any other bit-synchronous parameters can be displayed or altered, the LinePRotocol parameter must be set to BITSynchronous. After this value is specified, the SHow DefaultParameters command displays the bit-synchronous parameter list, and the SETDefault command can be used to alter bit-synchronous parameter values.

All bit-synchronous port parameters must be set with the SETDefault command, except those indicated otherwise in the table below. Table B-28 is a summary of all bit-synchronous parameters, listed alphabetically. Upper case characters represent the minimum unambiguous abbreviation of each parameter.

Table B-28
Bit-Synchronous Port Parameter Summary

Parameter	*Section*	*Parameter*	*Section*
AccessGroup	B.3.1	InitMacro *	B.3.1
AccessWord	B.3.1	InterAction *	B.3.1
AddressFilter	B.3.2	INTerfaceType	B.3.2
AUToDisconnect	B.3.1	LinePRotocol	B.3.2
BAud	B.3.2	MaxSessions *	B.3.1
BReakAction	B.3.3	PRIvilege *	B.3.1
BUffersize	B.3.1	RECvTimer	B.3.2
CarrierSense	B.3.2	RESpTimer	B.3.2
DUplex	B.3.2	UseDSRout	B.3.2
FlowControlFrom	B.3.3	UseDTRin	B.3.2
FlowControlTo	B.3.3	XmitTimer	B.3.2
IdleState	B.3.2		

* May be displayed with SHow, but not set with SETD.

B.3.1 Bit-Synchronous Port Transmission Parameters

The port transmission parameters for bit-synchronous ports are identical to the port transmission parameters for asynchronous ports. These parameters are described in detail in Section B.1.1.

All settable bit-synchronous port parameters must be specified with the SETDefault command, not the SET command.

B.3.2 Bit-Synchronous Port Physical Parameters

This section describes the bit-synchronous port physical parameters, usually set by the network manager for each port. The parameters and their possible values are listed in Table B-29.

Definitions of each parameter, explanations of each possible value, and an indication of the default follow the table. If the default value is appropriate, the parameter does not have to be set.

Table B-29 Bit-Synchronous Port Physical Parameters

Parameter	*Permitted Values*
AddressFilter	Disabled | <number> (0-254)
BAud	50 | 75 | 110 | 134.5 | 150 | 200 | 300 | 600 | 1200 | 1800 | 2400 | 3600 | 4800 | 7200 | 9600 | 19.2K | 38.4K | 56K | 64K
CarrierSense	OFF | ON
DUplex	Half | Full | XmitOnly | RecvOnly
IdleState	LineMark | SyncBytes
INTerfaceType	DCE | DTE
LinePRotocol	ASynchronous | BYTESynchronous | BITSynchronous
RECvTimer	Disabled | <number> (1-255 sixteenths of a second)
RESpTimer	Disabled | <number> (1-255 sixteenths of a second)
UseDSRout	(AlwaysAssert | OnConnection , NoToggle | ToggleonDisc)
UseDTRin	Ignore | AsDTR | AsDCD
XmitTimer	Disabled | <number> (1-255 sixteenths of a second)

The **AddressFilter** parameter determines the SDLC address. Only frames with the specified address or the broadcast address will be received. Setting the AddressFilter parameter to Disabled allows reception of all frames presented to the bit-synchronous interface.

The **BAud** parameter determines the baud rate of the port. If the SIO board is configured for external clocks, the setting of this parameter is ignored. If the SIO board is configured for internal clocks, the setting of this parameter determines the port's baud rate. The maximum load per SIO board is one 64K full-duplex port and one 9600 baud full-duplex port.

The **CarrierSense** parameter determines whether or not the system uses carrier sensing before line turnaround. The effect of this parameter depends on the settings of the DUplex and INTerfaceType parameters (see Table B-15 in Section B.2.2).

The **DUplex** parameter specifies the type of physical interface provided by the SIO board for the port. If DUplex is set to Full, the SIO board provides a Bell 212-type interface. If Duplex is set to Half, the SIO board provides a Bell 208-type interface. When the parameter is set to either XmitOnly or RecvOnly, the SIO board provides a one-way, Bell 208-type interface.

The **IdleState** parameter determines whether the quiescent state of the line is mark (HDLC/SDLC Abort) or synchronization (x'7e'). If the parameter is set to LineMark, the line returns to marking when the final frame is sent. If the parameter is set to SyncBytes, the line sends flag bytes between frames until CTS becomes false.

The **INTerfaceType** parameter specifies whether the port is acting as a DCE or DTE device. Section B.2.2 describes the INTerfaceType parameter.

The **LinePRotocol** parameter specifies whether bit-synchronous or character-synchronous transmission is used. The Communications Server automatically sets the value at boot time based on the SIO firmware present on the board and on the default value of the LinePRotocol parameter. If synchronous firmware is present, and the default LinePRotocol value is ASynchronous, the value is automatically changed to BYTESynchronous. For use with the SDLC pass-through service, this parameter must be set to BITSynchronous with the SETDefault command.

The **RECvTimer** parameter sets the reception error recovery timer. Section B.2.2 describes the RECvTimer parameter.

The **RESpTimer** parameter is currently not used by the CS/1-SDLC, and the setting of the parameter is ignored by the system.

The **UseDSRout** and **UseDTRin** parameters for bit-synchronous operation are identical to the same parameters for character-synchronous operation. Section B.2.2 describes these parameters.

The **XmitTimer** parameter sets the transmission error recovery timer. Section B.2.2 describes the XmitTimer parameter.

B.3.3 Bit-Synchronous Session Transmission Parameters

The session transmission parameters for bit-synchronous ports are identical to the session transmission parameters for character-synchronous ports. These parameters are described in Section B.2.3.

All settable bit-synchronous port parameters must be specified with the SETDefault command, not the SET command.

B.3.4 Sample Bit-Synchronous Configurations

This section contains samples of typical port configurations for use with various kinds of lines used with the CS/1-SDLC in the SDLC pass-through service:

Table B-30 Parameters compatible with switched lines

Table B-31 Parameters compatible with leased lines

Table B-32 Parameters compatible with directly connected lines

Table B-30 Configuration Parameters for SDLC Switched Lines

Parameter	*Setting*
AddressFilter	Disabled
AUToDisconnect	(1)
DeVice	Host
CarrierSense	ON
DUplex	Half
IdleState	LineMark
INTerfaceType	DTE
LinePRotocol	BITSynchronous
RECvTimer	64 (2)
RESpTimer	Disabled
UseDSRout	AlwaysAssert, ToggleonDisc (3)
UseDTRin	Ignore
XmitTimer	64 (2)
BReakAction	IGnore
FlowControlFrom	None (2)
FlowControlTo	None (2)

(1) User-selectable.
(2) These settings will allow transmission. In some installations, however, system performance may improve with some alteration.
(3) Varies in different installations.

Table B-31 Configuration Parameters for SDLC Leased Lines

Parameter	*Setting*
AddressFilter	Disabled
AUToDisconnect	Disabled
DeVice	Host
CarrierSense	OFF
DUplex	Full
IdleState	LineMark
INTerfaceType	DTE
LinePRotocol	BITSynchronous
RECvTimer	64 (1)
RESpTimer	Disabled
UseDSRout	AlwaysAssert, NoToggle (2)
UseDTRin	Ignore
XmitTimer	64 (1)
BReakAction	IGnore
FlowControlFrom	None (1)
FlowControlTo	None (1)

(1) These settings will allow transmission. In some installations, however, system performance may improve with some alteration.

(2) Varies in different installations.

Table B-32 Configuration Parameters for SDLC Directly Connected Lines

Parameter	*Setting*
AddressFilter	Disabled
AUToDisconnect	Disabled
DeVice	Host
CarrierSense	OFF
DUplex	Full
IdleState	LineMark
INTerfaceType	DCE
LinePRotocol	BITSynchronous
RECvTimer	64 (1)
RESpTimer	Disabled
UseDSRout	OnConnection, NoToggle (2)
UseDTRin	Ignore
XmitTimer	64 (1)
BReakAction	IGnore
FlowControlFrom	None (1)
FlowControlTo	None (1)

(1) These settings will allow transmission. In some installations, however, system performance may improve with some alteration.
(2) Varies in different installations.

B.3.5 Bit-Synchronous Handshake Control Lines

The effect of the settings of configuration parameters on the operation of handshake control lines is the same for bit-synchronous systems as for character-synchronous systems. Section B.2.5 describes the effect of configuration parameters on handshake control lines.

B.4 CS/1-X.25 Configuration Parameters

The CS/1-X.25 provides the Connection Service via virtual ports rather than physical ports. These virtual ports support a subset of the port configuration parameters described in Section B.1. Table B-33 lists the parameters that apply to the CS/1-X.25 and indicates the section in which each parameter is described.

All the parameters listed may be set remotely by the network manager using the SETDefault command, although any parameters that correspond to X.3 parameters may be reset interactively by the host.

Table B-33 CS/1-X.25 Port Configuration Parameters

Parameter	*Section*	*Parameter*	*Section*
AccessGroup	B.1.1	GlobalPassWord	B.1.5
AccessWord	B.1.1	GroupxPasswd	B.1.5
AUToDisconnect	B.1.1	IdleTimer	B.1.3
BReakAction	B.1.3	InitMacro	B.1.1
BReakChar	B.1.3	InterAction	B.1.1
CRPad	B.1.2	LFInsertion	B.1.3
DataBits	B.1.2	LineERase	B.1.4
DataForward	B.1.3	LocalEDiting	B.1.4
DATE	B.1.5	LocalPassWord	B.1.5
DeVice	B.1.1	MaxSessions	B.1.1
DOmain	B.1.5	MOde	B.1.3
ECHOData	B.1.3	NMPrompt	B.1.5
ECHOMask	B.1.3	Organization	B.1.5
ECMChar	B.1.3	PRIvilege	B.1.1
EOM	B.1.3	ReprintLine	B.1.4
ERase	B.1.4	VERBatim	B.1.4
FlowControlFrom	B.1.3	WelcomeString	B.1.5
FlowControlTo	B.1.3	WordERase	B.1.4

B.5 Configuration Parameters for the IVECS

The IVECS requires only minimal port configuration. Because each IVECS virtual port does not represent a single connector and physical line, most of the port parameters described in the previous sections are not applicable.

The IVECS uses nine configuration parameters:

AccessGroup
AUToDisconnect
BReakAction
FlowControlFrom
FlowControlTo
IdleTimer
PermanentVC
UseDCDout
UseDTRin

The **PermanentVC** parameter specifies a permanent virtual circuit from the current or specified port to the specified address or clearinghouse name. Permitted values are:

"" | "<address>"

To disable a permanent virtual circuit, set the parameter equal to null ("").

The other IVECS parameters are described in Section B.1. Additional parameters appear in the "SHow DefaultParameters" display for the IVECS, but only the parameters listed above may be changed.

All of the parameters in this section must be set remotely by the network manager from an asynchronous terminal port on a CS/1-A, CS/100-A, or CS/200.

B.6 Configuration Parameters for Other Communications Servers

Most servers that provide the Connection Service via virtual ports rather than physical ports require only minimal port configuration. Because a virtual port does not represent a single connector and physical line, most of the port parameters described in the previous sections are not applicable.

The CS/1-HSM, the CS/1-SNA, and the CS/100-488 use only four configuration parameters:

AccessGroup
AccessWord
AUToDisconnect
GroupxPasswd

Section B.1 describes these parameters.

All of the parameters in this section must be set remotely by the network manager from an asynchronous terminal port on a CS/1-A, CS/100-A, or CS/200.

B.7 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. These parameters apply only to the GS/1 Connection Service, and only to virtual ports accessed by a user dialing into the GS/1 from a PAD on an X.25 network. The Global Parameters described in Section B.7.5 apply to the GS/1 as a whole.

Table B-34 lists all virtual port parameters for the Gateway Server/1 alphabetically and gives the section number of each parameter description. Upper case 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 B-34 GS/1 Configuration Parameter Summary

Parameter	*Section*	*Parameter*	*Section*
AccessGroup	B.7.1	GroupxPasswd	B.7.5
AccessWord	B.7.1	IdleTimer	B.7.3
AUtodisconnect	B.7.1	InitMacro	B.7.1
BReakAction	B.7.3	InterAction	B.7.1
BReakChar	B.7.3	LFInsertion	B.7.3
CRPad	B.7.2	LineERase	B.7.4
DataBits	B.7.2	LocalEDiting	B.7.4
DataForward	B.7.3	LocalPassWord	B.7.5
DATE	B.7.5	MaxSessions	B.7.1
DeVice	B.7.1	MOde	B.7.3
DOmain	B.7.5	NMPrompt	B.7.5
ECHOData	B.7.3	Organization	B.7.5
ECMChar	B.7.3	PRIvilege	B.7.1
EOM	B.7.3	PROMPT	B.7.5
ERase	B.7.4	ReprintLine	B.7.4
FlowControlFrom	B.7.3	VERBatim	B.7.4
FlowControlTo	B.7.3	WelcomeString	B.7.5
GlobalPassWord	B.7.5	WordERase	B.7.4

B.7.1 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 B-35.

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 B-35 GS/1 Port Transmission Parameters

Parameter	*Permitted Values*
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)
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 3.2. 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 B.7.5 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 cannot be set to Host 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 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 and the DEFine command are described in reference [10].

**** 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. Reference [10] 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.

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 (reference [10] 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.

B.7.2 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 B-36.

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 B-36
GS/1 Port Physical Parameters

Parameter	*Permitted Values*
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.

B.7.3 GS/1 Session Transmission Parameters

Table B-37 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 B-37 GS/1 Session Transmission Parameters

Parameter	*Permitted Values*
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 **BReakChar** 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 lower case 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 B.7.4 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.

B.7.4 GS/1 Session Editing Parameters

Table B-38 summarizes the session editing parameters, which can be used in Command mode and in Data Transfer mode during sessions in which the MOde 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 B-38
GS/1 Session Editing Parameters

Parameter	*Permitted Values*
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 MOde 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.

B.7.5 GS/1 Global Parameters

Table B-39 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 B-39 GS/1 Global Parameters

Parameter	*Permitted Values*
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 B-39. 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. 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".

B.7.6 Bridge Implementation of X.3 Protocol

This section describes the Bridge implementation of the X.3 protocol. Table B-40 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 B-40 Bridge-to-X.3 Parameter Conversions

Parameter No.	*Bridge Name/Values*	*X.3 Name/Values*	*Conversion*
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 B-40 Bridge-to-X.3 Parameter Conversions (continued)

Parameter No.	*Bridge Name/Values*	*X.3 Name/Values*	*Conversion*
6	InterAction 0 = Verbose 1 = Brief 4 = NoEcho 8 = Completion 16 = NoMacroEcho 32 = Linefeed 64 = Broadcast off	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 B-40 Bridge-to-X.3 Parameter Conversions (continued)

Parameter No.	*Bridge Name/Values*	*X.3 Name/Values*	*Conversion*
11	BaudRate	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 B-40 Bridge-to-X.3 Parameter Conversions (continued)

Parameter No.	*Bridge Name/Values*	*X.3 Name/Values*	*Conversion*
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 C

DISK UTILITIES

This appendix describes the disk utilities of the Series/1 and Series/100 servers.

Appendix D describes error messages that may occur while performing the procedures described in this section.

C.1 Series/1 Disk Utilities

This section describes the Series/1 disk copying, disk formatting, and memory dump procedures. The equivalent functions for the Series/100 are described in Section C.2.

The procedures are executed from the MCPU monitor, via the system console terminal. For the procedure for accessing the monitor, refer to the description of bootstrap sequences in the *Series/1 Planning and Installation Guide* (reference [3]).

The console terminal must be an asynchronous, non-block-mode terminal, configured for 8 databits per byte and no parity. The default baud rate of the console port is 9600 baud; other baud rates are selectable via hardware jumper on the MCPU board. Reference [3] describes altering the console port baud rate.

C.1.1 Backing Up the System Diskette

This procedure applies only to a Series/1 server that boots from an internal disk drive. For a server that boots from an NCS, the equivalent procedure is performed on the NCS. Refer to the appropriate *NCS Installation and Operation Guide* for more information.

After adjusting and saving system generation parameters and completing any port configuration necessary to establish the appropriate configuration tables, the network manager should make a backup copy of the system diskette.

The Copy command can be executed only immediately after a power-on, reset, or system generation procedure. If communication software has been running prior to the execution of the Copy command, the server must be rebooted into the monitor. Refer to the bootstrap sequences described in reference [3].

For systems with MCPU PROMs designated Release 9 or earlier, the Copy command is stored on the system diskette; the diskette must be in place in the disk drive when the command is executed. For systems with MCPU PROMs designated M1 MMON 01B or later, the command is PROM-based and the system diskette need not be in place when the command is executed.

To create one or more copies of the system diskette, enter the Copy command (co) followed by the number of copies desired. For example, to request two copies, enter:

```
co 2
```

The monitor prompts the user to place the source diskette in the disk drive and press the return key. Next, the monitor prompts the user to place the destination diskette in the drive

and press the return key again. Repeat this procedure as many times as specified in the Copy command line.

The destination diskette may be unformatted; the Copy command automatically formats it.

C.1.2 Installing a Software Update

This section describes the procedure for installing a new software release on a Communications Server that is already configured and in place on the network.

This procedure applies only to a Series/1 server that boots from an internal disk drive. For a server that boots from an NCS, the equivalent procedure is performed on the NCS. Refer to the appropriate *NCS Installation and Operation Guide* for more information.

The general procedure for installing a software update is to replace only the communications software on the diskette, leaving all port configuration tables undisturbed. The exact procedure varies, depending on the sizes of the old and new software releases.

Some new software releases may be incompatible in terms of code size with prior releases, making it impossible to install a software update and preserve all configuration information. In some cases, the existing configuration information may be obsolete, and an installation that preserves all configuration information is unnecessary.

Review the needs of the local installation and refer to the release memo that accompanies the new release to determine which installation procedure to use:

- If the existing configuration information is to be retained, and if the new release is size-compatible with the old release, use the procedure described in this section.
- If the configuration information is not going to be retained, or if the two releases are not size-compatible, use the procedure outlined in the previous section for copying the entire diskette. Then complete the installation by performing the system generation and port configuration procedures.

If the release memo accompanying the software distribution diskette contains different instructions for installing the new software, follow those instructions instead of the procedure described here.

The software update installation procedure is performed using the Copy command. The procedure varies depending on the version of the MCPU PROM installed in the server.

MCPU PROM Release 9 or Earlier

To install a software update on a system with an MCPU PROM designated Release 9 or earlier, enter the Copy command with the partial option (-p), followed by the number of copies desired. For example, to make two updated diskettes, enter the command:

```
co -p 2
```

The monitor prompts for the starting block number and then for the ending block number of the range to be copied. The starting and ending block numbers may vary with each software release; refer to the release memo that accompanied the software distribution diskette.

Next, the monitor prompts the user to insert the source diskette in the disk drive and then to insert the destination diskette in the disk drive. Repeat this step as many times as specified in the command line.

MCPU PROM Release M1 MMON 01B or Later

To install a software update on a system with an MCPU PROM designated M1 MMON 01B or later, enter the Copy command with the partial option (p), followed by the starting and ending block numbers:

```
co p <starting block> <ending block>
```

The starting and ending block numbers vary with each software release; refer to the release memo that accompanied the software distribution diskette for these numbers.

For example, to copy the range of blocks from 200 through 220, enter the command:

```
co p 200 220
```

The monitor prompts the user to insert the source diskette in the disk drive and then to insert the destination diskette in the disk drive.

With these PROMs, multiple copies may not be specified in the command line. To update multiple diskettes, repeat the procedure once for each copy.

C.1.3 Formatting a Diskette

This section describes the procedure for formatting a blank diskette for use on a Communications Server; it applies only to a server with an internal disk drive.

During normal use, only the system diskette supplied by Bridge is needed. However, the network manager may want to keep two blank, formatted diskettes available in case a memory dump is necessary to help diagnose a system failure. The procedure for obtaining a memory dump is described in Section C.1.4.

**** NOTES ****

On a Series/1 server with MCPU PROMs designated M1 MMON 01C or later, the memory dump procedure automatically formats the diskette, so the network manager need not preformat the diskette.

If a diskette is intended to hold communications software, formatting is not normally required, since the Copy command automatically formats the diskette. Format the diskette only if specifically instructed to do so by a Bridge service representative.

The procedure varies depending on the revision level of the MCPU PROMs present in the system.

MCPU PROM Release 9 or Earlier

For systems with MCPU PROMs designated Release 9 or earlier, enter the following command to format both sides of the diskette currently in the disk drive:

```
fo
```

**** CAUTION ****

Ensure that the appropriate diskette is in the disk drive before terminating the command with the return key. After the return key is pressed, the system immediately formats whichever diskette is present, thus erasing all information previously on the diskette.

MCPU PROM Release M1 MMON 01B or Later

For systems with MCPU PROMs designated M1 MMON 01B or later, enter the following command to format both sides of the diskette currently in the disk drive:

```
fo <density>
```

**** CAUTION ****

Ensure that the appropriate diskette is in the disk drive before terminating the command with the return key. After the return key is pressed, the system immediately formats whichever diskette is present, thus erasing all information previously on the diskette.

For a diskette intended to hold a memory dump, specify 8 sectors per track for all Series/1 server models.

For a diskette intended to hold communications software, specify 8 sectors per track for all Series/1 servers except the CS/1-SNA, and 9 sectors per track for the CS/1-SNA only.

**** NOTE ****

If a diskette is intended to hold communications software, formatting is not normally required, since the Copy command automatically formats the diskette. Format the diskette only if specifically instructed to do so by a Bridge service representative.

If the command line does not specify a density, the system returns an error message and aborts the command.

C.1.4 Obtaining a Memory Dump

This procedure is used on the Series/1 server to write the contents of the MCPU RAM and the ESB RAM onto diskettes following a system crash. For the CS/1-SNA, a dump may also be made of the Screen Buffer Board (SBB) RAM. The information is used by Bridge Communications' technical support staff to diagnose the cause of the crash.

The procedure is applicable only to systems with a local disk drive.

The procedure is valid only if the MCPU Auto Reboot option was disabled prior to the crash. (To disable Auto Reboot, remove jumper F in MCPU configuration area E1.) Otherwise, the system resets and reboots automatically after a crash, overwriting both MCPU and ESB RAM memory.

Before sending a memory dump, Bridge recommends calling Technical Support to describe the problem.

The procedure varies depending on the amount of memory in the system, the revision level of the MCPU PROM, and the server type. This section describes the procedures for the following:

- Systems with either 256K or 384K memory and MCPU PROMs designated M1 MMON 01B or earlier.
- Systems with 384K memory and MCPU PROMs designated M1 MMON 01C or later.
- CS/1-SNA systems that contain an SBB board.

Whichever procedure is used, please send the following additional information along with the dump diskettes:

- The release number of the software running in the system.
- The release numbers of all firmware in the system.
- The transceiver brand name and model number.
- The date and time at which the crash occurred, and any information available about the network traffic load at that time.
- The condition of all LED indicators on the server front panel and on individual boards.
- The extent of the system affected (i.e., a single port, several ports, or the entire unit).
- A description of any symptoms present prior to the crash.
- The text of any error messages that appeared on the console terminal at the time of the crash (if one was attached).
- The text of any error messages that appeared on the console terminal during any step of the dump procedure, and a description of any action taken to recover from the error (e.g., skipped the step, repeated the step successfully).

MCPU PROM Release M1 MMON 01B or Earlier

This procedure requires two previously formatted diskettes; the instructions for formatting diskettes are provided in Section C.1.3.

To obtain a memory dump, perform these steps from the console terminal:

1. Display the contents of the system registers by entering the Display Register command:

   ```
   dr
   ```

   Write down the values listed in the resulting display. This information must be sent along with the dump diskettes.

2. At this point, if the diskettes have not been formatted, use the procedure outlined in the previous section to format them. Formatting the diskettes prior to obtaining the contents of the system registers (step 1) erases the contents of the registers.

3. Insert the first formatted diskette into the disk drive.

4. Write the contents of the MCPU RAM to the diskette. (For 256K systems, this is the entire MCPU RAM area; for 384K systems, this is the first 256K bytes of MCPU RAM.) Enter the Write command as follows:

   ```
   w 1 0 40000
   ```

   If an error message appears, refer to the text at the end of this procedure.

5. When the write is complete and the Disk Activity light on the disk drive goes out, remove the diskette and label it "MCPU RAM DUMP."

6. Insert the second formatted diskette into the disk drive.

7. Write the contents of the ESB RAM to the diskette by entering this version of the Write command:

   ```
   w 1 100000 1ffe0
   ```

   If this step fails, write down the error message and include this information with the dump diskettes; then continue to the next step.

8. If this is a 384K system, write the remaining 128K bytes of MCPU RAM to the same diskette by entering this version of the Write command:

   ```
   w 101 40000 20000
   ```

9. When the write is complete, remove the diskette and label it "ESB RAM DUMP" (for 256K systems) or "ESB RAM AND MCPU RAM DUMP" (for 384K systems).

10. Send the diskettes, the register values displayed in step 1, and any applicable information from the list at the beginning of Section C.1.4 to Bridge Communications or an authorized service representative.

In some instances a crash may leave the disk drive unusable because some monitor parame-

ters were overwritten. In this case, the system may respond to step 4 with an error message. To recover from this condition, enter the Software Reset command:

```
k
```

This procedure should reinitialize the monitor correctly without causing too much information to be lost. Return to step 4 above and continue with the memory dump. The information sent with the diskettes should include a note that the Software Reset command had to be entered.

MCPU PROM Release M1 MMON 01C or Later

The procedure for obtaining a memory dump is much simpler for systems with PROMs designated M1 MMON 01C or later. This procedure requires two diskettes.

It is not necessary to preformat the diskettes or to enter the Display Register command; the Dump command automatically performs these steps.

1. From the console terminal, enter the Dump command:

   ```
   du
   ```

   The system writes the first 256K bytes of MCPU RAM memory onto the first diskette.

   If an error message appears, refer to the text at the end of this procedure.

2. When the write is complete, and the Disk Activity light goes out, remove the diskette from the drive and label it "MCPU RAM DUMP."

3. Insert the second diskette. The system then writes the ESB RAM memory and the remaining bytes of MCPU RAM memory onto the second diskette.

4. When the write is complete, and the Disk Activity light goes out, remove the diskette and label it "ESB RAM AND MCPU RAM DUMP."

5. Send the diskettes, along with all the applicable information indicated at the beginning of Section C.1.4, to Bridge Communications or an authorized service representative.

In some instances a crash may leave the disk drive unusable because some monitor parameters were overwritten. In this case, the system may respond to step 1 with an error message. To recover from this condition, enter the Software Reset command:

```
k
```

This procedure should reinitialize the monitor correctly without causing too much information to be lost. Return to step 1 and continue with the memory dump. The information sent with the diskettes should include a note that the Software Reset command had to be entered.

CS/1-SNA Screen Buffer Board Dump

This procedure is used to obtain a dump of the SBB board RAM. It applies only to CS/1-SNA systems that contain an SBB board.

1. Insert a formatted diskette in the disk drive (refer to Section C.1.3).
2. Write the contents of the SBB RAM to the diskette by entering this version of the Write command:

```
w 1 140000 40000
```

3. When the write is complete, remove the diskette and label it "SBB RAM DUMP."

Send the SBB, MCPU, and ESB dump diskettes, along with any applicable information from the list at the beginning of Section C.1.4, to Bridge Communications or an authorized service representative.

C.2 Series/100 Disk Utilities

This section describes the Series/100 disk duplication, disk formatting, and memory dump procedures.

The Series/100 disk utility functions are performed through the Series/100 utilities diskette. When the diskette is booted, port 0 becomes a console port; the utilities can then be executed from an asynchronous terminal attached to port 0. On a CS/100-BSC, if a character-synchronous terminal is attached to port 0, that terminal must be disconnected and an asynchronous terminal must be connected in its place. The port is configured with a BAud parameter of Hi_AutoBaud and a PARIty parameter of AutoParity. The terminal should operate at 2400, 4800, or 9600 baud; any parity setting is acceptable.

To boot the utilities diskette, follow the usual system startup procedures, but insert the utilities diskette instead of the system diskette into the disk drive. The bootstrap procedures are described in the *Series/100 Planning and Installation Guide* (reference [4]). After the system is booted, enter the sequence "<RETURN>.<RETURN>" on the terminal attached to port 0; this sequence permits the Series/100 server to determine the terminal's baud rate and parity setting.

C.2.1 Backing Up the System Diskette

This procedure applies only to a Series/100 server that boots from an internal disk drive. For a server that boots from an NCS, the equivalent procedure is performed on the NCS. Refer to the appropriate *NCS Installation and Operation Guide* for more information.

Once the system generation parameters have been adjusted for an installation, and any port configuration necessary to establish the appropriate configuration tables is complete, make a backup copy of the system diskette.

If the Sysgen menu is still on the screen, choose option 3 to exit the Sysgen program. If the Series/100 communications software has been running, the system must be rebooted with the utilities diskette in the disk drive. In either case, the program can be executed when an angle-bracket prompt (>) appears on the screen of a terminal attached to port 0.

To create one or more copies of the system diskette, enter the Copy command (co) followed by the number of copies desired. For example, to request two copies, enter:

```
co 2
```

The system prompts the user to place the source diskette in the disk drive and press the return key. Next, the system prompts the user to place a new diskette in the drive and press the return key. Repeat this procedure as many times as specified in the command line.

The destination diskette may be unformatted; the Copy utility automatically formats it.

C.2.2 Installing a Software Update

This section describes the procedure for installing a new software release on a Communications Server that is already configured and in place on the network.

This procedure applies only to a Series/100 server that boots from an internal disk drive. For a server that boots from an NCS, the equivalent procedure is performed on the NCS. Refer to the appropriate *NCS Installation and Operation Guide* for more information.

The general procedure for installing a software update is to replace only the communications software on the diskette, leaving all port configuration tables undisturbed. The exact procedure varies, depending on the sizes of the old and new software releases.

Some new software releases may be incompatible in terms of code size with prior releases, making it impossible to install a software update and preserve all configuration information. In some cases, the existing configuration information may be obsolete, and an installation that preserves all configuration information is unnecessary.

Review the needs of the local installation and refer to the release memo that accompanies the new release to determine which installation procedure to use:

- If the existing configuration information is to be retained, and if the new release is size-compatible with the old release, use the procedure described in this section.
- If the configuration information is not going to be retained, or if the two releases are not size-compatible, use the procedure outlined in the previous section for copying the entire diskette. Then complete the installation by performing the system generation and port configuration procedures.

If the release memo accompanying the software distribution diskette contains different instructions for installing the new software, follow those instructions instead of the procedure described here.

The software update installation procedure is performed using the Copy utility on the Series/100 utilities diskette. If the system is not already booted into the utilities diskette, follow the instructions at the beginning of Section C.2.

When an angle-bracket prompt (>) appears on the screen of a terminal attached to port 0, enter the Copy command with the partial option (co -p) followed by the number of updated copies to be made. For example, to update two software diskettes and retain the existing configuration parameter tables on each of the diskettes, enter the following command:

```
co -p 2
```

The system prompts for the starting block number and then for the ending block number of the range to be copied. The starting and ending block numbers may vary with each software release, and must be obtained from the release memo that accompanied the software distribution diskette.

After prompting the user for starting and ending block numbers, the system prompts the user to place the source diskette in the disk drive and press the return key. Next, the system prompts the user to place the destination diskette in the disk drive and press the return key. Repeat these steps as many times as specified in the command line.

C.2.3 Formatting a Diskette

This section describes the procedure for formatting a blank diskette for use on a Communications Server. The procedure applies only to a Series/100 server that has an internal disk drive.

During normal use, only the system diskette supplied by Bridge is needed. The network manager may, however, want to keep two formatted diskettes available in case a memory dump is necessary to help diagnose a system failure.

To format the diskette currently in the disk drive, enter the Format command:

```
fo
```

The system prompts the user to insert the diskette to be formatted and press the return key.

**** CAUTION ****

Ensure that the appropriate diskette is in the disk drive before pressing the return key. After the return key is pressed, the system immediately formats whichever diskette is present, erasing all information previously on the diskette.

C.2.4 Obtaining a Memory Dump

This procedure is used to write the contents of the MP's private and shared RAM onto diskettes following a system crash. The information is used by Bridge Communications' technical support staff to diagnose the cause of the crash.

The memory dump procedure applies only to systems with a local disk drive.

This procedure is valid only if the Auto Reboot option was disabled prior to the crash (see reference [4]). Otherwise, the system resets and reboots automatically after a crash, overwriting both private and shared RAM.

Before sending a memory dump, Bridge recommends calling Technical Support to describe the problem.

Please send the following additional information along with the dump diskettes:

- The release number of the software running in the system.
- The release numbers of all firmware in the system.
- The transceiver brand name and model number.
- The date and time at which the crash occurred, and any information available about the network traffic load at that time.
- The condition of all LED indicators on the server front panel (and on individual boards, if known).
- The extent of the system affected (i.e., a single port, several ports, or the entire unit).
- A description of any symptoms present prior to the crash.
- The text of any error messages that appeared on the console terminal at the time of the crash (if one was attached).

- The text of any error messages that appeared on the console terminal during any step of the dump procedure, and a description of any action taken to recover from the error (e.g., skipped the step, repeated the step successfully).

The memory dump procedure is performed from a console terminal attached to port 0 on the Series/100 server. To set up the system for a console terminal, follow these steps:

1. Remove the cable, if any, connected to port 0 on the Series/100 server.
2. Unbend a paper clip or cut a length of wire long enough to reach from pin 7 to pin 11 of the RS-232 connector. Insert one end into the pin 7 receptacle and the other end into the pin 11 receptacle of port 0, labeled "J0C", on the Series/100 server back panel. Leave the wire in place for 2 to 3 seconds, then remove it.

   The RS-232 jumper card accessory, available from Bridge, may be used in place of the paper clip.
3. Attach a terminal to port 0. The terminal should be set up for either 9600 or 1200 baud, no parity, and 8 databits.
4. Press the return key. A message followed by an angle-bracket prompt (>) appears on the terminal screen, and the Self Test LED stops blinking and remains lit.

   Write down the screen message and include it with the documentation to be sent with the diskettes.

The remainder of the memory dump procedure varies depending on the revision level of the MP PROM. This section describes the procedures for servers with the following PROMs:

- T1 MMON 01C or earlier
- T1 MMON 01D or later

MP PROM Release T1 MMON 01C or Earlier

This procedure requires two previously formatted diskettes; instructions for formatting diskettes are provided in Section C.2.3.

1. Display the contents of the system registers by entering the Display Register command on the console terminal:

   ```
   dr
   ```

   Write down the values listed in the resulting display. This information must be sent along with the dump diskettes.
2. Insert the first formatted diskette into the disk drive.

3. Write the contents of the shared RAM to the diskette by entering this version of the Write command:

```
w 1 200000 20000
```

   If an error message appears, refer to the text at the end of this procedure.

4. When the write is complete and the Disk Activity light on the disk drive goes out, remove the diskette and label it "SHARED RAM DUMP."

5. Insert the second formatted diskette into the disk drive.

6. Write the contents of the private RAM to the diskette by entering this version of the Write command:

```
w 1 220000 20000
```

7. When the write is complete and the Disk Activity light on the disk drive goes out, remove the diskette and label it "PRIVATE RAM DUMP."

8. Send the two diskettes, the error message, and the register values, with a description of how and when the crash occurred and the state of the system at the time, to Bridge Communications or an authorized service representative.

In some instances a crash may leave the disk drive unusable because some monitor parameters were overwritten. In this case, the system may respond to step 3 with an error message. To recover from this condition, enter the Software Reset command:

```
k
```

This procedure should reinitialize the monitor correctly without causing too much information to be lost. Return to step 3 above and continue with the memory dump. The information sent with the diskettes should include a note that the Software Reset command had to be entered.

MP PROM Release T1 MMON 01D or Later

The procedure for obtaining a memory dump is much simpler for systems with PROMs designated T1 MMON 01D or later. This procedure requires two diskettes.

It is not necessary to preformat the diskettes or to enter the Display Register command; the Dump command automatically performs these steps.

1. From the console terminal, enter the Dump command:

```
du
```

   The system begins writing the contents of memory onto the first diskette.

   If an error message appears, refer to the text at the end of this procedure.

2. When prompted to label the diskette, check that the Disk Activity light is out, remove the diskette from the drive and label it "MEMORY DUMP #1"

3. Insert the second diskette. The system then writes the contents of memory onto the second diskette.

   When prompted to label the diskette, check that the Disk Activity light is out, remove the diskette from the drive and label it "MEMORY DUMP #2"

4. The monitor continues to prompt for additional diskettes. Be certain to label each diskette "MEMORY DUMP #n" with the appropriate sequence number.

5. Send the diskettes, along with all the applicable information indicated at the beginning of Section C.2.4, to Bridge Communications or an authorized service representative.

In some instances a crash may leave the disk drive unusable because some monitor parameters were overwritten. In this case, the system may respond to step 1 with an error message. To recover from this condition, enter the Software Reset command:

```
k
```

This procedure should reinitialize the monitor correctly without causing too much information to be lost. Return to step 1 and continue with the memory dump. The information sent with the diskettes should include a note that the Software Reset command had to be entered.

APPENDIX D

MONITOR ERROR MESSAGES

This appendix provides an alphabetical list of common error messages generated by the monitor and describes the probable causes of each message.

Bridge Communications MCPU Monitor
>

This message and prompt appear when the self-tests have completed. Control returns to the monitor.

Disk controller not present

This message appears if the disk controller does not respond.

Diskette not present

This message appears if there is no diskette in the drive or if the diskette is improperly inserted.

Drive not ready

This message indicates that the drive is not ready to perform the necessary operation. May indicate a malfunctioning drive or a problem with the cable that connects the drive controller and drive. The cause of this error should be investigated; call Bridge or an authorized Bridge service representative.

EC<n> - Failed Test # <x>

This message is displayed if an error is encountered in test x.

In servers with an EC/2, the test number is encoded in hexadecimal on the five self-test LEDs. For example, if test 10 fails, LED A lights, corresponding to hexadecimal 10000.

EC<n> - not present

This message appears if the Ethernet Controller does not respond to a Multibus memory access. Control returns to the monitor.

EC<n> - Passed Station Address - <xxxxxxxxxx> M0 EDL1 rev. <xxy> (EC/1)
EC<n> - Passed Station Address - <xxxxxxxxxx> M0 EDL2 rev. <xxy> (EC/2)

One of these messages appears if no errors are encountered in the Ethernet Controller tests.

EC - timed out

This message appears if the Ethernet Controller is present but does not respond to a status request. Control returns to the monitor.

File not present

This message indicates that the specified file does not exist or is not present on the diskette.

File in use

This message indicates that the file is in use.

Floppy controller not present

This message appears if the system has no internal disk drive or if the disk drive is present but does not respond.

Floppy parameters exceeded

This message indicates that the capacity of the server's disk has been exceeded.

Format Error

This message appears if the diskette in the drive is not formatted or is formatted incorrectly.

Illegal ID

Indicates that the main processor board has received an illegal identification code from another board. The cause of this error should be investigated; call Bridge or an authorized Bridge service representative.

Loaded

Indicates successful loading of software over the network.

MCPU - Failed Test # <x>

This message is displayed if an error is encountered in test x.

MCPU - Passed M1 MMON rev. <xxy>

This message appears if no errors are encountered in the self-tests.

No Ethernet Card

This message appears if the server attempts a network bootstrap and the Ethernet board is not present.

read error

This message appears if the system attempts to access the diskette and the data field of the sector being accessed has been corrupted.

seek error

This message appears if the identification field of a sector being accessed has been corrupted.

Series1 Power-up
Series100 Power-up
Series200 Power-up

One of these message appears when the board enters the test sequence, and stays on the screen whether the MCPU tests terminate or fail.

SIO <n> - Passed M<x aaaa> rev. <xxy>
SIO <n> - Passed T<x aaaa> rev. <xxy>
SIO <n> - Passed T<x aaaa> rev. <xxy> IOX1
SIO <n> - Passed T<x aaaa> rev. <xxy> IOX1/IOX2
SIO <n> - Passed T<x aaaa> rev. <xxy> SBX

One of these messages appears if no errors are encountered in the SIO self-tests.

SIO <n> - Failed Test # <x>

This message appears if an error is encountered in test x.

SIO <n> - not present

This message appears if any of the possible SIO boards fails to respond to a Multibus request. Control returns to the monitor. This message indicates an error only if an SIO board is actually in place in the slot indicated in the message.

SIO <n> - timed out
SIO <n> - timed out channel attn #1/2

This message appears if SIO boards are present, but do not respond to a status request. Control returns to the monitor.

write error

This message appears if the system is unable to write on a particular sector of the diskette. This error usually indicates a damaged diskette.

write protected

This message appears if the diskette in the drive is write-protected and the system attempts to write to the diskette.

INDEX

Bridge Communications, Inc.
2081 Stierlin Road
Mountain View, CA 94043
Telephone: 415/969-4400