Configuring TCP Services

Bay Networks

Bay Networks

Bay Networks Software License

Note: *This is Bay Networks basic license document. In the absence of a software license agreement specifying varying terms, this license — or the license included with the particular product — shall govern licensee's use of Bay Networks software.*

This Software License shall govern the licensing of all software provided to licensee by Bay Networks ("Software"). Bay Networks will provide licensee with Software in machine-readable form and related documentation ("Documentation"). The Software provided under this license is proprietary to Bay Networks and to third parties from whom Bay Networks has acquired license rights. Bay Networks will not grant any Software license whatsoever, either explicitly or implicitly, except by acceptance of an order for either Software or for a Bay Networks product ("Equipment") that is packaged with Software. Each such license is subject to the following restrictions:

1. Upon delivery of the Software, Bay Networks grants to licensee a personal, nontransferable, nonexclusive license to use the Software with the Equipment with which or for which it was originally acquired, including use at any of licensee's facilities to which the Equipment may be transferred, for the useful life of the Equipment unless earlier terminated by default or cancellation. Use of the Software shall be limited to such Equipment and to such facility. Software which is licensed for use on hardware not offered by Bay Networks is not subject to restricted use on any Equipment, however, unless otherwise specified on the Documentation, each licensed copy of such Software may only be installed on one hardware item at any time.

2. Licensee may use the Software with backup Equipment only if the Equipment with which or for which it was acquired is inoperative.

3. Licensee may make a single copy of the Software (but not firmware) for safekeeping (archives) or backup purposes.

4. Licensee may modify Software (but not firmware), or combine it with other software, subject to the provision that those portions of the resulting software which incorporate Software are subject to the restrictions of this license. Licensee shall not make the resulting software available for use by any third party.

5. Neither title nor ownership to Software passes to licensee.

6. Licensee shall not provide, or otherwise make available, any Software, in whole or in part, in any form, to any third party. Third parties do not include consultants, subcontractors, or agents of licensee who have licensee's permission to use the Software at licensee's facility, and who have agreed in writing to use the Software only in accordance with the restrictions of this license.

7. Third-party owners from whom Bay Networks has acquired license rights to software that is incorporated into Bay Networks products shall have the right to enforce the provisions of this license against licensee.

8. Licensee shall not remove or obscure any copyright, patent, trademark, trade secret, or similar intellectual property or restricted rights notice within or affixed to any Software and shall reproduce and affix such notice on any backup copy of Software or copies of software resulting from modification or combination performed by licensee as permitted by this license.

Bay Networks Software License *(continued)*

9. Licensee shall not reverse assemble, reverse compile, or in any way reverse engineer the Software. [Note: For licensees in the European Community, the Software Directive dated 14 May 1991 (as may be amended from time to time) shall apply for interoperability purposes. Licensee must notify Bay Networks in writing of any such intended examination of the Software and Bay Networks may provide review and assistance.]

10. Notwithstanding any foregoing terms to the contrary, if licensee licenses the Bay Networks product "Site Manager," licensee may duplicate and install the Site Manager product as specified in the Documentation. This right is granted solely as necessary for use of Site Manager on hardware installed with licensee's network.

11. This license will automatically terminate upon improper handling of Software, such as by disclosure, or Bay Networks may terminate this license by written notice to licensee if licensee fails to comply with any of the material provisions of this license and fails to cure such failure within thirty (30) days after the receipt of written notice from Bay Networks. Upon termination of this license, licensee shall discontinue all use of the Software and return the Software and Documentation, including all copies, to Bay Networks.

12. Licensee's obligations under this license shall survive expiration or termination of this license.

Contents

Appendix A
Site Manager Default Settings

Index

Figures

Tables

About This Guide

If you are responsible for configuring and managing Bay Networks routers or BNX platforms, read this guide to discover how to customize Bay Networks router software for Transmission Control Protocol (TCP) services.

Configuring TCP Services offers

- An overview of TCP (see Chapter 1)

- Implementation notes that may affect how you configure TCP services (see Chapter 2)

- Instructions on editing TCP, Telnet, and FTP parameters (see Chapter 3)

Software Suites

Routing and Switching software is available in the following suites:

- The *System Suite* includes IP routing, 802.1 Transparent Bridge, Source Route Bridge, Translation Bridge, SNMP Agent, Bay Networks HDLC, PPP, OSPF, EGP, BGP, and basic DLSw.

- The *LAN Suite* includes DECnet Phase 4, AppleTalk Phase 2, OSI, VINES, IPX, and ATM DXI, in addition to the System Suite.

- The *WAN Suite* includes ATM DXI, Frame Relay, LAPB, and X.25, in addition to the System Suite.

- The *Corporate Suite* includes the System, LAN, and WAN suites in their entirety.

- The *ARE ATM Suite* provides RFC 1483 and 1577 compliance, ATM UNI 3.0 signaling, in addition to the LAN Suite.

- The *ARE VNR Corporate Suite* provides ATM Forum LAN Emulation, in addition to the ARE ATM Suite and Corporate Suite.

- The *BNX Suite* includes IP Routing, SNMP Agent, Bay Networks HDLC, PPP, OSPF, EGP, BGP, File-Based Performance Statistics, Frame Relay switching, and Frame Relay billing, and selected components from the Corporate, ARE ATM, and ARE VNR Corporate suites.

Availability of features and functionality described in this guide depends on the suites you are using.

Audience

Written for system and network managers, this guide describes how to configure the Bay Networks implementation of TCP services to suit your environment.

Before You Begin

Before using this guide, you must complete the following procedures:

- Create and save a configuration file that has at least one IP interface.
- Retrieve the configuration file in local, remote, or dynamic mode.

Refer to *Configuring Routers* or *Configuring Customer Access and Trunks (BNX Software)*, depending on the type of installed software, for instructions.

Bay Networks Customer Support

Bay Networks provides live telephone technical support to our distributors, resellers, and service-contracted customers from two U.S. and three international support centers. If you have purchased your Bay Networks product from a distributor or authorized reseller, contact the technical support staff of that distributor or reseller for assistance with installation, configuration, troubleshooting, or integration issues.

Customers also have the option of purchasing direct support from Bay Networks through a variety of service programs. The programs include priority access telephone support, on-site engineering assistance, software subscription, hardware replacement, and other programs designed to protect your investment.

To purchase any of these support programs, including PhonePlus™ for 24-hour telephone technical support, call 1-800-2LANWAN. Outside the U.S. and Canada, call (408) 764-1000. You can also receive information on support programs from your local Bay Networks field sales office, or purchase Bay Networks support directly from your reseller. Bay Networks provides several methods of receiving support and information on a nonpriority basis through the following automated systems.

CompuServe

Bay Networks maintains an active forum on CompuServe. All you need to join us online is a computer, a modem, and a CompuServe account. We also recommend using the CompuServe Information Manager software, available from CompuServe.

The Bay Networks forum contains libraries of technical and product documents designed to help you manage and troubleshoot your Bay Networks products. Software agents and patches are available, and the message boards are monitored by technical staff and can be a source for problem solving and shared experiences.

Customers and resellers holding Bay Networks service contracts can visit the special libraries to acquire advanced levels of support documentation and software.

To open an account and receive a local dial-up number, call CompuServe at 1-800-524-3388 and ask for Representative No. 591.

- In the United Kingdom, call Freephone 0800-289378.

- In Germany, call 0130-37-32.

- In Europe (except for the United Kingdom and Germany), call (44) 272-760681.

- Outside the U.S., Canada, and Europe, call (614) 529-1349 and ask for Representative No. 591, or consult your listings for an office near you.

Once you are online, you can reach our forum by typing the command GO BAYNETWORKS at any ! prompt.

InfoFACTS

InfoFACTS is the Bay Networks free 24-hour fax-on-demand service. This automated system contains libraries of technical and product documents designed to help you manage and troubleshoot your Bay Networks products. The system can return a fax copy to the caller or to a third party within minutes of being accessed.

World Wide Web

The World Wide Web (WWW) is a global information system for file distribution and online document viewing via the Internet. You need a direct connection to the Internet and a Web Browser (such as Mosaic or Netscape).

Bay Networks maintains a WWW Home Page that you can access at http://www.baynetworks.com. One of the menu items on the Home Page is the Customer Support Web Server, which offers technical documents, software agents, and an E-mail capability for communicating with our technical support engineers.

How to Get Help

For additional information or advice, contact the Bay Networks Technical Response Center in your area:

United States	1-800-2LAN-WAN
Valbonne, France	(33) 92-966-968
Sydney, Australia	(61) 2-903-5800
Tokyo, Japan	(81) 3-328-005

Conventions

This section describes the conventions used in this guide.

angle brackets (< >)   Indicate that you choose the text to enter based on the description inside the brackets. Do not type the brackets when entering the command. Example: if command syntax is **ping** *<ip_address>*, you enter **ping 192.32.10.12**

arrow character (➔)	Separates menu and option names in instructions. Example: Protocols➔AppleTalk identifies the AppleTalk option in the Protocols menu.
bold text	Indicates text that you need to enter and command names in text. Example: Use the **dinfo** command.
brackets ([ ])	Indicate optional elements. You can choose none, one, or all of the options.
italic text	Indicates variable values in command syntax descriptions, new terms, file and directory names, and book titles.
quotation marks (" ")	Indicate the title of a chapter or section within a book.
screen text	Indicates data that appears on the screen. Example: Set Bay Networks Trap Monitor Filters
ellipsis points	Horizontal (. . .) and vertical (⋮) ellipsis points indicate omitted information.
vertical line (|)	Indicates that you enter only one of the parts of the command. The vertical line separates choices. Do not type the vertical line when entering the command.
	Example: If the command syntax is
	show at routes	**nets**, you enter either **show at routes** or **show at nets**, but not both.

Ordering Bay Networks Publications

To purchase additional copies of this document or other Bay Networks publications, order by part number from Bay Networks Press™ at the following numbers. You may also request a free catalog of Bay Networks Press product publications.

Phone: 1-800-845-9523
FAX - U.S./Canada: 1-800-582-8000
FAX - International: 1-916-939-1010

Acronyms

ANSI	American National Standards Institute
ARP	Address Resolution Protocol
ATM	Asynchronous Transfer Mode
BGP	Border Gateway Protocol
CMIP	Common Management Information Protocol
DLSw	data link switching
EGP	Exterior Gateway Protocol
FDDI	Fiber Distributed Data Interface
FTP	File Transfer Protocol
IEEE	Institute of Electrical and Electronic Engineers
ILI	intelligent link interface
IP	Internet Protocol
MAC	Media Access Control
MOP	Maintenance Operations Protocol
OSI	Open Systems Interconnection
OSPF	Open Shortest Path First
PVCs	permanent virtual circuits
QENET	Quad Ethernet Link Module
RIP	Routing Information Protocol
SMDS	Switched Multimegabit Data Services
SNAP	Subnetwork Access Protocol
SNMP	Simple Network Management Protocol
SRM	system resource modules
SVCs	switched virtual circuits
TCP	Transmission Control Protocol
TCP/IP	Transmission Control Protocol/Internet Protocol
TFTP	Trivial File Transfer Protocol

Chapter 1
Transmission Control Protocol Overview

In the 1970s, the Defense Advanced Research Projects Agency (DARPA) of the U.S. Department of Defense developed the Transmission Control Protocol (TCP) to provide communication among hosts manufactured by different vendors.

DARPA designed TCP to work within a layered hierarchy of networking protocols, using the Internet Protocol (IP) to transfer data.

This chapter introduces TCP concepts, features, and terminology and consists of the following sections:

- "Reliability"
- "Connection Types"
- "Connections and Connection States"
- "TCP and IP Service Users"
- "Telnet"
- "File Transfer Protocol"

Reliability

Since IP does not always guarantee reliable transfer of data, TCP implements several features to ensure that data arrives at its destination uncorrupted and in the order sent. These features include

- **Sequence numbers.** TCP assigns a sequence number to each data segment it transmits. The receiving host uses the sequence numbers to make sure that all the data arrives in order.

- **Out-of-order caching.** As TCP receives data segments, it puts them in sequential order and forwards them to the receiving TCP client. If TCP does not receive one or more segments and cannot complete the sequential ordering, it stores the remaining segments in cache memory for as long as the TCP connection exists. When TCP receives the missing segments, it takes the stored segments from cache memory, puts them into sequential order with the newly received segments, and then forwards them to the receiving TCP client. Out-of-order caching ensures that data arrives in the correct order while saving bandwidth and retransmission time.

- **Checksums.** To ensure the integrity of the data, the sending host adds a checksum to each segment it transmits. The receiving host recalculates the checksum, and if there is damage, discards the segment.

- **Flow control.** Flow control allows the receiving host to regulate how much data is sent to it. To activate flow control, the receiving host advertises a *window* that indicates how much data it can accept. When the transmit window is full, the sending host must stop sending data until the receiving host can open the window again. To control the rate of data transfer on your TCP connections, you can specify the maximum window size allowed for each connection.

- **Acknowledgment with retransmission.** TCP requires the receiving host to acknowledge that it has received the data. If the sending host does not receive an acknowledgment within a set timeout interval, the sending station retransmits the data. TCP determines the timeout interval by estimating the average time it takes to send a segment and receive an acknowledgment for it.

Connection Types

TCP allows both *active* and *passive* connections (or *opens*). For passive opens, a *TCP client* (the process or program that uses TCP) waits to accept incoming connection requests. Clients using passive opens can listen for specific connection requests or for a range of inbound requests. In an active open, the client initiates the connection.

Connections and Connection States

TCP establishes a set of access points, referred to as *ports*, for each host. It associates each port with a network and host address to form a *socket*. A pair of sockets, together with sequence numbers, window sizes, and status information, form a *TCP connection*.

Table 1-1 lists the states through which a TCP connection proceeds during its lifetime.

Table 1-1.   TCP Connection States

State	Definition
LISTEN (2)	TCP listens for a connection request from any remote TCP.
SYN SENT (3)	TCP sent a connection request (SYN segment) and waits for a matching connection request and acknowledgment from the remote TCP.
SYNRECEIVED (4)	TCP sent a connection request, received a matching request, and waits for a confirming connection request acknowledgment from the remote TCP.
ESTABLISHED (5)	Connection open. Data can be received and sent. This is the normal state for the data transfer phase of the connection.
FINWAIT-1 (6)	TCP waits for a connection termination request (FIN segment) from the remote TCP, or for an acknowledgment of a previously sent connection termination request.
FINWAIT-2 (7)	TCP waits for a connection termination request from the remote TCP.
CLOSEWAIT (8)	TCP waits for a connection termination request from the client.
CLOSING (10)	TCP waits for a connection termination request acknowledgment from the remote TCP.
LASTACK (9)	TCP waits for acknowledgment of the connection termination request previously sent to the remote TCP.
TIMEWAIT (11)	TCP waits for enough time to pass to ensure that the remote TCP received the acknowledgment of its connection termination request.
CLOSED (1)	No connection.

TCP and IP Service Users

TCP is the layer or service between IP, at the lower layer in the hierarchy of network protocols, and programs running at higher layers in the hierarchy. Figure 1-1 shows a simple network architecture with four users of TCP/IP services: the Data Link Switching Service (DLSw), Telnet, FTP, and the Border Gateway Protocol (BGP).
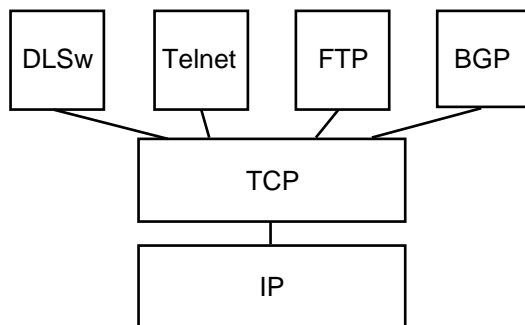
Figure 1-1.   TCP between IP and Clients

The interface between TCP and programs that use TCP consists of a set of messages exchanged between the clients and TCP, and a set of functions and macros that user programs call to exchange TCP messages. These programs use the functions and macros to

•   Open, close, abort, and get the status of connections

•   Control the flow of data

•   Encapsulate data for TCP to transmit

•   Process received TCP data

When a program passes data to TCP, the TCP layer formats the data and calls on the IP layer to transmit the data to its destination.

For information on creating TCP on the router and editing TCP parameters, refer to "Configuring and Customizing TCP" in Chapter 3.

Telnet

Telnet allows you to access the Technician Interface. You can execute Technician Interface commands from a remote host (inbound Telnet) or originate an outgoing Telnet session (outbound Telnet) to another Bay Networks router or network device that accepts Telnet. You use outbound Telnet to access remote routers when Site Manager or Simple Network Management Protocol (SNMP) is unavailable.

To use Telnet to access the Technician Interface, you must assign at least one IP address to the router. The number of Telnet connections you can make to the Technician Interface is limited only by the availability of system resources (that is, system memory).

➡ **Note:** *We recommend that you establish no more than one Telnet session per router.*

For information on creating Telnet on the router and editing Telnet parameters, refer to "Configuring and Customizing the Telnet Server" and "Configuring and Customizing the Telnet Client" in Chapter 3.

For complete information about accessing and using the Technician Interface with Telnet, see *Using Technician Interface Software.*

File Transfer Protocol

The File Transfer Protocol (FTP) allows you to

- Download files from your host system to a remote router and retrieve files from the router

- Examine the directory listing of files on the remote router

- Delete files on the router

The FTP client residing on your host and the FTP server residing on the router rely on the underlying support of TCP and IP for the reliable, sequenced transfer of data and control messages.

The FTP client on your host initiates an FTP session with an FTP server on the router. The session establishes two separate connections between host and router: a control connection and a data connection (Figure 1-2).
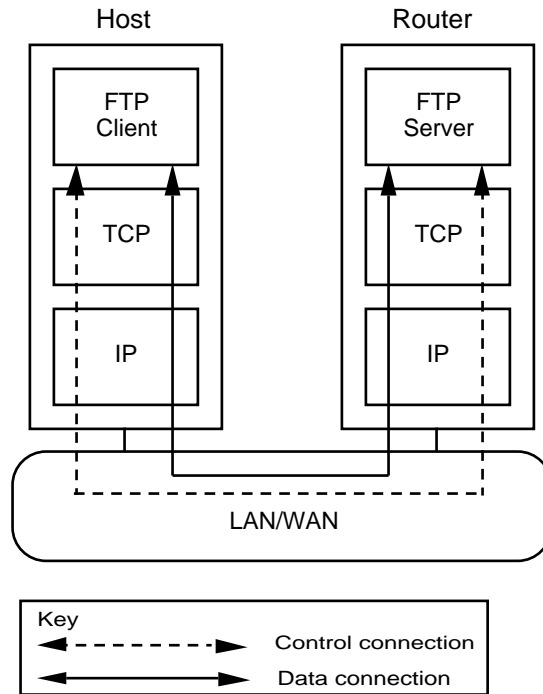
Figure 1-2.   FTP Client and Server

Table 1-2 describes the FTP commands that the FTP server supports on Bay Networks routers.

Table 1-2.   FTP Commands Supported by the FTP Server

Command	Code	Description
Access Control Commands		
User Name	USER	Initiates an FTP session for the user.
Password	PASS	Specifies a user's encrypted identification for access control.
Logout	QUIT	Terminates the session and closes the control connection.
Transfer Parameter Commands		
Data Port	PORT	Specifies the data port to be used in the data connection.
Representation Type	TYPE	Specifies the data transfer type. The server supports transfer of ASCII and image (binary) data.
Transfer Mode	MODE	Specifies the transfer mode. The server supports stream mode only.
File Structure	STRU	Specifies the file structure type. The server supports file (no record) structure only.
FTP Service Commands		
Retrieve	RETR	Causes the server to transfer the specified file to the client.
Abort	ABOR	Causes the server to abort the previous FTP service command and any associated transfer of data.
Store	STOR	Causes the server to accept the data transferred over the data connection and store it on the server.
Store Unique	STOU	Specifies the same operation as the **Store** command and, in addition, causes the server to create the resulting file in the current directory under a name unique to that directory.
Delete	DELE	Causes the server to delete the specified file on the server.
List	LIST	Causes the server to send to the client a detailed list of files.
Name List	NLIST	Causes the server to send to the client a list of filenames.
Status	STAT	Causes the server to send to the client the control connection status. If the server receives the command during file transfer, the server sends the client the status of the transfer.
Help	HELP	Provides helpful information.
No Operation	NOOP	Specifies no action. Causes the server to send an OK reply.
Change Working Directory	CWD	Causes the server to change the volume.
Implementation-specific FTP Commands		
Compact	COMP	Causes the server to compact the flash card. This command should follow a delete command.

As network administrator, you use Site Manager to create the FTP server on the router and edit FTP server parameters. For complete information and instructions, refer to "Configuring and Customizing the FTP Server" in Chapter 3.

For More Information about TCP

If you would like more information about the Transmission Control Protocol, refer to

Comer, Douglas E. *Internetworking with TCP/IP, Volume I: Principles, Protocols, and Architecture*. Englewood Cliffs, New Jersey: Prentice Hall, Inc., Second Edition, 1991.

Chapter 2
TCP Implementation Notes

This chapter contains specific implementation notes to keep in mind when you configure Bay Networks TCP services.

Memory Considerations

The Transmission Control Protocol requires a significant amount of memory to

- Retain copies of outbound data in case they must be retransmitted

- Retain copies of inbound data in case they are received out of order and must be rearranged

- Manage the TCP connections

The amount of memory used per TCP connection is dynamic. Each connection uses a small amount of overhead memory (less than 1 KB), even if the connection is idle. As the size of the transmit-and-receive window increases, so does the memory for connections. It expands as much as TCP allows.

You can control the window size by setting a value for the Max. Window Size parameter in the Edit TCP Global Parameters window (see Chapter 3). The maximum amount of memory TCP can use for a connection is equal to the overhead memory plus twice the window size (because the window can fill in both directions).

The value you set for Max. Window Size depends on how much memory you need for services other than TCP. If you have a complicated configuration, specify a low Max. Window Size value for TCP connections since space is limited. Systems with less involved configurations can support more TCP connections and a higher Max. Window Size value.

If TCP consumes too much memory on the router, connections slow down or even abort. TCP uses feedback mechanisms to indicate to clients when resources are becoming scarce. However, if clients disregard this feedback, TCP has to break connections. TCP attempts to monitor the connections consuming the most memory and break those first to maintain connections consuming less memory.

Chapter 3
Editing TCP, Telnet, and FTP Parameters

Once you enable IP on your router, you can use Site Manager to create TCP, Telnet, and FTP on the router and customize TCP, Telnet, and FTP parameters.

For each TCP, Telnet, and FTP parameter, this manual provides default settings, valid parameter options, the parameter function, instructions for setting the parameter, and the Management Information Base (MIB) object ID.

The Technician Interface lets you modify parameters by issuing **set** and **commit** commands that specify the MIB object ID. This process is equivalent to modifying parameters using Site Manager. For more information about using the Technician Interface to access the MIB, refer to *Using Technician Interface Software*.

Caution: *The Technician Interface does not verify that the value you enter for a parameter is valid. Entering an invalid value can corrupt your configuration.*

To enable IP on the router, see *Configuring IP Services.*

To configure and customize TCP on the router, see the following sections:

- "Creating TCP"
- "Editing TCP Global Parameters"
- "Deleting TCP from the Router"

To configure and customize Telnet on the router, see the following sections:

- "Creating a Telnet Server"
- "Editing Telnet Server Global Parameters"
- "Deleting a Telnet Server from the Router"

- • "Creating a Telnet Client"
- • "Editing Telnet Client Global Parameters"
- • "Deleting a Telnet Client from the Router"

To configure and customize FTP on the router, see the following sections:

- • "Creating an FTP Server"
- • "Editing FTP Global Parameters"
- • "Deleting the FTP Server from the Router"

➡ **Note:** *These instructions assume that you have already configured IP on the router. If you did not configure IP, see* Configuring Routers *or* Configuring Customer Access and Trunks (BNX Software), *depending on the type of installed software.*

Configuring and Customizing TCP

Use Site Manager to create TCP, edit TCP parameters, and delete TCP from the router.

Creating TCP

To create TCP on the router, select Protocols➔Global Protocols➔TCP➔Create TCP from the Configuration Manager window (refer to Figure 3-1).
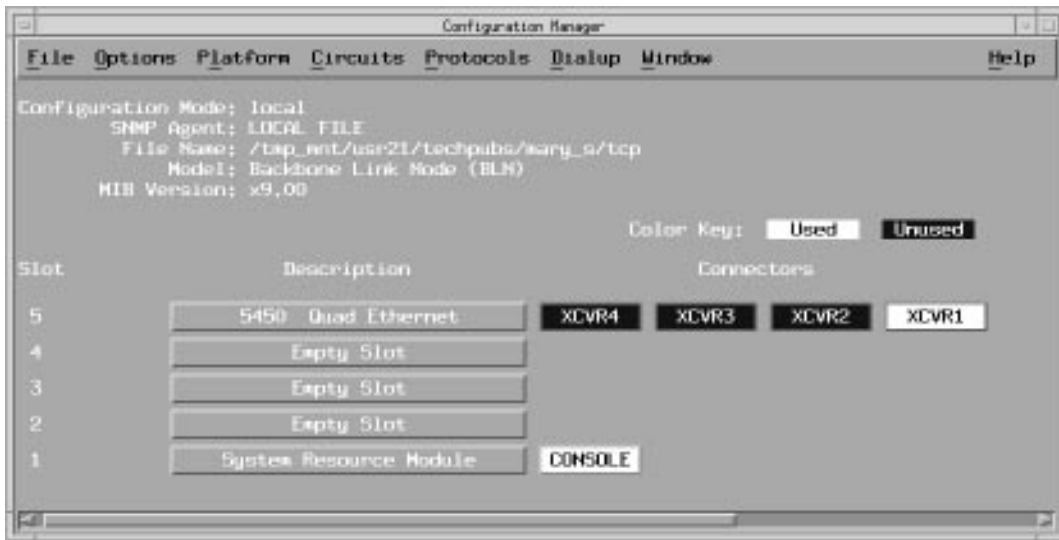
Figure 3-1.   Configuration Manager Window

Editing TCP Global Parameters

To edit TCP global parameters, follow these steps:

1. **Select Protocols➤Global Protocols➤TCP➤Global from the Configuration Manager window.**

   The Edit TCP Global Parameters window appears (refer to Figure 3-2).
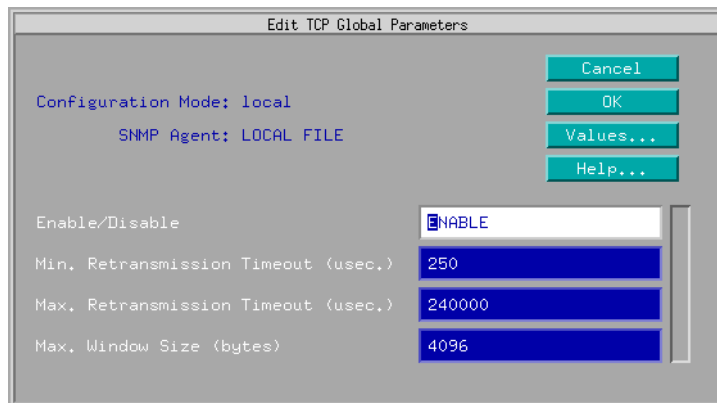
Figure 3-2.   Edit TCP Global Parameters Window

2. Edit the parameters in this window, using the guidelines in the next section.

3. Click on OK to save your changes and exit the window.

If you want to delete TCP, go to "Deleting TCP from the Router."

TCP Global Parameter Descriptions

Use the following descriptions as a guide when you configure the parameters in the Edit TCP Global Parameters window (refer to Figure 3-2).

Parameter:	**Enable/Disable**
Default:	Enable
Options:	Enable │ Disable
Function:	Enables or disables TCP on the router.
Instructions:	Select Disable to disconnect from TCP. Also, you can select Disable if you do not need TCP, but want to access previous TCP statistics.
MIB Object ID:	1.3.6.1.4.1.18.3.5.3.3.1.2

Parameter:	**Min. Retransmission Timeout (msec.)**
Default:	250 milliseconds (msec.)
Range:	100 to 15000 msec.
Function:	Sets the minimum value for the retransmission timeout. When one side of a TCP connection sends a frame and does not receive an acknowledgment from the other side of the connection within the timeout period, the sending station retransmits the frame.
Instructions:	Specify the value you want to use for the minimum timeout period. If you are transmitting on a high-speed network and you set the Min. Retransmission Timeout value too high, network performance may degrade because TCP must wait for the timeout period to elapse before retransmitting unacknowledged data.
MIB Object ID:	1.3.6.1.4.1.18.3.5.3.3.1.5

Parameter:	**Max. Retransmission Timeout (msec.)**
Default:	240000 msec.
Range:	15000 to 240000 msec.
Function:	Sets the maximum value for the retransmission timeout. When one side of a TCP connection sends a frame and does not receive an acknowledgment from the other side of the connection within the timeout period, the sending station retransmits the frame.
Instructions:	Specify the value you want to use for the maximum timeout period. If you are transmitting on a low-speed network and you set the Max. Retransmission Timeout value too low, the network may become congested as TCP retransmits unacknowledged frames that have not yet reached their destination.
MIB Object ID:	1.3.6.1.4.1.18.3.5.3.3.1.6

Parameter:	**Max. Window Size (bytes)**
Default:	4096 bytes
Range:	512 to 65535 bytes
Function:	Sets the maximum transmit-and-receive window size that TCP allows for each connection.
Instructions:	Specify the window size. The larger the window size, the more memory each TCP connection consumes.
MIB Object ID:	1.3.6.1.4.1.18.3.5.3.3.1.18

Deleting TCP from the Router

Caution: *The system automatically deletes Telnet and BGP from the router when you delete TCP.*

To delete TCP from the router, follow these steps:

1. **Select Protocols➔Global Protocols➔TCP➔Delete TCP from the Configuration Manager window (refer to Figure 3-1).**

    Site Manager asks: Do you REALLY want to delete TCP?

2. **Click on OK to delete TCP.**

Configuring and Customizing the Telnet Server

You use the Telnet Server to establish inbound Telnet sessions. The following sections describe how to create the Telnet Server using Site Manager, edit Telnet Server parameters, and delete the Telnet Server from the router.

Creating a Telnet Server

To create a Telnet Server on the router for inbound Telnet sessions, follow these steps:

1. **Select Protocols➔Global Protocols➔Telnet Server➔Create Telnet Server from the Configuration Manager window (refer to Figure 3-1).**

    The Telnet Configuration window appears (refer to Figure 3-3). The three parameters displayed locate and define the scripts that run automatically at login.
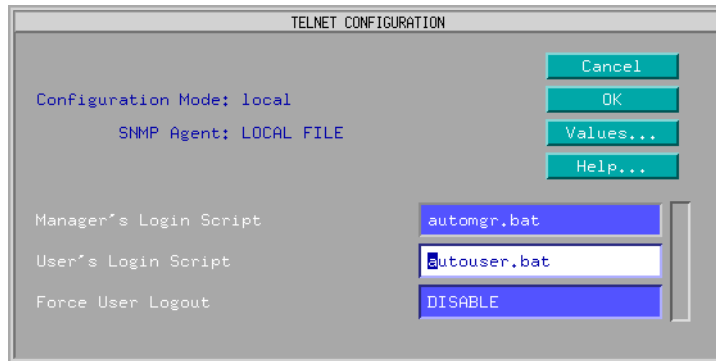
Figure 3-3.   Telnet Configuration Window

2. **Set these parameters, using the guidelines in the next section.**

3. **Click on OK to save your changes and exit the window.**

Telnet Configuration Parameter Descriptions

Use the following descriptions as a guide when setting Telnet Configuration parameters:

Parameter:	**Manager's Login Script**
Default:	*automgr.bat*
Options:	The name of the manager's login script file.
Function:	At login, executes the manager's login script file automatically.
Instructions:	If you did not change the name of the manager's login script file, accept the default. Otherwise, enter the new name (must be eight characters or less).
MIB Object ID:	1.3.6.1.4.1.18.3.5.3.7.1.21

Parameter:	**User's Login Script**
Default:	*autouser.bat*
Options:	The name of the user's login script file.
Function:	At login, executes the user's login script file automatically.
Instructions:	If you did not change the name of the user's login script file, accept the default. Otherwise, enter the new name (must be eight characters or less).
MIB Object ID:	1.3.6.1.4.1.18.3.5.3.7.1.22

Parameter:	**Force User Logout**
Default:	Disable
Options:	Enable │ Disable
Function:	Specifies whether the user can press control-c to cancel a user autoscript at login (when a user autoscript is in effect).
Instructions:	Select Enable to prevent using control-c to cancel the user autoscript at login.
	Select Disable to allow the user to press control-c to cancel the user autoscript at login.
	Use the default (Disable) if you want users to access the Technician Interface. Set to Enable if you want users to enter the Telnet logout command.
MIB Object ID:	1.3.6.1.4.1.18.3.5.3.7.1.23

Editing Telnet Server Global Parameters

To edit Telnet Server global parameters, follow these steps:

1. **Select Protocols➤Global Protocols➤Telnet Server➤Global from the Configuration Manager window (refer to Figure 3-1).**

   The Edit Telnet Server Global Parameters window appears (refer to Figure 3-4).

```
                Edit Telnet Server Global Parameters

                                              ┌─────────┐
                                              │ Cancel  │
                                              └─────────┘
Configuration Mode: local                     ┌─────────┐
                                              │   OK    │
          SNMP Agent: LOCAL FILE              └─────────┘
                                              ┌─────────┐
                                              │ Values..│
                                              └─────────┘
                                              ┌─────────┐
                                              │ Help... │
                                              └─────────┘

Enable/Disable                    ENABLE

TI Lines per Screen               24

TI More                           ENABLE

TI Prompt

Login Timeout (min.)              1

Password Timeout (min.)           1

Command Timeout (min.)            15

Login Retries                     3

Diagnostic Report                 DISABLE

Diagnostic Exercise               DISABLE
```

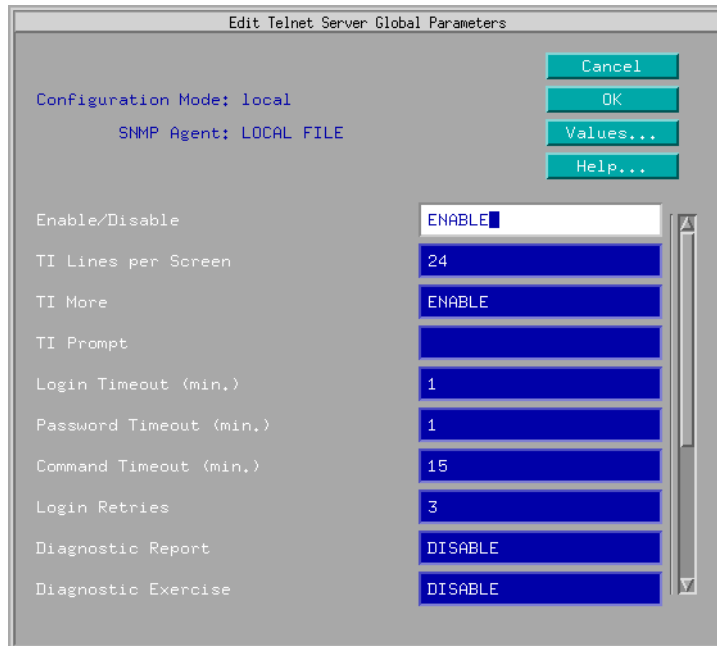**Figure 3-4.   Edit Telnet Server Global Parameters Window**

**2.   Edit the parameters in this window, using the guidelines in the next
      section.**

3.   Click on OK to save your changes and exit the window.

Telnet Server Global Parameter Descriptions

Use the following descriptions as a guide when you configure the parameters in
the Edit Telnet Server Global Parameters window.

Parameter:	**Enable/Disable**
Default:	Enable
Options:	Enable │ Disable
Function:	Specifies whether Telnet is enabled for the IP router, allowing you to establish Telnet sessions to the Technician Interface.
Instructions:	Select Enable to enable Telnet for the IP router. Select Disable to disable Telnet for the IP router.
MIB Object ID:	1.3.6.1.4.1.18.3.5.3.7.1.2

Parameter:	**TI Lines per Screen**
Default:	24 lines
Range:	1 to 24 lines
Function:	Specifies the maximum number of lines displayed on the Telnet Technician Interface console screen. The screen may override the number of lines you specify if Telnet can negotiate the window size with the remote client.
Instructions:	Set according to your console requirements.
MIB Object ID:	1.3.6.1.4.1.18.3.5.3.7.1.3

Parameter:	**TI More**
Default:	Enable
Options:	Enable │ Disable
Function:	Specifies whether the Technician Interface pauses after each screen fills with data.
Instructions:	Select Enable to configure the Technician Interface to pause after each screen fills with data. Select Disable to configure the Technician Interface not to pause after each screen fills with data.
MIB Object ID:	1.3.6.1.4.1.18.3.5.3.7.1.4

Caution: *Site Manager disconnects the current session if you modify the TI Prompt parameter.*

Parameter:	**TI Prompt**
Default:	None
Range:	1 to 18 alphanumeric characters
Function:	Specifies the character string used as the login prompt on the Telnet Technician Interface console screen.
Instructions:	Specify a character string.
MIB Object ID:	1.3.6.1.4.1.18.3.5.3.7.1.5

Parameter:	**Login Timeout (min.)**
Default:	1 minute
Range:	1 to 99 minutes (99 = infinity)
Function:	Specifies the number of minutes that can elapse before the Technician Interface disconnects the Telnet session if you do not enter a login ID at the login prompt.
Instructions:	Accept the default value (1 minute) or specify a different value.
MIB Object ID:	1.3.6.1.4.1.18.3.5.3.7.1.6

Parameter:	**Password Timeout (min.)**
Default:	1 minute
Range:	1 to 99 minutes (99 = infinity)
Function:	Specifies the number of minutes that can elapse before the Technician Interface disconnects the Telnet session if you do not enter a password at the password prompt.
Instructions:	Accept the default value (1 minute) or specify a different value.
MIB Object ID:	1.3.6.1.4.1.18.3.5.3.7.1.7

Parameter:	**Command Timeout (min.)**
Default:	15 minutes
Range:	1 to 99 minutes (99 = infinity)
Function:	Specifies the number of minutes that can elapse before the Technician Interface disconnects the Telnet session if you do not enter a command at the command prompt.
Instructions:	Accept the default value (15 minutes) or specify a different value.
MIB Object ID:	1.3.6.1.4.1.18.3.5.3.7.1.8

Parameter:	**Login Retries**
Default:	3 login attempts
Range:	1 to 99 login attempts
Function:	Specifies the maximum number of login attempts you can make before the Technician Interface disconnects the Telnet session.
Instructions:	Accept the default value (3) or specify a different value.
MIB Object ID:	1.3.6.1.4.1.18.3.5.3.7.1.9

Parameter:	**Diagnostic Report**
Default:	Disable
Options:	Enable │ Disable
Function:	Specifies whether the Technician Interface displays a record of all processing operations. Used for diagnostic purposes only.
Instructions:	Accept the default (Disable). This parameter is for field service personnel only.
MIB Object ID:	1.3.6.1.4.1.18.3.5.3.7.1.15

Parameter:	**Diagnostic Exercise**
Default:	Disable
Options:	Enable | Disable
Function:	Used for diagnostic purposes only.
Instructions:	Accept the default (Disable). This parameter is for field service personnel only.
MIB Object ID:	1.3.6.1.4.1.18.3.5.3.7.1.16

Parameter:	**Diagnostic Network Data**
Default:	Disable
Options:	Enable | Disable
Function:	Specifies whether the Technician Interface displays Telnet protocol information. Used for diagnostic purposes only.
Instructions:	Accept the default (Disable). This parameter is for field service personnel only.
MIB Object ID:	1.3.6.1.4.1.18.3.5.3.7.1.17

Parameter:	**Diagnostic PTY Data**
Default:	Disable
Options:	Enable | Disable
Function:	Specifies whether the Technician Interface displays pseudo-terminal driver (PTY) information. Used for diagnostic purposes only.
Instructions:	Accept the default (Disable). This parameter is for field service personnel only.
MIB Object ID:	1.3.6.1.4.1.18.3.5.3.7.1.18

Parameter:	**Diagnostic Options**
Default:	Disable
Options:	Enable | Disable
Function:	Specifies whether the Technician Interface displays Telnet options information. Used for diagnostic purposes only.
Instructions:	Accept the default (Disable). This parameter is for field service personnel only.
MIB Object ID:	1.3.6.1.4.1.18.3.5.3.7.1.19

Parameter:	**Manager's Login Script**
Default:	*automgr.bat*
Options:	The name of the manager's login script file.
Function:	At login, executes the manager's login script file automatically.
Instructions:	If you did not change the name of the manager's login script file, accept the default. Otherwise, enter the new name (must be eight characters or less).
MIB Object ID:	1.3.6.1.4.1.18.3.5.3.7.1.21

Parameter:	**User's Login Script**
Default:	*autouser.bat*
Options:	The name of the user's login script file.
Function:	At login, executes the user's login script file automatically.
Instructions:	If you did not change the name of the user's login script file, accept the default. Otherwise, enter the new name (must be eight characters or less).
MIB Object ID:	1.3.6.1.4.1.18.3.5.3.7.1.22

Parameter:	**Force User Logout**
Default:	Disable
Options:	Enable │ Disable
Function:	Specifies whether the user can press control-c to cancel a user autoscript at login (when a user autoscript is in effect).
Instructions:	Set the parameter to Enable to prevent using control-c to cancel the user autoscript at login.
	Set the parameter to Disable to allow the user to press control-c to cancel the user autoscript at login.
	Use the default (Disable) if you want users to access the Technician Interface. Set to Enable if you want users to enter the Telnet logout command.
MIB Object ID:	1.3.6.1.4.1.18.3.5.3.7.1.23

Parameter:	**TI History Depth**
Default:	20 commands
Range:	1 to 40 commands
Function:	Specifies the maximum number of Technician Interface commands stored in the local command history table. The table stores each command you enter at the Technician Interface prompt, on a First-In, First-Out (FIFO) basis.
Instructions:	Set the maximum number of commands that you want the router to store, for subsequent recall with the Technician Interface **history** command.
MIB Object ID:	1.3.6.1.4.1.18.3.5.3.7.1.24

Deleting a Telnet Server from the Router

To delete a Telnet Server from the entire router, follow these steps:

1. **Select Protocols➔Global Protocols➔Telnet Server➔Delete Telnet Server in the Configuration Manager window (refer to Figure 3-1).**

   Site Manager asks: Do you REALLY want to delete Telnet Server?

2. **Click on OK to delete the Telnet Server.**

Configuring and Customizing the Telnet Client

You use the Telnet Client to establish outbound Telnet sessions. Use Site Manager to create the Telnet Client, edit Telnet Client parameters, and delete the Telnet Client from the router.

Creating a Telnet Client

To create a Telnet Client on the router for outbound Telnet sessions, select Protocols➔Global Protocols➔Telnet Client➔Create Telnet Client from the Configuration Manager window (refer to Figure 3-1).

Editing Telnet Client Global Parameters

To edit Telnet Client global parameters, follow these steps:

1. **Select Protocols➔Global Protocols➔Telnet Client➔Global from the Configuration Manager window (refer to Figure 3-1).**

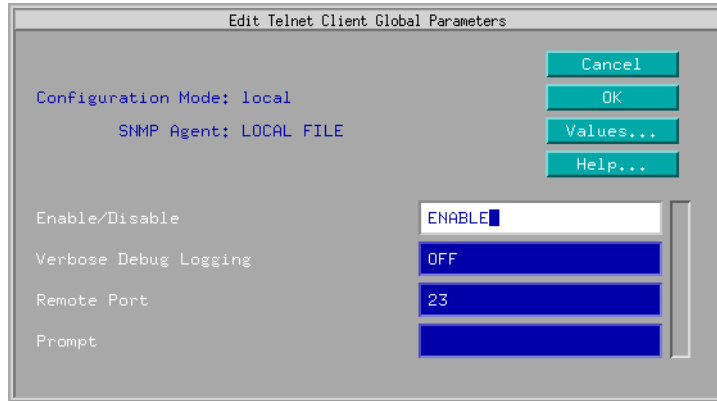   The Edit Telnet Client Global Parameters window appears (refer to Figure 3-5).

Figure 3-5.   Edit Telnet Client Global Parameters Window

2.   Edit the parameters in this window, using the descriptions in the next section as a guide.

3.   Click on OK to save your changes and exit the window.

Telnet Client Global Parameter Descriptions

Use the descriptions in this section as a guide when you configure the parameters in the Edit Telnet Client Global Parameters window (refer to Figure 3-5).

Parameter:	**Enable/Disable**
Default:	Enable
Options:	Enable	Disable
Function:	Specifies whether the Telnet Client is enabled for the IP router, allowing you to establish outbound Telnet sessions from the Technician Interface to another router or to a UNIX station that supports Telnet.
Instructions:	Select Enable to enable Telnet Client for the IP router or Disable to disable it.
MIB Object ID:	1.3.6.1.4.1.18.3.5.3.7.2.2

Parameter:	**Verbose Debug Logging**
Default:	OFF
Options:	ON │ OFF
Function:	Specifies whether the Technician Interface displays the negotiation process between the Telnet Server and Telnet Client. This parameter is for diagnostic use only.
Instructions:	Select ON to enable verbose debug logging or OFF to disable it.
MIB Object ID:	1.3.6.1.4.1.18.3.5.3.7.2.3

Parameter:	**Remote Port**
Default:	23
Options:	Any valid TCP port number.
Function:	Specifies the default remote Telnet Server's TCP port.
Instructions:	Enter the appropriate value for the default remote Telnet Server's TCP port.
MIB Object ID:	1.3.6.1.4.1.18.3.5.3.7.2.4

Parameter:	**Prompt**
Default:	None
Options:	Any text string less than 40 characters long
Function:	Specifies the default Telnet Client command prompt.
Instructions:	Enter any text string less than 40 characters long; for example, Router1%.
MIB Object ID:	1.3.6.1.4.1.18.3.5.3.7.2.5

Deleting a Telnet Client from the Router

To delete a Telnet Client from the entire router, follow these steps:

1. **Select Protocols➤Global Protocols➤Telnet Client➤Delete Telnet Client in the Configuration Manager window (refer to Figure 3-1).**

   Site Manager asks: Do you REALLY want to delete Telnet Client?

2. **Click on OK to delete Telnet Client from the router.**

Configuring and Customizing the FTP Server

Use Site Manager to create the FTP Server, edit FTP Server parameters, and delete the FTP Server from the router.

Creating an FTP Server

To create an FTP server on the router, select Protocols➜Global Protocols➜FTP➜Create FTP from the Configuration Manager window (refer to Figure 3-1).

Editing FTP Global Parameters

To edit global parameters for the FTP server, follow these steps:

1. **Select Protocols➜Global Protocols➜FTP➜Global from the Configuration Manager window (refer to Figure 3-1).**

   The Edit FTP Global Parameters window appears (refer to Figure 3-6).

Figure 3-6.   Edit FTP Global Parameters Window

2. **Edit the parameters in this window, using the descriptions in the next section as a guide.**

3. **Click on OK to save your changes and exit the window.**

FTP Global Parameter Descriptions

Use the following descriptions as a guide when you configure the parameters in the Edit FTP Global Parameters window.

Parameter:	**Enable/Disable**
Default:	Enable
Options:	Enable │ Disable
Function:	Specifies whether the FTP subsystem is enabled or disabled.
Instructions:	Specify Disabled if you want to disable FTP on the router.
MIB Object ID:	1.3.6.1.4.1.18.3.5.3.10.1.2

Parameter:	**Default Volume**
Default:	Volume 2
Options:	Volume 1 to 13, Volume A
Function:	Specifies the number of the file system volume to which FTP writes transferred files and from which FTP retrieves files for transfer.
Instructions:	On systems with a diskette, specify Volume A.
MIB Object ID:	1.3.6.1.4.1.18.3.5.3.10.1.3

Parameter:	**Login Retries**
Default:	3 retries
Options:	0 to 5 retries
Function:	Specifies the number of FTP login retries allowed after a login failure.
Instructions:	Enter a value representing the number of login attempts that FTP will accept after a login failure before rejecting logins.
MIB Object ID:	1.3.6.1.4.1.18.3.5.3.10.1.4

Parameter:	**Idle Time Out (secs)**
Default:	900 seconds
Options:	1 to 9999 seconds
Function:	Specifies the length of time (in seconds) that FTP waits before closing an idle FTP control connection.
Instructions:	Determine the maximum idle time you want to allow and specify the time value in seconds.
MIB Object ID:	1.3.6.1.4.1.18.3.5.3.10.1.5

Parameter:	**Max. Sessions**
Default:	3 sessions
Options:	1 to 10000 sessions
Function:	Specifies the maximum number of FTP sessions allowed at one time.
Instructions:	Determine the maximum number of simultaneous sessions you want to allow and specify a value.
MIB Object ID:	1.3.6.1.4.1.18.3.5.3.10.1.6

Parameter:	**Type of Service**
Default:	Binary
Options:	Binary │ ASCII
Function:	Specifies the current data transmission type.
Instructions:	To transfer files consisting of ASCII characters, specify ASCII transmission. For non-ASCII files, specify Binary.
MIB Object ID:	1.3.6.1.4.1.18.3.5.3.10.1.7

Parameter:	**Control Connection**
Default:	Low Delay
Options:	Normal │ Low Delay
Function:	Specifies the Type of Service value that FTP inserts in IP datagrams on a control connection.
Instructions:	Choose the option that determines how the Internet transport layer handles datagrams on a control connection.
MIB Object ID:	1.3.6.1.4.1.18.3.5.3.10.1.8

Parameter:	**Data Transfer**
Default:	High Throughput
Options:	Normal │ High Throughput
Function:	Specifies the Type of Service value that FTP inserts in IP datagrams on a data transfer connection.
Instructions:	Choose the option that determines how the Internet transport layer handles datagrams on a data transfer connection.
MIB Object ID:	1.3.6.1.4.1.18.3.5.3.10.1.9

Parameter:	**TCP Window Size**
Default:	60000 bytes
Range:	5000 to 64000 bytes
Function:	Specifies the size of the windows used for TCP connections.
Instructions:	Determine the window size you require and specify the size in bytes.
MIB Object ID:	1.3.6.1.4.1.18.3.5.3.10.1.10

Deleting the FTP Server from the Router

To delete the FTP server from the entire router, follow these steps:

1. **Select Protocols➔Global Protocols➔FTP➔Delete FTP in the Configuration Manager window.**

   Site Manager asks: Do you REALLY want to delete FTP?

2. **Click on OK to delete the FTP server from the router.**

Appendix A
Site Manager Default Settings

This appendix lists the default settings for Site Manager. Use the Configuration Manager to edit any of the Site Manager default settings listed here.

TCP Parameters

Table A-1 lists the Site Manager default parameter settings for the Transmission Control Protocol (TCP).

Table A-1.   TCP Configuration Parameters

Parameter	Default
Enable/Disable	Enable
Min. Retransmission Timeout	250 ms
Max. Retransmission Timeout	240000 ms
Max. Window Size	4096 bytes

Telnet Parameters

Tables A-2 and A-3 list the Site Manager default parameter settings for Telnet.

Table A-2.   Telnet Server Configuration Parameters

Parameters	Default
Enable/Disable	Enable
TI Lines per Screen	24 lines
TI More	Enable
TI Prompt	None
Login Timeout	1 minute
Password Timeout	1 minute
Command Timeout	15 minutes
Login Retries	3 login attempts
Diagnostic Report	Disable
Diagnostic Exercise	Disable
Diagnostic Network Data	Disable
Diagnostic PTY Data	Disable
Diagnostic Options	Disable
Manager's Login Script	*automgr.bat*
User's Login Script	*autouser.bat*
Force User Logout	Disable
TI History Depth	20 commands

Table A-3.   Telnet Client Configuration Parameters

Parameters	Default
Enable/Disable	Enable
Verbose Debug Logging	OFF
Remote Port	23
Prompt	None

FTP Parameters

Table A-4 lists the Site Manager default parameter settings for the File Transfer Protocol (FTP).

Table A-4.   FTP Configuration Parameters

Parameters	Default
Enable/Disable	Enable
Default Volume	Volume 2
Login Retries	3 retries
Idle Time Out	900 seconds
Max Sessions	3 sessions
Type of Service	Binary
Control Connection	Low delay
Data Transfer	High Throughput
TCP Window Size	16000 bytes

Index

Max. Sessions parameter, 3-21

Max. Window Size parameter, 3-6

memory
    and number of Telnet connections, 1-5
    considerations for configuring TCP, 2-1

Min. Retransmission Timeout parameter, 3-5

O

outbound Telnet, 1-5, 3-16. *See also* Telnet client

out-of-order caching, 1-2

P

Parameters. *See* individual names

Password Timeout parameter, 3-11

ports, 1-3

Prompt parameter, 3-18

R

reference material, 1-8

Remote Port parameter, 3-18

S

sequence numbers, 1-1

Simple Network Management Protocol (SNMP),
        1-5

sockets, 1-3

T

TCP
    clients, 1-2, 1-4
    connection states, 1-3 to 1-4
    connections for, 1-2
    creating, 3-2
    deleting from the router, 3-6

editing parameters for, 3-3
memory considerations, 2-1
overview of, 1-1 to 1-4
ports, 1-3

TCP global parameters, 3-4 to 3-6
    descriptions of, 3-4 to 3-6
    editing, 3-3
    Enable/Disable, 3-4
    Max. Retransmission Timeout, 3-5
    Max. Window Size, 2-1, 3-6
    Min. Retransmission Timeout, 3-5

TCP Window Size parameter, 3-23

Technician Interface, 1-5

Telnet, 1-4 to 1-5

Telnet client, 1-4
    command prompt, 3-18
    creating, 3-16
    deleting from the router, 3-18
    editing parameters for, 3-16 to 3-17
    parameter descriptions for, 3-17 to 3-18

Telnet client global parameters, 3-17 to 3-18
    editing, 3-16 to 3-17
    Enable/Disable, 3-17
    Prompt, 3-18
    Remote Port, 3-18
    Verbose Debug Logging, 3-18

Telnet configuration parameters, 3-7 to 3-8
    Force User Logout, 3-8
    Manager's Login Script, 3-7
    User's Login Script, 3-8

Telnet server, 3-6 to 3-16
    creating, 3-6
    deleting from the router, 3-16
    editing parameters for, 3-8 to 3-9

Telnet server global parameters
    Command Timeout, 3-12
    Diagnostic Exercise, 3-13
    Diagnostic Network Data, 3-13
    Diagnostic Options, 3-14
    Diagnostic PTY Data, 3-13
    Diagnostic Report, 3-12
    Force User Logout, 3-15

U

V

W