

Using Norton pcANYWHERE™ for Windows



Using Norton pcANYWHERE™ for Windows

The software described in this book is furnished under a license agreement and may be used only in accordance with the terms of the agreement.

Copyright Notice

Copyright © 1993–1994 Symantec Corporation. All Rights Reserved.

No part of this publication may be copied without the express written permission of Symantec Corporation, Peter Norton Group, 10201 Torre Avenue, Cupertino, CA 95014.

Trademarks

Symantec and pcANYWHERE are trademarks of Symantec Corporation.

Windows is a trademark of Microsoft Corporation. Other product names mentioned in this manual may be trademarks or registered trademarks of their respective companies and are hereby acknowledged.

Printed in the United States of America.

10 9 8 7 6 5 4 3 2 1

Symantec Service and Support Solutions

Symantec is committed to excellent service worldwide. Our goal is to provide you with professional assistance in the use of our software and services, wherever you are located.

Technical Support and Customer Service solutions vary by country. If you have questions about the services described below, please refer to the section “Worldwide Service and Support” at the end of this chapter.

Registering your Symantec product

To register your Symantec product, please complete the registration card included with your package and drop the card in the mail. You can also register via modem during the installation process (if your software offers this feature) or via fax to (800) 800-1438 or (541) 984-8020.

Technical support

Symantec offers several technical support options designed for your individual needs to help you get the most out of your software investment.

World Wide Web

The Symantec World Wide Web site offers a complete online technical support solution. Point your Web browser to sos.symantec.com

FTP

Point your Web browser to sos.symantec.com/ftp/index.html to search for and download technical notes and software patches.

You can also click the LiveUpdate button (if your software offers this feature), to automatically download and install software patches and virus definitions.

America Online

On AOL, enter Keyword: SYMANTEC to join the Symantec forum. For AOL subscription information: U.S. and Canada dial (800) 227-6364.

CompuServe

GO SYMANTEC to join the Symantec forums.
For CompuServe subscription information:
U.S. and Canada dial (800) 848-8199.
All other locations dial +1 (614) 718-2800.

Symantec BBS

To connect to the Symantec BBS, set your modem to 8 data bits, 1 stop bit, no parity and dial (541) 484-6669.

Automated fax retrieval system

To receive general product information, fact sheets and product upgrade order forms directly to your fax machine, please call our Customer Service fax retrieval system at (800) 554-4403 or (541) 984-2490.

For technical application notes, please call our Technical Support fax retrieval system at (541) 984-2490 and select option 2.

StandardCare Support

90 days of telephone technical support (from the date of your first call) at no charge to all registered users of Symantec software.

Please see the back of this manual for the support telephone number for your product.

PriorityCare and PremiumCare Support

Expanded telephone support services available to all registered customers. For complete information, please call our automated fax retrieval service, located in the United States, at (800) 554-4403 or (541) 984-2490, and request document 070, or visit sos.symantec.com/telesupp.html

Support for old and discontinued versions

When a new version of this software is released, registered users will receive upgrade information in the mail. Telephone support will be provided for the previous version for 6 months after the release of the new version. Technical information may still be available through online support.

When Symantec announces that a product will no longer be marketed or sold, telephone support will be discontinued 60 days later. Support will only be available for discontinued products through online services. See the section "Technical Support" for online service options.

Customer Service

Symantec's Customer Service department can assist you with non-technical questions. Call Customer Service to:

- Order an upgrade.
- Subscribe to the Symantec Support Solution of your choice.
- Fulfill your request for product literature or demonstration disks.
- Find out about dealers and consultants in your area.
- Replace missing or defective CDs, disks, manuals, etc.
- Update your product registration with address or name changes.

You can also visit Customer Service online at www.symantec.com/custserv for the latest Customer Service FAQs, to find out the status of your order or return, or to post a query to a Customer Service discussion group.

Worldwide Service and Support

Symantec provides Technical Support and Customer Service worldwide. Services vary by country and include International Partners who represent Symantec in regions without a Symantec office. For general information, please contact the Symantec Service and Support Office for your region.

Service and Support offices

NORTH AMERICA

Symantec Corporation	(800) 441-7234 (USA & Canada)
175 W. Broadway	(541) 334-6054 (all other locations)
Eugene, OR, 97401	Fax: (541) 984-8020

Automated Fax Retrieval	(800) 554-4403
	(541) 984-2490

BRAZIL

Symantec Brazil	+55 (11) 5561 0284
Av. Juruca, 302 - cj 11	Fax: +55 (11) 5530 8869
São Paulo - SP	
04080 011	
Brazil	

EUROPE

Symantec Europe Ltd. +31 (71) 535 3111
Kanaalpark 145 Fax: +31 (71) 535 3150
2321 JV Leiden
The Netherlands

Automated Fax Retrieval +31 (71) 535 3255

ASIA/PACIFIC RIM

Symantec Australia Pty. Ltd. +61 (2) 9850 1000
408 Victoria Road Fax: +61 (2) 9850 1001
Gladesville, NSW 2111
Australia

Automated Fax Retrieval +61 (2) 9817 4550

Most International Partners provide Customer Service and Technical Support for Symantec products in your local language. For more information on other Symantec and International Partner locations, please call our Technical Support automated fax retrieval service, in the United States at +1 (541) 984-2490, choose Option 2, and request document 1400.

Every effort has been made to ensure the accuracy of this information. However, the information contained herein is subject to change without notice. Symantec Corporation reserves the right for such change without prior notice.

SYMANTEC LICENSE AND WARRANTY

The software which accompanies this license (the "Software") is the property of Symantec or its licensors and is protected by copyright law. While Symantec continues to own the Software, you will have certain rights to use the Software after your acceptance of this license. Except as may be modified by a license addendum which accompanies this license, your rights and obligations with respect to the use of this Software are as follows:

- You may:

- (i) use one copy of the Software on a single computer;
- (ii) make one copy of the Software for archival purposes, or copy the software onto the hard disk of your computer and retain the original for archival purposes;
- (iii) use the Software on a network, provided that you have a licensed copy of the Software for each computer that can access the Software over that network;
- (iv) after written notice to Symantec, transfer the Software on a permanent basis to another person or entity, provided that you retain no copies of the Software and the transferee agrees to the terms of this agreement; and
- (v) if a single person uses the computer on which the Software is installed at least 80% of the time, then after returning the completed product registration card which accompanies the Software, that person may also use the Software on a single home computer.

- You may not:

- (i) copy the documentation which accompanies the Software;
- (ii) sublicense, rent or lease any portion of the Software;
- (iii) reverse engineer, decompile, disassemble, modify, translate, make any attempt to discover the source code of the Software, or create derivative works from the Software; or
- (iv) use a previous version or copy of the Software after you have received a disk replacement set or an upgraded version as a replacement of the prior version, unless you donate a previous version of an upgraded version to a charity of your choice, and such charity agrees in writing that it will be the sole end user of the product, and that it will abide by the terms of this agreement. Unless you so donate a previous version of an upgraded version, upon upgrading the Software, all copies of the prior version must be destroyed.

- Sixty Day Money Back Guarantee:

If you are the original licensee of this copy of the Software and are dissatisfied with it for any reason, you may return the complete product, together with your receipt, to Symantec or an authorized dealer, postage prepaid, for a full refund at any time during the sixty day period following the delivery to you of the Software.

- Limited Warranty:

Symantec warrants that the media on which the Software is distributed will be free from defects for a period of sixty (60) days from the date of delivery of the Software to you. Your sole remedy in the event of a breach of this warranty will be that Symantec will, at its option, replace any defective media returned to Symantec within the warranty period or refund the money you paid for the Software. Symantec does not warrant that the Software will meet your requirements or that operation of the Software will be uninterrupted or that the Software will be error-free.

THE ABOVE WARRANTY IS EXCLUSIVE AND IN LIEU OF ALL OTHER WARRANTIES, WHETHER EXPRESS OR IMPLIED, INCLUDING THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. THIS WARRANTY GIVES YOU SPECIFIC LEGAL RIGHTS. YOU MAY HAVE OTHER RIGHTS, WHICH VARY FROM STATE TO STATE.

- Disclaimer of Damages:

REGARDLESS OF WHETHER ANY REMEDY SET FORTH HEREIN FAILS OF ITS ESSENTIAL PURPOSE, IN NO EVENT WILL SYMANTEC BE LIABLE TO YOU FOR ANY SPECIAL, CONSEQUENTIAL, INDIRECT OR SIMILAR DAMAGES, INCLUDING ANY LOST PROFITS OR LOST DATA ARISING OUT OF THE USE OR INABILITY TO USE THE SOFTWARE EVEN IF SYMANTEC HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

SOME STATES DO NOT ALLOW THE LIMITATION OR EXCLUSION OF LIABILITY FOR INCIDENTAL OR CONSEQUENTIAL DAMAGES SO THE ABOVE LIMITATION OR EXCLUSION MAY NOT APPLY TO YOU.

IN NO CASE SHALL SYMANTEC'S LIABILITY EXCEED THE PURCHASE PRICE FOR THE SOFTWARE. The disclaimers and limitations set forth above will apply regardless of whether you accept the Software.

- U.S. Government Restricted Rights:

RESTRICTED RIGHTS LEGEND. Use, duplication, or disclosure by the Government is subject to restrictions as set forth in subparagraph (c) (1) (ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.227-7013 or subparagraphs (c) (1) and (2) of the Commercial Computer Software-Restricted Rights clause at 48 CFR 52.227-19, as applicable, Symantec Corporation, 10201 Torre Avenue, Cupertino, CA 95014.

- General:

This Agreement will be governed by the laws of the State of California. This Agreement may only be modified by a license addendum which accompanies this license or by a written document which has been signed by both you and Symantec. Should you have any questions concerning this Agreement, or if you desire to contact Symantec for any reason, please write:

Symantec Customer Service, 175 W. Broadway,
Eugene, OR 97401.

Contents

About This Guide

Assumptions	15
Conventions	16

Chapter 1 Welcome to Norton pcANYWHERE

What PCs Can Run Norton pcANYWHERE?	17
What Is Remote Control?	18
What Is an Online Service?	19
How Does the Remote PC Connect to the Host PC or Online Service?	19
How Does pcANYWHERE Know What Kind of Connection to Make?	20
Can I Track What Happens During a Session?	21
Can I Automate Repetitious Procedures?	22
Quick Start	22
Connecting via Modems	23
Connecting Over a LAN	25
What's New in Version 2.0?	27
Converting pcANYWHERE Version 1.0's Configuration Files	28
Accessing Program Modules	30

Chapter 2 Installation and General Setup

Installing Norton pcANYWHERE on a Standalone PC	33
Licensing Norton pcANYWHERE	34
Specifying the Program Directory	34
Changes to Your System Files	36
Registering Electronically	36
Starting Norton pcANYWHERE	37
Installing Norton pcANYWHERE on a LAN	38
Licensing Norton pcANYWHERE	42
Specifying the Program Directory	43
Specifying Data File Management	44
Creating Shared Configuration Data Files	45
Installing Norton pcANYWHERE on Network Workstations	47
Changes to Your System Files	47
Customizing Norton pcANYWHERE Host Installation	48
Uninstalling Norton pcANYWHERE	48
Adjusting Your AUTOEXEC.BAT File	49
Starting Norton pcANYWHERE	49
Using Cue Cards and The Norton Assistant	50

Chapter 3 Hardware Configurations

Creating a Modem Hardware Configuration	53
Adjusting Advanced Hardware Options	56
Creating a Direct Serial Hardware Configuration	57
Creating a Leased-Line Hardware Configuration	59
Creating an Interrupt 14 Hardware Configuration	62
Creating Network Hardware Configurations	64
Creating a Node Hardware Configuration	65
Creating ACS Hardware Configurations	67
Using TCP/IP Protocol	73
Customizing the Command Set for Your Modem	73

Chapter 4 Gateways

Gateway Concepts	75
Configuring Gateways	77
Modifying Gateway Settings	79
Loading the Gateway TSR	79

Chapter 5 Configuring Norton pcANYWHERE

Setting Options in the Configure Menu	81
Defining Your Computer's Name and Security Level	82
Setting Up Host Operations	85
Configuring Host Options	85
Configuring Caller Information	92
Remote Operations	98
Adding TCP/IP Hosts	100
Creating a List of Host PCs	102
Mapping Drives	104

Chapter 6 Starting a Remote Control Session

Starting the Host PC	107
Initiating the Session from the Host PC	109
Using Quick Connect to Load a Host	112
Canceling a Host Session	114
Loading the DOS Host TSR	115
Starting the Remote	116
Initiating the Session from the Remote PC	116
Using Quick Connect to Connect with a Host	118
Connecting through a Gateway	120
Using an Incoming Gateway	120
Using an Outgoing Gateway	122

Chapter 7 Online Services

Customizing Terminal Emulation	125
Configuring Terminal Settings	126
Setting Up Macro Keys	128
Setting Up Translation Tables	130
Customizing Font and Colors	132
Calling an Online Service	133
Creating a List of Online Services	133
Advanced Online Session Options	135
Starting an Online Session	137
Connecting Through a pcANYWHERE Gateway	138
Using Quick Connect for Online Sessions	140

Chapter 8 Managing Remote Control and Online Sessions

Managing the Remote Control Session	143
Using Online Menu Options Available to Host and Remote	143
Using Remote Online Menu Options	147
Using Host Online Menu Options	158
Transferring Files during a Remote Control Session	158
Controlling Online Service Sessions	159
Running Scripts	159
Printing from the Terminal Window	160
Editing Terminal Window Text	160
Adjusting Session Options	161
Ending an Online Service Session	164
Transferring Files to and from an Online Service	164
Selecting Protocol Options	166
Uploading and Downloading Files	166

Chapter 9 File Transfer

Using the Norton pcANYWHERE File Manager	169
Selecting Files and Directories	170
Deselecting Files	172
Sending Files	172
Transferring the Clipboard	175
Viewing Clipboard Contents	176
Managing Directories and Files	177
Making Directories	178
Deleting Files and Directories	178
Renaming Files and Directories	179
Copying Files	180
Comparing Directories	181

Synchronizing and Cloning Directories	182
Setting File Manager Options	185
Selecting File Sorting Options	185
Selecting File Details Options	186
Selecting File Transfer Options	186

Chapter 10 Utilities

Capturing Remote Control and Online Session Information	189
Recording Sessions	189
Playing Back Recorded Sessions	193
Copying a Recorded Session to Another File	196
Saving Screen Shots	197
Saving Screens from Record Files	198
Displaying Screen Shots	199
Saving Screens as Plain Text	200
Logging Remote Control and Online Sessions	200
Creating an Activity Log Report	202
Deleting and Archiving Logged Information	205
Creating Activity Reports Using Archived Data	206

Appendix A Technical Information

The Role of the PC	207
Serial Port Addressing	207
Hardware Interrupts	208
UARTs	209
The Role of the Modem	210
Speed	210
Data Compression	211
Modem Commands	211
Modem Switches	212
Using the PC and the Modem Together	213
Data Rate	213
Flow Control	213
Standard Serial Cables (RS-232-C)	214
Null Modem Cables	216
Special Telephone Lines	217
Error Detection and Correction	220
Serial Hardware Configurations	221
Miscellaneous Modem Hardware Configuration Options	222
Norton pcANYWHERE for Windows Command Lines	223
Command-Line Arguments	223
Command-Line Options	224
Command Line Examples	225

Windows Communication with OLE and Visual Basic	226
Object Linking and Embedding (OLE 2) Automation Support	226
Using Visual Basic as an OLE Controller	227

Appendix B Terminal Emulation

Terminal Emulation Keys	229
ADDS Viewpoint	230
ADM 3A	230
ANSI	231
DG 100/200	232
Hazeltine 1500	235
IBM 3101	235
Televideo 912/920	236
Televideo 925	238
VT 100/102/220	240
VT 52	243
Wyse 50	244
X3270	247
Translation Table Codes	249
The ASCII Character Set	249
Converting Decimal Numbers to Hex	252

Appendix C Troubleshooting

Interpreting Error Messages	253
Solving Problems	261
Serial Communications	261
Keyboard	264
DOS Graphics	264
Remote Printing	265

Glossary

Index

About This Guide

Welcome to Norton pcANYWHERE for Windows, version 2.0.

Chapter 1, “Introduction,” provides an overview, a Quick Start section for experienced software users, and information important to users of earlier version of Norton pcANYWHERE for Windows. For example, it explains how configuration files from version 1.0 can be converted for use with version 2.0.

Chapters 2 through 5 explain how to install and configure pcANYWHERE. Chapters 6 through 9 guide you through sessions in which you remotely control another PC or communicate with an online service. Chapter 10 explains a number of utilities provided with Norton pcANYWHERE for Windows.

At the back of the guide are three appendices that provide technical and troubleshooting information and a glossary of terms used in the guide.

Assumptions

This manual assumes that you know how to use Windows 3.1 and higher. If you are not familiar with such Windows terms as “dialog boxes,” “icons,” “option buttons,” and “list boxes,” you’ll find this manual easier to understand if you first read Microsoft’s booklet entitled “Getting Started with Microsoft Windows.”

This manual assumes that you are using a right-handed mouse, with the left button being the primary button. Whenever you are instructed to click or double-click an item, you should use the left button. (Remember, you can always configure your mouse for left-handed use—making the right mouse button the primary button—by using the Windows Control Panel. See the *Microsoft Windows User’s Guide* for more information and details about navigation and selection techniques.

Conventions

To help you find information easily, the Norton pcANYWHERE documentation set adheres to the following conventions:

ALL CAPS	Path, directory, or file.
Initial Caps	Interface objects, such as menus, dialog boxes, or options.
SMALL CAPS	Pull-down menu commands.
Key+Key	Key combination: you hold down the first key and press the second key.
monospaced	Something you enter from the keyboard.
[parameter]	Optional command syntax. Do not enter the brackets themselves.
parameter parameter	“Or.” You can use only one option.
choose	Indicates that you highlight a menu command using the mouse or keyboard, then click or press Enter to activate the command.
enter	Indicates that you type text, then press the Enter key.
select	Indicates that you highlight a dialog box option using the mouse or keyboard.

NOTE: Notes clarify discussions.

TIP: Tips are hints about the outcome of procedures or shortcuts you can use to perform them.

CAUTION: Cautions alert you to conditions that could cause unexpected but non-destructive results.

WARNING: Warnings alert you to conditions that could result in data loss or corruption.

Welcome to Norton pcANYWHERE



Norton pcANYWHERE for Windows is a complete, high-speed communications solution for standalone PCs and for PCs on local area networks (LANs). Norton pcANYWHERE allows you to:

- Remotely control one PC from another, when both PCs are running pcANYWHERE software.
- Use your PC to communicate with a variety of computers that provide services you are interested in but which are not running pcANYWHERE software.

You can make a connection via telephone lines, a network, or a combination of the two. Norton pcANYWHERE solves both your remote control and general communications needs. For example, you may want to transfer files from one computer to the other, check an electronic bulletin board for information, or access electronic mail.

This chapter:

- Explains the concepts *remote control* and *online service*
- Provides an overview of the configuration information needed to connect two computers
- Provides an overview of many of Norton pcANYWHERE's features
- Lists the features that are new in this release
- Lists the changes that users of previous releases need to be aware of

What PCs Can Run Norton pcANYWHERE?

Requirements to run Norton pcANYWHERE are:

- A 386SX or higher
- MS/DOS 3.3 or higher
- Windows 3.1 or higher
- At least 2 MB available RAM

Norton pcANYWHERE currently supports the Novell NetWare IPX network protocol as well as NetBIOS (a standard networking protocol introduced by IBM), Banyan VINES, TCP/IP (Transmission Control Protocol/Internet Protocol) Winsock 1.1-compliant, NASI/NCSI, and Telebit ACS. Banyan VINES should be version 5.0 or greater.

What Is Remote Control?

Remote control is the method by which one PC controls another. Usually the two PCs are at different locations. For example, you can use a laptop in New York to connect with and operate a PC in Los Angeles. The laptop you are using in New York is referred to as the *remote PC* and you are the *remote user*. The PC you are accessing in Los Angeles is referred to as the *host PC*. Its user, if there is one present, is called the *host user*. You have access to any information available to the PC in Los Angeles as if you were sitting in front of that PC. An image of the host PC's screen or desktop appears on your laptop. By using drive mapping, the drives on your laptop can appear as additional drives on the PC in Los Angeles. You use Norton pcANYWHERE on each PC to set it up as either the remote or host PC.

What are the benefits of remote control?

- You can use your office PC even when you are not in the office. If you travel as part of your job or work from home, you may need to connect with your office PC to check electronic mail, add sales or other information to a database, or download a file you forgot to take with you. In this scenario, the office PC is the host PC, and your home PC or your on-the-road laptop is the remote PC. Norton pcANYWHERE sends information through the modems, telephone lines, and/or networks that connect the two PCs. pcANYWHERE sends your keystrokes and mouse movements from the remote to the host where they are processed. It then sends the screen image from the host to the remote.
- Several people can access the same PC from remote locations—although not at the same time. For example, field personnel can access a central database located at the office.
- As a consultant, you can use your office PC to access, troubleshoot, and update applications on a client's PC.
- If you manage computers or networks, you can use Norton pcANYWHERE to operate a user's PC. This saves you a trip to the user's office, which may not be in the same building or even the same city. You can then fix the user's problem. Or you can educate a

user about fixing his or her own problem by connecting to the user's PC via the network and calling the user over the phone to explain step-by-step what you are doing. You can also transfer files from one PC to the other.

- If you do technical support or training, you can monitor the actions of customers or students long-distance, operate their PCs when necessary, and so forth. You can use voice-first or the chat window to communicate verbally as well. You can also transfer updates to customers or information to students.

What Is an Online Service?

An *online service* is a service such as CompuServe, Dow Jones, MCI Mail, or an electronic bulletin board. The service may be on another PC, a mainframe, or a minicomputer. Online services offer information on a vast variety of topics. Each service usually has its own set of procedures by which you identify yourself and log on. Norton pcANYWHERE supports several terminal emulation types and file-transfer protocols commonly used by online services. Each service will tell you which of these to use.

When you connect to a service via Norton pcANYWHERE, you are the remote user and your PC is the remote PC. However, the online service is not a host PC. Your PC does not display an image of the host's screen nor does it control the host. Your PC simulates (emulates) the type of terminal required to gain access to the host. Your PC is in terminal mode, an operating mode for transmitting keystrokes and receiving transmitted data. You see the commands you type and the data sent as a response from the host.

How Does the Remote PC Connect to the Host PC or Online Service?

Two computers can be connected:

- Over telephone lines via modems. This is called a *serial connection*.

A *modem* is a communications device that enables a computer to transmit information over a standard telephone line. One modem converts computer data to analog signals for transmission over telephone lines (modulates), and another modem converts those signals back to computer data at the other end (demodulates). Modems can transmit at different speeds or data transfer rates. The two modems mutually determine and then use the highest speed available to both of them.

- Directly by a null modem cable. This is called a *direct serial connection*.

A *null modem cable* is a serial cable that has been modified to allow it to connect two computers directly, eliminating the need for a modem. (See Appendix A, “Technical Information” for information on null modem cables.)

- Across a local area network (LAN), such as Novell NetWare. This is called a network connection.
- Over telephone lines and across a LAN using a pcANYWHERE gateway or asynchronous communications server (ACS).

A pcANYWHERE *gateway* is a small memory-resident program (TSR) that resides on a network station with two Norton pcANYWHERE compatible communications devices, such as a modem and a network interface card. pcANYWHERE gateways allow users to share a modem on a network, so that each user does not need an individual modem.

An *asynchronous communications server (ACS)* is a communications server that manages a pool of modems. It directs outgoing messages to the next available modem and directs incoming messages to the appropriate PC.

How Does pcANYWHERE Know What Kind of Connection to Make?

To make the connection between the remote PC and the host PC or online service, Norton pcANYWHERE needs to know:

- The *name* that identifies your PC to other PCs running Norton pcANYWHERE.
- The *hardware configuration* that specifies the device used to make the connection and their settings. You will have more than one hardware configuration if you can connect using more than one combination of hardware (although you can use only one configuration at a time). For example, you may use a modem hardware configuration to reach one computer and a network hardware configuration to reach another. See Chapter 3, “Hardware Configurations.”

Before connecting to an online service, the remote PC specifies which hardware configuration it intends to use.

- A *session configuration* that specifies all the information Norton pcANYWHERE needs to start either a remote control session or an online session. For example, you may include the telephone number for the computer to which the remote PC will connect. The session configuration includes a hardware configuration as one of its settings. In general, you create a session configuration for each computer you access regularly. A session configuration for a host PC has different options than a session configuration for an online service.
- *Caller privileges* that list the remote PCs from which your PC, when serving as a host, will accept a connection. Caller privileges also specify how the remote user can interact with the host. Different users can have different levels of access. If you do not select the Individual Privileges option, the settings configured in the Default Privileges dialog box will be used for all remote callers. See “Setting up a Host” in Chapter 5.
- A *Quick Connect feature* that allows you to specify a simple, minimal connection on either the host or remote PC. Quick Connect is further explained in Chapter 6, “Starting a Remote Control Session,” and Chapter 7, “Online Services.” If you plan to access a host or online service on a regular basis, it is more convenient to create the hardware, session, and caller information configurations for the particular host or online service.

Can I Track What Happens During a Session?

Norton pcANYWHERE allows you to track and troubleshoot sessions by logging connection attempts and recording all or parts of sessions. See Chapter 10, “Utilities,” for details.

You can log connections made to or from remote and host PCs. You can log all sessions or only specific sessions. Different information is stored in a host log than in a remote log. For example, the log for the remote PC can document connections to both host PCs and online services. Once a log file is created, you can view the information, create and print reports using specific criteria, and archive logged data in history files.

Also, with an online session (a session with a bulletin board service, information service, minicomputer, or mainframe), Norton pcANYWHERE allows you to capture host screens, cut-and-paste, and print from the terminal window.

Recorded sessions can be saved in a record file, which is real-time recording similar to a movie, or in a screen file, which contains recorded screens similar to a series of snapshots. Playback options allow you to control how you view a recorded session; for example, you can adjust the playback's speed.

Can I Automate Repetitious Procedures?

Norton pcANYWHERE includes a script language that allows you to perform operations automatically when calling online services. Additional commands in the script language allow you to automate some operations during remote control sessions. Scripts are saved in script files then executed either automatically upon beginning a session or anytime that you choose to execute one during a session. Script files allow you to automate tasks such as running programs, transferring files, performing arithmetic operations, and much more. In addition, an option is available that allows you to create a script by recording the activities of your session to a script file. (See Chapter 8, "Managing Remote Control and Online Sessions," for information on recording script files.)

Also included is a script builder tool, which is an editor that simplifies the task of creating and editing script files. Part of the script builder is a script reference dialog box that lists all script commands and provides a brief description of each one. You can use the reference dialog box to choose commands with which to build a script. For details, see the technical reference guide for the script language, *Creating Norton pcANYWHERE Scripts*.

Quick Start

This section shows you how to start a remote control session between two PCs connected by modems or two PCs on the same LAN. It provides minimal configuration information and is written for experienced software users too impatient to read the entire user's guide. It assumes that you will want to communicate with more than one other PC, so it does not use the Quick Connect feature. It also assumes that you will read the other chapters to learn about capabilities and functions of pcANYWHERE not described here. For example, several security features on the host PC may be important to you.

If you find you need more detailed information about configuration or connection procedures than is offered in this Quick Start section, please read the appropriate chapters of this manual before proceeding.

Connecting via Modems

The following procedures explain how to set up a remote control session for two PCs, each of which is using its modem as the communications device.

Perform the first procedure on both the host and remote PCs. The second procedure is just for the host, and the third procedure is just for the remote.

To set up the host and remote PC:

- 1 Insert Disk 1 of the installation diskettes into your computer's floppy disk drive.
- 2 Make sure that Windows (version 3.1 or later) is running on your computer or workstation. Choose RUN... from the File menu of Program Manager or Norton Desktop and type A:Install.EXE or B:Install.EXE in the text box.
- 3 Click OK. Change disks when prompted and select the Restart Windows option at the end of the installation.
- 4 Open the pcANYWHERE program group and double-click the pcANYWHERE icon.

The pcANYWHERE main window appears.

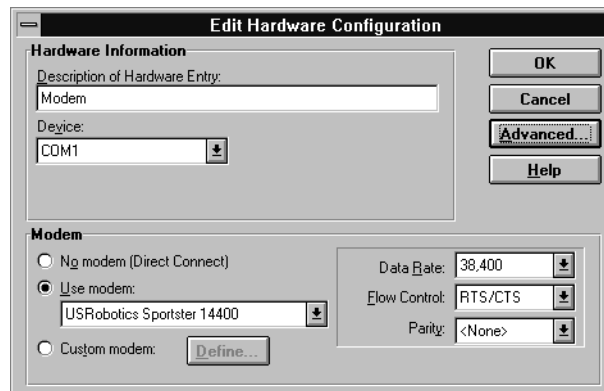
- 5 Choose SYSTEM HARDWARE... from the Configure menu.

The Configure System Hardware dialog box appears.

- 6 Click the Modem entry then click the Edit... button.

The Edit Hardware Configuration dialog box appears (Figure 1-1).

Figure 1-1 The Edit Hardware Configuration dialog box contains all the settings required for a modem connection.



- 7 Select the communications port, (COM1 through COM4), to which your modem is attached from the Device drop-down list box in the Hardware Information group box.

NOTE: The port you identified in the Smart Setup dialog box is listed. For details, see “What’s New in Version 2.0?” later in this chapter.

- 8 Select the Use Modem option button in the Modem group box.
- 9 Select the name of your modem from the Use Modem drop-down list box. If the name of your modem does not appear in the list, consult your modem’s manufacturer for an alternative choice or choose Hayes Compatible.
The data rate is set automatically based on the modem selected.
- 10 Click OK to save the settings and return to the Configure System Hardware dialog box.
- 11 Click Close to return to the pcANYWHERE main window.

To continue setting up a host PC:

- 1 Click the Be A Host PC load button.
- 2 Select the Modem entry from the drop-down list box in the Your Hardware Configuration Name group box.
- 3 Click the Wait for Call button.

The pcANYWHERE waiting icon appears. The host is ready to accept a call.

To continue setting up a remote PC:

- 1 Click the Call A Host PC load button.
- 2 Select the pcANYWHERE Host via Modem entry and click the Call button.
The pcANYWHERE Waiting... dialog box appears.
- 3 Type in the phone number of the host PC in the Phone Number text box.
- 4 Click OK. pcANYWHERE dials the number.

If the connection is successful, an image of the host screen appears on your PC. Your keystrokes and mouse movements are sent to and processed by the host PC. You can double-click the pcANYWHERE [In Session] Icon to access the Online Menu.

Connecting Over a LAN

The following procedures explain how to set up a remote control session for two PCs on the same LAN (Local Area Network). It assumes that your network administrator has installed Norton pcANYWHERE on the network. It further assumes that you can define your own hardware and session configurations. However, your administrator may have set these up for you, and you may not have the network or pcANYWHERE rights necessary to change them.

Perform the first procedure on both the host and remote PCs. The second procedure is just for the host, and the third procedure is just for the remote.

To set up the host and remote PC:

- 1 Log on to the network.
- 2 Choose RUN... from the File menu of the Program Manager or the Norton Desktop main window.
- 3 Type *netpathname*\INSTALL in the Command Line text box.
- 4 Click OK.

(Replace *netpathname* with the network drive and directory that contains the Norton pcANYWHERE program files.)

- 5 Select the Restart Windows option at the end of the installation.
- 6 Open the pcANYWHERE program group and double-click the pcANYWHERE icon.

Every time you access a network installation of Norton pcANYWHERE, you must enter a personal ID (up to six characters.) Use the same ID each time you run pcANYWHERE.

The pcANYWHERE main window appears.

- 7 Choose SYSTEM HARDWARE... from the Configure menu.
The Configure System Hardware dialog box appears.
- 8 Click the Network entry then click the Edit... button.
The Edit Hardware Configuration dialog box appears (see Figure 1-1).
- 9 Select the correct network driver (NetWare IPX, NetBIOS, or Banyan) from the Device drop-down list box.
- 10 Click OK to save the settings and return to the Configure System Hardware dialog box.
- 11 Click Close to return to the pcANYWHERE main window.

- 12 Choose SYSTEM SETUP... from the Configure menu.
The System Setup dialog box appears.
- 13 Type a computer name for your PC that will uniquely identify this computer. (The remote user needs to know the name given the host PC.)
- 14 Click OK to save the settings and return to the pcANYWHERE main window.

To continue setting up a host PC:

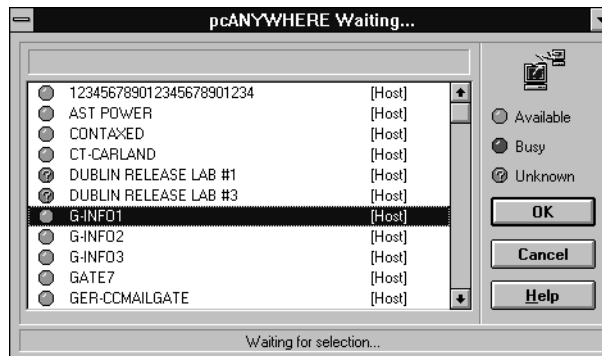
- 1 Click the Be A Host PC load button.
- 2 Select the Network entry from the drop-down list box in the Your Hardware Configuration Name group box.
- 3 Click the Wait for Call button.
The pcANYWHERE waiting icon appears. The host is ready to accept a call.

To continue setting up a remote PC:

- 1 Click the Call A Host PC load button.
- 2 Select the pcANYWHERE Host via Network entry and click the Call button.

The pcANYWHERE Waiting... dialog box appears listing all available hosts (Figure 1-2).

Figure 1-2 On the screen, a green light indicates the host is available and is waiting for a call.



- 3 Select the host name from the list.
- 4 Click OK.

If the connection is successful, an image of the host screen appears on the remote PC. Your keystrokes and mouse movements are sent to and processed by the host PC. You can double-click the pcANYWHERE [In Session] icon to access the Online Menu.

What's New in Version 2.0?

The features that are new in Norton pcANYWHERE for Windows, version 2.0 are:

- Installation—the Norton pcANYWHERE install program does not change your Windows' keyboard, mouse or display drivers.
- Smart Setup—You are asked to enter a computer name, modem type, serial port, and network the first time you run pcANYWHERE. The information provided becomes the default settings.
- Clipboard transfer—Text or graphics contained in either the host's or remote's Clipboard can now be transferred during a remote computing session.
- Drive and file synchronization, cloning, and comparing—Synchronization, cloning, and comparing allow automatic duplication and verification of host and remote drives and files.
- Remote drive mapping—This allows drives on the remote PC to be accessed during a remote control session. By mapping the remote's drives to an available drive on the host, the remote's drives appear as additional drives on the host PC.
- Bidirectional gateways—Formerly, gateways were *unidirectional* and could only receive incoming calls or make outgoing calls. Now a gateway can be configured to do either or both. When it does both, it is a *bidirectional gateway*.
- Custom modem—When your modem cannot be found in the list of modems supported by Norton pcANYWHERE, this new feature lets you customize the modem command set.
- Drive security—The host user can limit a remote user's access to floppy, hard (fixed), or network drives. The remote user can have read/write, read-only, or no access to a type of drive.
- Caller log in—The host can now require that a remote caller use a combination of a login name plus a password if that level of security is desired.
- Prevention of file transfers—The host can prohibit a remote caller from uploading or downloading files on the host.

- Data encryption—The host user can refuse, allow, or insist on data encryption for all data transmitted during a remote control session. Both the host and remote PC must have Norton pcANYWHERE for Windows, version 2.0, or Norton pcANYWHERE for DOS, version 5.0, to use encryption.
- Script recording—A script can be automatically created by enabling script recording which will record the script commands that occur during a session.
- OLE 2 (Object Linking and Embedding) Support—pcANYWHERE 2.0 acts as an OLE-Server, allowing OLE-Controller applications to access pcANYWHERE's command lines. See your Microsoft Windows documentation for details.
- Support for the Winsock standard TCP/IP (Transmission Control Protocol/Internet Protocol).
- Support for long filenames—If your version of Windows provides long filename capability, pcANYWHERE supports this feature.
- Cue Cards—Dialog boxes containing helpful information about a control or button. You enable the Cue Card feature from the Help menu, then you can position the mouse pointer on a control or button and click the right mouse button to display the information.
- The Norton Assistant—Macros that walk you through a procedure. When you run a Norton Assistant macro, pcANYWHERE pauses to allow you to interact with the macro and input data. Norton pcANYWHERE assumes that the information you enter during the execution of a Norton Assistant macro is valid, and the information is saved in the program.

Converting pcANYWHERE Version 1.0's Configuration Files

If you want to use your Norton pcANYWHERE for Windows version 1.0 configuration files (files that contain hardware configurations, session configurations, and caller information) with pcANYWHERE for Windows version 2.0, copy the old configuration files into the new pcANYWHERE version 2.0 directory. When you start pcANYWHERE version 2.0 for the first time, the old configuration files will be converted automatically.

NETWORK USERS: Automatic conversion is performed for your personal configuration files. The shared configuration files (and the default configuration files used as a starter set for each new user) are converted when the network administrator runs Norton pcANYWHERE version 2.0 for the first time using the ID @@@.

What are the names of the configuration files?

For standalone installation, the filenames match the specification *AW.??6*.

- *AW.OS6* Online service session configurations
- *AW.PC6* Remote control session configurations
- *AW.CI6* Caller information configurations
- *AW.HW6* Hardware configurations

For network installation, the filenames of personal configuration files match the specification *AWuserid.??6*, where *userid* is an ID up to six characters long that you use with pcANYWHERE. If your user ID is less than six characters in length, pcANYWHERE adds underscores to make the length of *userid* equal to six characters. For example, if your *userid* is DAVE, the filenames match the specifications *AWDAVE__.??6*.

The filenames for shared configuration files match the specification *AW.??6*. The default configuration files (used as a starter set for each new user) match the specification *AW@@@__.??6*.

Where are the 1.0 configuration files now?

For a standalone installation, if you are using the *AW* environment variable in your *AUTOEXEC.BAT* file, you will find the 1.0 configuration files in the directory specified by that variable. Otherwise, the configuration files are in the directory where you installed pcANYWHERE for Windows version 1.0.

For a network installation, if you are using the *AW* environment variable in your *AUTOEXEC.BAT* file, you will find the personal files in the directory specified by that variable. If your network administrator disabled the use of that variable by Norton pcANYWHERE, personal files are in the directory that was designated for personal files during the installation of pcANYWHERE for Windows version 1.0. Shared files are in the directory that was designated for shared files during that installation. If your network administrator did not perform an advanced installation, both the personal directory and the shared directory are the directory where Norton pcANYWHERE for Windows 1.0 was installed.

Where do I move the files?

For a standalone installation, put the files in the directory specified by the *AW* environment variable or the directory where pcANYWHERE for Windows version 2.0 is installed.

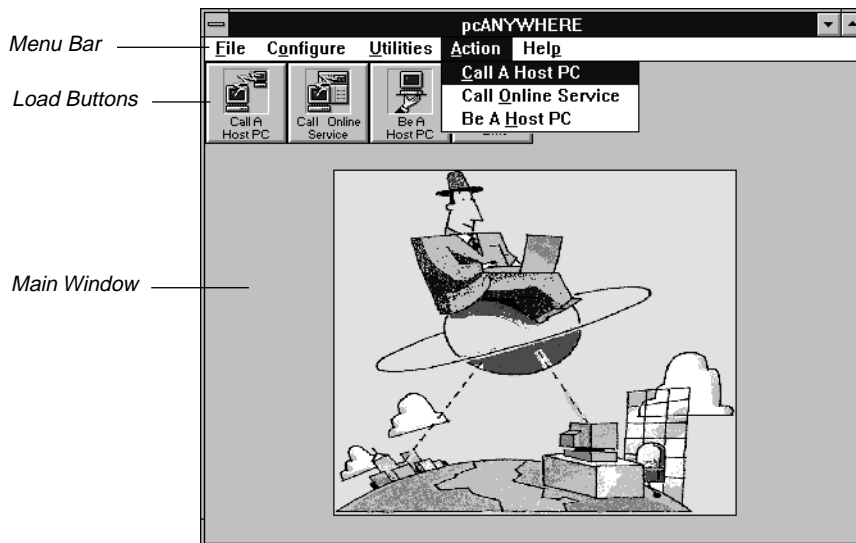
For a network installation, put the personal files in the directory specified by the AW environment variable or the directory your network administrator chose for personal files when pcANYWHERE version 2.0 was installed. The network administrator should copy the shared configuration files to the directory specified for shared files in pcANYWHERE for Windows version 2.0.

Accessing Program Modules

Norton pcANYWHERE has three windows that correspond to its main functions: Call A Host PC, Call Online Service, and Be A Host PC (Figure 1-3). To load one of the three program modules, click its load button. The selected load button changes appearance, as if it has been pressed, to indicate the currently loaded module. To change to a different module, click its load button and the previously selected button pops out. When you use the Action menu to move between modules, the load buttons automatically change as well.

Activate Cue Cards and The Norton Assistant from the Help menu.

Figure 1-3 The main window corresponds to the selected load button.





Call A Host PC

Load the Call A Host PC window when you want to control a Norton pcANYWHERE Host computer. From this window you also create and manage a list of one or more hosts to choose from for remote computing sessions. See Chapter 5, "Configuring Norton pcANYWHERE" for additional information.



Call Online Service

Load the Call Online Service window when you want to connect with bulletin board services (BBSs), information services such as CompuServe, and other multi-user systems such as mainframes and minicomputers. From this window you also create and manage a list of one or more online services to choose from for online sessions. See Chapter 7, "Online Services," and Chapter 8, "Managing Remote Control and Online Sessions," for more information.



Be A Host PC

Load the Be A Host PC window when you want to establish your computer as a Norton pcANYWHERE host to be accessed individually by one or more remote users. From this window you also select certain host communications parameters and session options. See Chapter 5, "Configuring Norton pcANYWHERE," for more information on host operation.

Installation and General Setup

2

This chapter covers:

- Installation on a standalone PC
- Installation on a network
- Installation on a network workstation
- Customizing installation for host operation
- Uninstalling Norton pcANYWHERE for Windows

Installing Norton pcANYWHERE on a Standalone PC

Standalone installation installs all the files needed by one user on a standalone PC. During the installation, pcANYWHERE asks you to select certain user options. These options affect every Norton pcANYWHERE for Windows session on your computer. You should read the following section carefully before installing the program.

To install Norton pcANYWHERE for Windows:

- 1 Insert Disk 1 of the installation diskettes into your computer's floppy disk drive.
- 2 Make sure that Windows (version 3.1 or later) is running on your computer or workstation. Choose RUN... from the File menu of Program Manager or Norton Desktop and type `A:Install` or `B:INSTALL` in the text box.
- 3 Click OK.

Or,

Type `A:INSTALL` or `B:INSTALL` at the DOS prompt.

The Symantec installation program begins. Follow any on-screen instructions.

Licensing Norton pcANYWHERE

The Norton pcANYWHERE for Windows installation program requires that you provide licensing information before continuing with the installation.

To license your copy of Norton pcANYWHERE:

- 1 Type your name in the Name text box (Figure 2-1).

Figure 2-1 You must provide license information before continuing with the installation.



- 2 Type your company's name in the Company text box.
- 3 Click OK.

The Install pcANYWHERE Program Files To dialog box appears. Continue to the next section.

Specifying the Program Directory

After you have entered the license information for your copy of Norton pcANYWHERE, the installation program searches for previous installations of Norton pcANYWHERE for Windows. If it finds a directory with the program installed, it suggests that you install to that directory. Otherwise it suggests that you install to C:\WINAW.

NOTE: The installation program searches for previous installations of Norton pcANYWHERE for Windows. If you re-install to a directory where you have previously installed and configured Norton pcANYWHERE for Windows, the installation program locates your existing configuration files and converts them to the new version. See Chapter 1, “Welcome to Norton pcANYWHERE,” for information on conversion of configuration files.

To accept the suggested installation drive and directory:

- Click OK in the Install pcANYWHERE Program Files To dialog box (Figure 2-2).

The installation begins. Change diskettes when you are prompted.

Figure 2-2 The Target Drive Status group box displays available disk space.



To select a different drive and directory:

- 1 Select the desired drive letter in the Drives list box (see Figure 2-2).

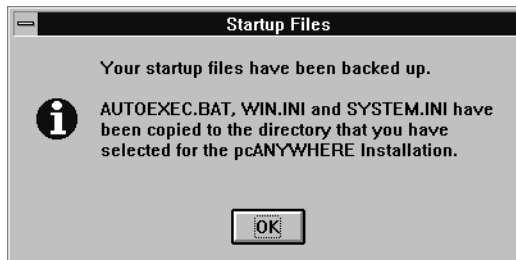
NOTE: If you do not have sufficient available disk space on the selected drive, select another drive or click Exit Install to halt the installation. Delete or move some files and start the installation program again.

- 2 Edit the directory displayed in the Install To text box if desired.
- 3 Click OK to begin the installation. Change diskettes when you are prompted.

Changes to Your System Files

The installation program copies all necessary Norton pcANYWHERE for Windows program files to your computer. The installation then creates backups of AUTOEXEC.BAT, WIN.INI, and SYSTEM.INI files, and alters the originals based on whether you are upgrading from an earlier version of pcANYWHERE and how the host was set up (Figure 2-3). Norton pcANYWHERE for Windows creates a program group and confirms that the installation has been completed by asking you to exit to DOS or restart Windows. Changes made to your Windows system files do not take effect until you restart Windows.

Figure 2-3 pcANYWHERE modifies your startup files and stores backups in your pcANYWHERE directory.



Registering Electronically

You can register your copy of Norton pcANYWHERE for Windows directly from your computer and send the registration information electronically to our toll free number. As a registered user, you will receive future product announcements and important notices.

After completing the registration forms, Norton pcANYWHERE checks the communication port and modem on your PC and asks you for dialing information (Figure 2-4). pcANYWHERE then dials a toll-free number and uploads your registration form to the Symantec database.

Figure 2-4 pcANYWHERE automatically dials the toll-free number after you provide the pre-dialing information.

You can mail or fax the registration information by canceling the phone call and printing the form in either mail or fax format (Figure 2-5).

Figure 2-5 Select the pre-configured mail or fax forms to register your copy of pcANYWHERE conveniently.

Starting Norton pcANYWHERE

To start Norton pcANYWHERE:

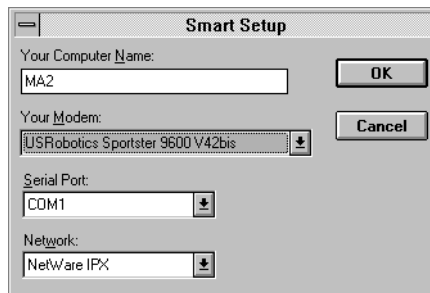
- Double-click the Norton pcANYWHERE program icon in the Norton pcANYWHERE program group.

Or,

- Choose RUN... from the Program Manager or Norton Desktop File menu, type *pathname*\WINAW and click OK. Replace *pathname* with the name of the directory to which you installed pcANYWHERE.

The first time you start Norton pcANYWHERE, you are asked to provide some hardware and system information (Figure 2-6).

Figure 2-6 The Smart Setup dialog box contains the basic information required for a connection. These configurations can be reset at any time.



- Your Computer Name—Identifies your PC when making network connections. Select a name of not more than 24 characters and one that is not likely to be used by another PC on the network. The following characters are not valid characters for use in your computer name: \ / : ; , * ? . " < > = + | [] _ ' .
- Your Modem—Specifies the modem being used on your PC. If your modem is not listed, choose the Hayes modem that most closely emulates yours or choose Hayes Compatible.
- Serial Port—Specifies what serial port your PC is using for modem communications.
- Network—Specifies what network driver your PC requires.

The information entered above can be changed as often as necessary.

Installing Norton pcANYWHERE on a LAN

This section explains how to perform an administrative installation of Norton pcANYWHERE to your network. To do an administrator install, you need full read and write access privileges to the network. The pcANYWHERE program files and options set during the administrative installation affect every user who runs Norton pcANYWHERE.

The default settings are shown in Figure 2-7, with C:\PCAWNET being replaced by the pathname you provide during installation. The pcANYWHERE program files are shared by all users and always go to a

shared directory on the network. All data files are, by default, set as personal but can be reset to shared by the administrator at the time of installation. The default directory shown for both shared and personal files is the pcANYWHERE install directory. This is not a problem, because users can share a personal directory even though they do not share personal files within the directory. When files are personal, an ID provided by each user becomes a part of each file's name (Figure 2-8). For shared files, the ID is omitted. Users can modify their own personal files, but only the network administrator (using the ID @@@) can modify shared files. To prevent users from editing or changing the shared configurations, the administrator should set a master password to the @@@ ID. See Chapter 5, "Configuring Norton pcANYWHERE," for information on setting a master password.

Figure 2-7 The administrative installation allows you to customize the status and location of pcANYWHERE files.

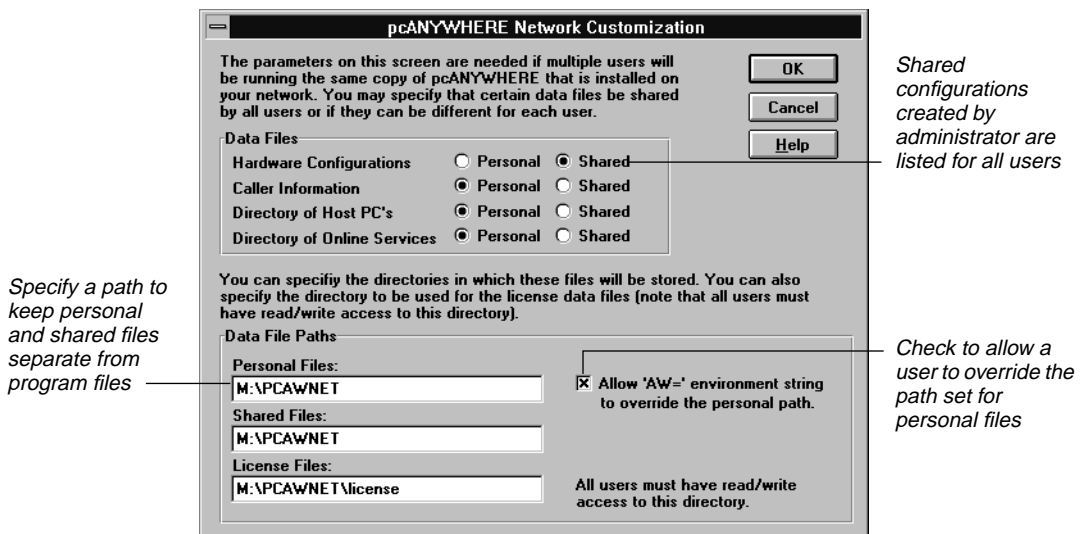
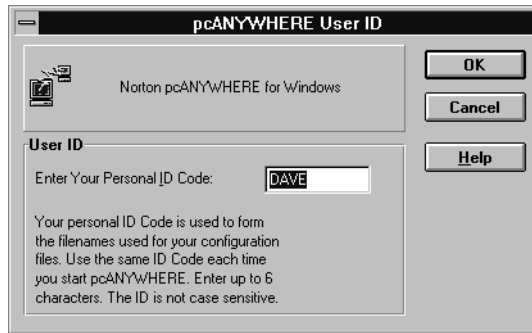


Figure 2-8 Enter the same personal ID code each time to access the personal configuration files you have created.



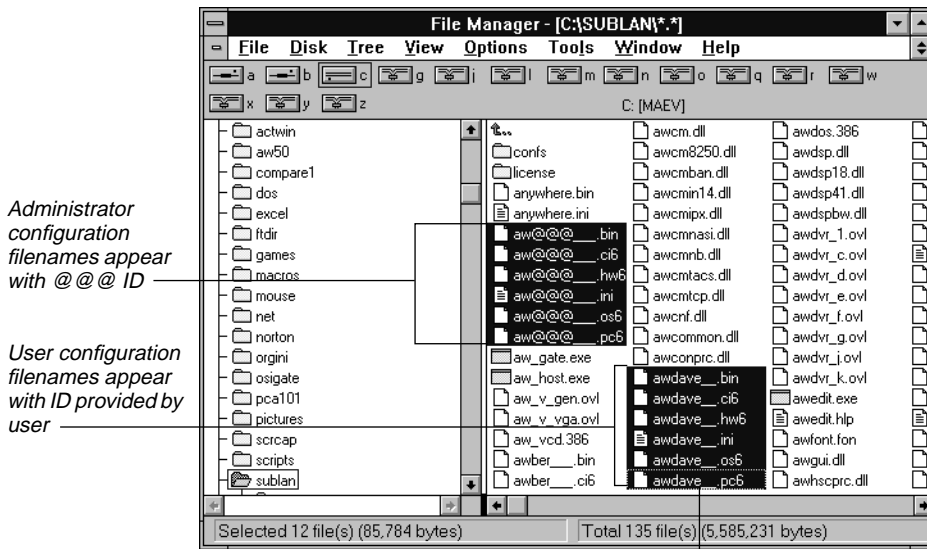
For network installation, the general configuration files are always personal files. They are named *AWuserid.BIN* and *AWuserid.INI* where *userid* represents the ID provided by the user.

The following files can be personal or shared files:

- The caller information file (*AWuserid.C16*)
- The hardware configuration file (*AWuserid.HW6*)
- The remote control session configuration file (*AWuserid.PC6*)
- The online session configuration file (*AWuserid.OS6*)

Every time a user accesses pcANYWHERE from the network, pcANYWHERE asks for an ID (up to six characters). Each personal filename has eight characters before its extension; if the user ID has fewer than six characters, Norton pcANYWHERE adds underscore characters to the end of the filename to ensure eight characters. The first time the user provides the ID, pcANYWHERE creates personal configuration and information files (Figure 2-9).

Figure 2-9 The six configuration files are created using the user-provided ID.



Underscores are added to IDs having fewer than eight characters

If you do not want personal files mixed in with program files, you can:

- Give each user a location for personal files by setting the AW environment variable in the user's AUTOEXEC.BAT file. See "Adjusting your AUTOEXEC.BAT File" later in this chapter for more details.
- Specify a directory for personal files in the Data File Paths group box during installation (see Figure 2-7).

To do an administrative network installation from Windows:

- 1 Log in at any network workstation.

NOTE: Be sure to log in as supervisor, or at least under a network account that has full read and write access to the network drive and directory to which you are installing the software.

- 2 Insert Disk 1 of the installation diskettes into the workstation's floppy disk drive.

- 3 Make sure that Windows (version 3.1 or later) is running on your computer or workstation. Choose RUN... from the File menu of Program Manager or Norton Desktop and type `A:INSTALL /A` or `B:INSTALL /A` in the Command Line text box in the Run dialog box

Or,

Click the Browse... button to locate the correct drive and directory and select the `INSTALL.EXE` file. Then type a space and `/A` after the filename in the Command Line text box. If the `/A` switch is not entered, `pcANYWHERE` performs a standard installation.

- 4 Click OK.

The Symantec installation program begins. Follow any on-screen instructions to complete the installation.

To do an administrative network installation from the DOS prompt:

- 1 Log in at a network workstation.
- 2 Insert Disk 1 of the installation diskettes in the workstation's floppy disk drive.
- 3 Type `A:INSTALL /A` or `B:INSTALL /A` at the DOS prompt and press Enter.

The Symantec installation program begins. Follow any on-screen instructions to complete the installation.

Licensing Norton pcANYWHERE

The Norton `pcANYWHERE` for Windows installation program requires that you provide licensing information before continuing with the installation.

To license your copy of Norton pcANYWHERE:

- 1 Type your name in the Name text box (see Figure 2-1).
- 2 Type your company's name in the Company text box.
- 3 Click OK.

The Install `pcANYWHERE` Program Files To dialog box appears. Continue to the next section.

Specifying the Program Directory

After you've registered your copy of Norton pcANYWHERE, the installation program searches for previous installations of Norton pcANYWHERE for Windows. If it finds a directory with the program installed, it suggests that you install to that directory. Otherwise it suggests that you install to C:\WINAW.

NOTE: The installation program searches only for previous installations of the *Windows* version of Norton pcANYWHERE. If you re-install to a directory where you have previously installed and configured Norton pcANYWHERE for Windows, the installation program retains all your existing configurations.

To accept the suggested installation drive and directory:

- Click OK in the Install pcANYWHERE Program Files dialog box (see Figure 2-2).

To select a different drive and directory:

- 1 Select the desired drive letter in the Drives list box (see Figure 2-2).

NOTE: If you do not have sufficient available disk space on the selected drive, select another drive or click Exit Install to halt the installation. Delete or move some files and start the installation program again.

- 2 Edit the directory displayed in the Install To text box if desired.
- 3 Click OK to begin the installation. Change diskettes when you are prompted.

The installation program copies special driver files to your Window's SYSTEM directory and adds the following statements to the [386Enh] section of your SYSTEM.INI file:

```
NetHeapSize=24
TimerCriticalSection=500
device=pathname\aw.386
device=pathname\awdos.386
```

where *pathname* represents the directory in which Norton pcANYWHERE is installed.

Specifying Data File Management

Personal data files are coded with the individual ID entered the first time each user runs Norton pcANYWHERE from a network station. These files should be stored in a network directory to which all Norton pcANYWHERE users have read and write access.

Shared data files are shared by all users and should be placed in a network directory to which users have read access only. Only the network administrator should have read and write access to the shared directory for maintaining the shared data files.

Data file paths are set for the following types of files:

- **Personal Files**—pcANYWHERE stores personal files in a drive and directory to which the user has read and write access. Personal files are listed with the ID the user provides (see Figure 2-8).
- **Shared Files**—pcANYWHERE stores shared files in a directory to which users have *read-only* access privileges to prevent editing of existing configurations or creation of new ones. All users running a network version of pcANYWHERE may access shared files.
- **License Files**—pcANYWHERE stores license files in a directory to which users have read and write access privileges. These files are used to monitor the usage of Norton pcANYWHERE.

If you have purchased Norton pcANYWHERE Connect Packs, you install them after the main installation when prompted. Use the installation program provided with the Connect Packs. For more information on installing Connect Packs, see the documentation supplied with them.

You can allow individual users to override the personal files path set by the administrator by checking the Allow AW= check box in the pcANYWHERE Network Customization dialog box (see Figure 2-7). Enter the following command in the AUTOEXEC.BAT file to alter the personal file path for his or her network station:

```
SET AW=path
```

See “Adjusting your AUTOEXEC.BAT File” later in this chapter.

Creating Shared Configuration Data Files

Before performing the user's workstation installations, it is recommended that the administrator first perform a workstation install using the administrator's ID (@@@) to create configurations that are shared by all workstation users. Creating shared information files *before* performing the individual workstation install makes the configurations available to all users the first time they run pcANYWHERE. Any configurations created *after* the workstation user runs pcANYWHERE are not available to that user unless the user provides a new User ID upon starting pcANYWHERE, or performs a new workstation installation.

To create shared configurations:

- 1 Follow the instructions for installing Norton pcANYWHERE on a network workstation (details follow this section).
- 2 Double-click the Norton pcANYWHERE program icon in the Norton pcANYWHERE program group.

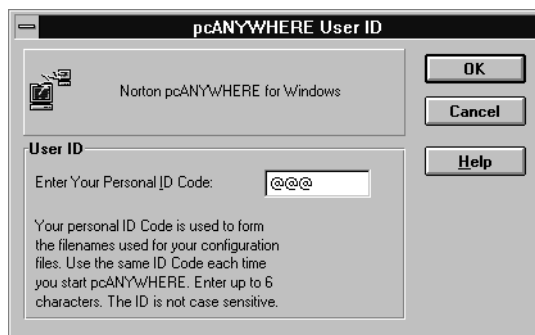
Or,

Choose RUN... from the Program Manager or Norton Desktop File menu, type *netpathname\WINAW* and click OK.

- 3 In the ID prompt box, type @@@ (Figure 2-10).

Each time you start Norton pcANYWHERE from your network station, you are prompted to enter a six-character User ID. Use the @@@ supervisor ID to create shared configurations.

Figure 2-10 Enter the Supervisor ID @@@ to create shared configurations.



- 4 Enter a computer name, the serial port your PC uses for modem communications, the network drivers your PC requires, if any, and your modem in the Preferences dialog box. (See "Starting Norton pcANYWHERE" later in this chapter for additional information.)

This information is requested the first time you run pcANYWHERE after installation or anytime you enter a new ID, and is used as the default settings in your pcANYWHERE program. You can change these selections whenever necessary. See Chapter 3, “Hardware Configurations,” for more information.

- 5 Set the configurations for the data files you indicated as shared in the pcANYWHERE Network Customization dialog box. For detailed information on creating any of the following configurations, see Chapter 5, “Configuring Norton pcANYWHERE.”

To create hardware configurations:

- 1 Choose SYSTEM HARDWARE... from the Configure Menu.
- 2 Click the New... button.
- 3 Create the desired hardware configurations. (See Chapter 5, “Configuring Norton pcANYWHERE,” for details.)

Hardware configurations you create appear in the hardware list box on each individual workstation.

To create caller information:

- 1 Click the Be A Host PC load button in the pcANYWHERE main window.
- 2 Click the default privileges or individual privileges button.
- 3 Click the Settings... button.
- 4 Set the desired configurations. (See “Configuring Caller Information” section in Chapter 5, “Configuring Norton pcANYWHERE,” for details.)

The caller information options you configure are in effect for every workstation user running pcANYWHERE.

TIP: As a security measure, enter a master password for the Supervisor ID (@@@) to prevent other network users from accessing or changing the shared configuration files you have created. For more information on master passwords, see “Setting the Master Password” section in Chapter 5, “Configuring Norton pcANYWHERE,” for details.

As a supervisor, you can use the @@@ supervisor ID as your own personal setup or you can enter a new ID to use as your personal working setup. Remember, any shared data configurations you create while using the supervisor ID are made available to all workstation users running pcANYWHERE.

Installing Norton pcANYWHERE on Network Workstations

After the administrator has installed Norton pcANYWHERE on the network server and has created the shared data files, users on the network can install pcANYWHERE on their local workstations.

A workstation installation should be performed at each individual PC that is running Norton pcANYWHERE from the network. This section explains how to perform workstation installations. Before beginning, be sure your network administrator has completed the network installation.



Ask your network administrator: Which network drive and directory (*netpathname*) contains the Norton pcANYWHERE program files?

To run the local installation program:

- 1 Log on to the network.
- 2 Choose RUN... from the File menu of the Program Manager or the Norton Desktop main window.
- 3 Type *netpathname*\INSTALL in the Command Line text box.
- 4 Click OK .

(Replace *netpathname* with the network drive and directory that contains the Norton pcANYWHERE program files. Ask your network administrator for help if necessary.)

Or,

Log on to the network and type *netpathname*\INSTALL at the DOS prompt.

Changes to Your System Files

The installation program copies all necessary Norton pcANYWHERE program files to your computer. The installation then creates a backup of AUTOEXEC.BAT, WIN.INI, and SYSTEM.INI and alters the originals based on whether you are upgrading from an earlier version of pcANYWHERE and how the host was set up (see Figure 2-3). Norton pcANYWHERE creates a program group and confirms that the installation has been completed by asking you to exit to DOS or restart Windows. Changes made to your Windows system files do not take effect until you restart Windows.

Customizing Norton pcANYWHERE Host Installation

The two Windows drivers that are added to your SYSTEM.INI [386Enh] section, AW.386 and AWDOS.386, are needed only if a PC is going to be a host. If you wish to restrict a PC to remote operation only, these drivers can be removed from the SYSTEM.INI file.

A DOS memory-resident program named AW_HOST.EXE is part of the pcANYWHERE software. This TSR version of the host program can be used to allow your PC to be a host even if Windows is not running. You must run pcANYWHERE from Windows at least once, however, to configure the DOS TSR options (see Chapter 5, "Configuring Norton pcANYWHERE," for information on configuring the TSR).

AW_HOST can be run from a DOS prompt before running Windows, or placed in your AUTOEXEC.BAT file to be executed each time you start your PC. (See Chapter 6, "Starting a Remote Control Session," for additional information.)

Uninstalling Norton pcANYWHERE

To make it quick and easy for you to remove Norton pcANYWHERE for Windows from your computer, an uninstall program was included during installation. Run this program *only* if you want to completely remove Norton pcANYWHERE from your computer. All program files are removed, along with references to Norton pcANYWHERE drivers in your AUTOEXEC.BAT and Windows SYSTEM.INI and WIN.INI files. The configuration files are not removed in the event you wish to save them for later use. If you wish to use your saved configuration files, you can either re-install Norton pcANYWHERE to the directory where those files are located, or move them to the new Norton pcANYWHERE for Windows directory.

To uninstall Norton pcANYWHERE for Windows:

- 1 Double-click the Remove Norton pcANYWHERE icon in the Norton pcANYWHERE program group.

Or,

Type *pathname*/INSTALL /U in the Program Manager (or Norton Desktop) Run dialog box, or at the DOS prompt. Replace *pathname* with the drive and directory that contains the Norton pcANYWHERE program files.

The pcANYWHERE Uninstall confirmation box appears.

- 2 Click OK to continue with the uninstall or Cancel to cancel the procedure and return to the Program Manager main window.

Adjusting Your AUTOEXEC.BAT File

You may want to adjust your AUTOEXEC.BAT file in one or both of the following ways:

To start pcANYWHERE from any directory:

- Add the name of the directory where pcANYWHERE program files are stored to your path.

For example, a PATH statement may look like the following (assuming S:\WINAW is the location of the pcANYWHERE files):

```
PATH C:\DOS;C:\WINDOWS;S:\WINAW
```

To store your personal configuration and information files in a different directory:

- Add the AW environment variable. Norton pcANYWHERE stores your personal configuration and information files in the directory specified by the AW environment variable—unless your network administrator prohibited the use of this variable by not enabling the option during installation.

For example, a `SET AW=F:\JOHN` line added to your AUTOEXEC.BAT file causes your pcANYWHERE configuration files to be stored in a directory named JOHN on the F: drive.

If an environment variable is not set, these files are stored in the pcANYWHERE program directory.

Starting Norton pcANYWHERE

Every time you start Norton pcANYWHERE from your network station, you are prompted to enter a user ID. This ID is not intended to provide password-protection, but rather to specify your unique set of personal data files for program configuration. You establish your ID the first time you start the program. Always enter the same ID to ensure that Norton pcANYWHERE is started using your unique configuration files.

To start Norton pcANYWHERE:

- 1 Double-click the Norton pcANYWHERE program icon in the Norton pcANYWHERE program group.

Or,

Choose RUN... from the Program Manager or Norton Desktop File menu, type *pathname*\WINAW and click OK (press Enter). Replace *pathname* with the name of the directory where you installed pcANYWHERE.

- 2 Type a personal user ID up to six characters long in the Enter Your Personal ID Code text box in the User ID group box (see Figure 2-8).

If you are starting Norton pcANYWHERE for the first time, or if you are using a new User ID, you are asked to provide the following hardware and system information (see Figure 2-6).

- Your Computer Name—Identifies your PC when making network connections. Select a name of not more than 30 characters.
- Your Modem—Specifies the modem being used on your PC. If your modem is not listed, choose the Hayes modem that closely emulates yours or choose Hayes Compatible.
- Serial Port—Specifies what serial port your PC is using for modem communications.
- Network—Specifies what network drivers your PC requires.

See Chapter 5, “Configuring Norton pcANYWHERE,” for details on the above options.

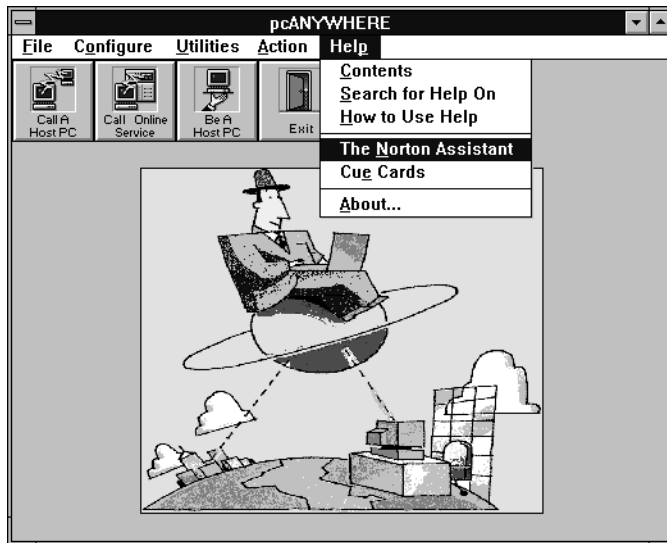
Using Cue Cards and The Norton Assistant

Cue Cards are text boxes that contain information on a selected control or button. The Norton Assistant contains predefined macros that assist the user in accomplishing certain pcANYWHERE functions.

To use cue cards:

- 1 Choose CUE CARDS from the Help menu (Figure 2-11).

Figure 2-11 A checkmark indicates that Cue Cards are enabled.

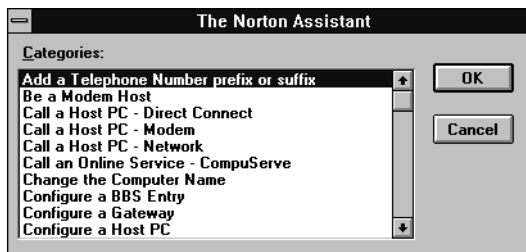


- 2 Position your mouse pointer on any control or button.
- 3 Click the right mouse button.
A text box appears with information about the selected control or button.
- 4 Click the left mouse button to clear the cue card from the screen.

To use The Norton Assistant:

- 1 Enable THE NORTON ASSISTANT from the Help menu (see Figure 2-11).
The Norton Assistant dialog box appears (Figure 2-12).
- 2 Select a Norton Assistant macro from the list box.

Figure 2-12 Select a function you want to configure from the list.



3 Click OK.

The Norton Assistant blackboard appears.

Follow the instructions on the blackboard to complete the selected Norton Assistant function. The Norton Assistant may ask you to select an option or type information.

4 Click the Next button to continue.

The Norton Assistant blackboard prompts you through the execution of the selected macro.

The blackboard closes when the Norton Assistant is finished.

Hardware Configurations

3

This chapter explains Norton pcANYWHERE hardware configurations for both standalone and network installations. (If you have not yet done so, you should read Chapter 1, “Welcome to Norton pcANYWHERE.”) The first section covers general serial connections and the second section explains network connections. If Norton pcANYWHERE is installed on a standalone station with no network attached, you can skip the “Creating Network Hardware Configurations” section.

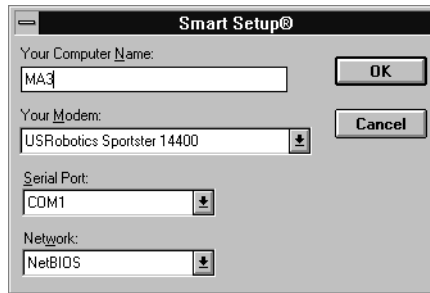
This chapter covers:

- Modem configurations
- Direct serial connections
- Leased lines
- Interrupt 14 connections
- Node connections
- Network: Telebit ACS
- Network: NACS/NASI Network:
- Network: TCP/IP
- Custom configurations

Creating a Modem Hardware Configuration

When you run Norton pcANYWHERE for the first time after installation, it asks you to name your computer, specify the serial port your PC uses, select the network drivers your PC requires, if any, and select your modem from the list provided. pcANYWHERE uses the default modem settings for the modem you select. When you create a hardware configuration, the port, modem, and network selected in the Smart Setup dialog box appear as defaults. You can change these selections whenever necessary.

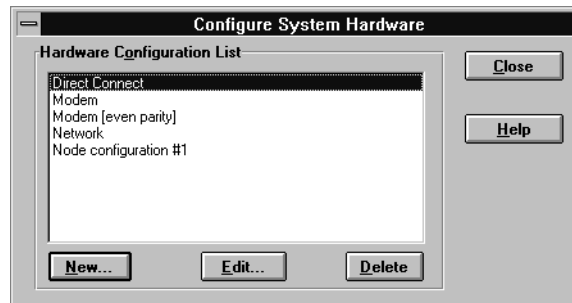
Figure 3-1 The pcANYWHERE Smart Setup dialog box appears the first time you run pcANYWHERE.



To create a modem hardware configuration:

- 1 Choose SYSTEM HARDWARE... from the Configure menu.
The Configure System Hardware dialog box appears (Figure 3-2).

Figure 3-2 Use the Configure System Hardware dialog box to customize some of the basic hardware settings to match your system.



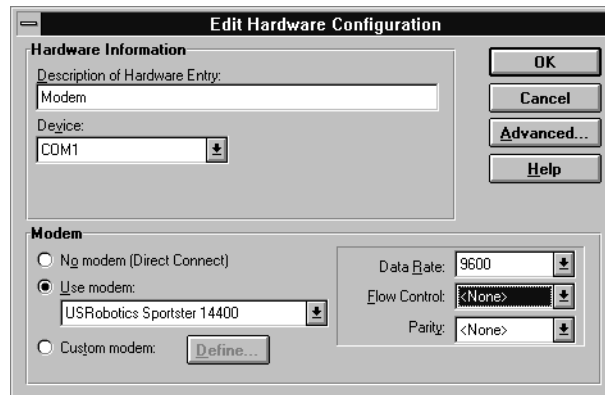
- 2 Select the existing Modem entry in the Hardware Configuration List box and click Edit... if you want to update this entry.

Or,

Click New... to add a new entry of your own.

The Edit Hardware Configuration dialog box appears (Figure 3-3).

Figure 3-3 The Edit Hardware Configuration dialog box lets you modify some basic hardware settings.



- 3 Select the communications port, (COM1 through COM4), to which your modem is attached from the Device drop-down list box in the Hardware Information group box.

NOTE: Windows and DOS standards for serial ports are not always identical. You may need to modify the Windows SYSTEM.INI file to change how Windows handles COM3 and COM4 if you want to use either of these two ports. For more information on Windows, see Appendix A, “Technical Information.”

- 4 Select the Use Modem option button in the Modem group box.
- 5 Select the name of your modem from the Use Modem drop-down list box. If the name of your modem does not appear in the list, consult your modem’s manufacturer for an alternative choice or see “Customizing the Command Set for Your Modem,” later in this chapter.

Norton pcANYWHERE automatically sets the remaining modem options to default settings. You may modify any of the communications options whenever you want. You may want to consider lowering the Data Rate setting if you have a slow PC and experience problems with connections. Flow Control and Parity should remain at their default settings, as shown in Figure 3-3 for remote computing sessions, but may be adjusted as necessary for online service sessions. See Chapter 8, “Managing Remote Control and Online Sessions,” for additional information on setting options for connecting to online services. For more information on modems and communications, refer to your modem’s manual.

- 6 Click OK to save the settings and return to the Configure System Hardware dialog box.

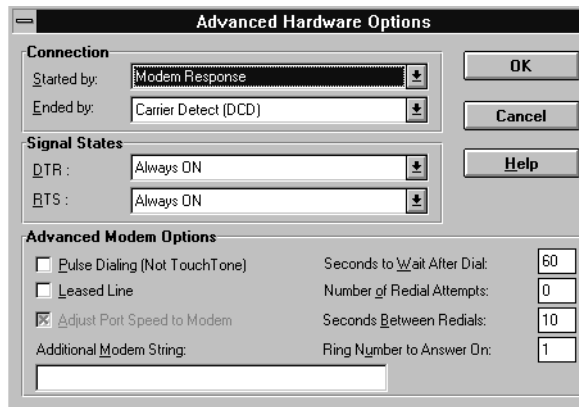
Adjusting Advanced Hardware Options

When you select a device in the Edit Hardware Configuration dialog box, the settings in the Advanced Hardware Options dialog box change to use the most common settings for that device. You probably do not need to adjust the advanced hardware options for remote computing sessions. However, if you have difficulty connecting with online services, you may need to alter one or more of the settings. If you selected Manual modem in the Use Modem list box, enter the initialization string recommended by your modem's manufacturer in the Additional Modem String text box. For more information on Manual modem, see Appendix A, "Technical Information."

To access advanced modem options:

- 1 Choose SYSTEM HARDWARE... from the Configure menu.
The Configure System Hardware dialog box appears (see Figure 3-2).
- 2 Select the existing Modem entry in the Hardware Configuration List box and click Edit... if you want to update this entry.
Or,
Click New... to add a new entry of your own.
The Edit Hardware Configuration dialog box appears (see Figure 3-3).
- 3 Click the Advanced... button in the Edit Hardware Configuration dialog box.
The Advanced Hardware Options dialog box appears (Figure 3-4).

Figure 3-4 Advanced hardware options are set automatically by Norton pcANYWHERE.



- 4 Change the advanced settings if necessary. See online help, your modem's manual, or documentation referring to an online service for more information.
- 5 Click OK to save the settings and return to the Edit Hardware Configuration dialog box.

Or,

Click Cancel to exit without saving changes.

To start a connection with this hardware configuration, proceed to Chapter 6, "Starting a Remote Control Session."

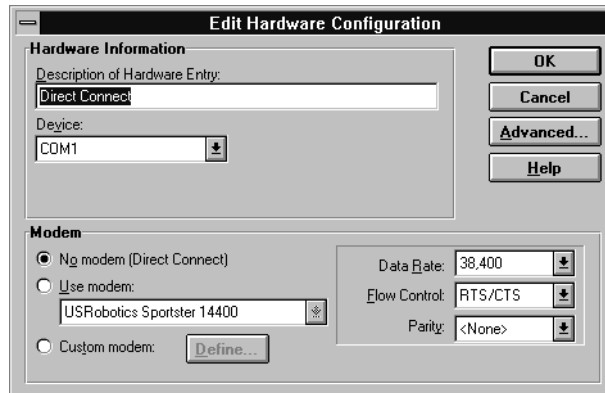
Creating a Direct Serial Hardware Configuration

Direct serial connections require a special cable called a *null modem cable*, that connects the serial ports of two PCs directly and is often used to transfer files between a desktop PC and laptop. For more information on cables, see Appendix A, "Technical Information."

To create a direct connect hardware configuration:

- 1 Choose SYSTEM HARDWARE... from the Configure menu.
The Configure System Hardware dialog box appears (see Figure 3-2).
- 2 Click the New... button.
The Edit Hardware Configuration dialog box appears (Figure 3-5).

Figure 3-5 When configuring a direct connection, make sure settings in the Modem group box are identical on both the host and remote.



- 3 Enter a new name for this hardware configuration in the Description Of Hardware Entry text box.

Make sure the name describes the type of connection for which the configuration is created.

- 4 Select the communications port (COM1 through COM4) to which your cable is attached from the Device drop-down list box in the Hardware Information group box.

NOTE: Windows and DOS standards for serial ports are not always identical. You may need to modify the Windows SYSTEM.INI file to change how Windows handles COM3 and COM4 if you want to use either of these two ports. For more information, see Appendix A, “Technical Information.”

- 5 Click the No Modem (Direct Connect) option button in the Modem group box.

Notice the Use Modem prompt button dims. No modems are used for direct connections.

Select a Data Rate, Flow Control, and Parity.

- Data Rate—set this to 9600 and work your way up to the fastest speed available through your PC’s communications ports.
- Flow Control—set according to the Data Rate. For connections of 9600 or faster, flow control should be set to RTS/CTS.
- Parity—set to None if the configuration is to be used for pcANYWHERE remote control sessions.

NOTE: Both remote and host Norton pcANYWHERE computers need identical Data Rate, Flow Control and Parity selections.

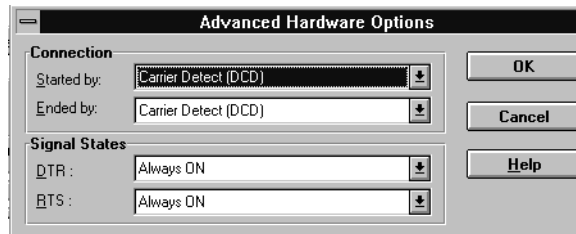
- 6 Click OK to save settings and return to the Configure System Hardware dialog box.

To access advanced direct connect options:

- 1 Click the Advanced... button on the Edit Hardware Configuration dialog box (see Figure 3-5).

The Advanced Hardware Options dialog box appears (Figure 3-6).

Figure 3-6 Norton pcANYWHERE automatically configures advanced hardware options for direct connections.



- 2 Click OK to save the advanced settings and return to the Edit Hardware Configuration dialog box.

Generally, the remote will default to the configuration shown in Figure 3-6. Unlike the host, the remote does not need to set any advanced hardware options.

To start a connection with this hardware configuration, proceed to Chapter 6, “Starting a Remote Control Session.”

Creating a Leased-Line Hardware Configuration

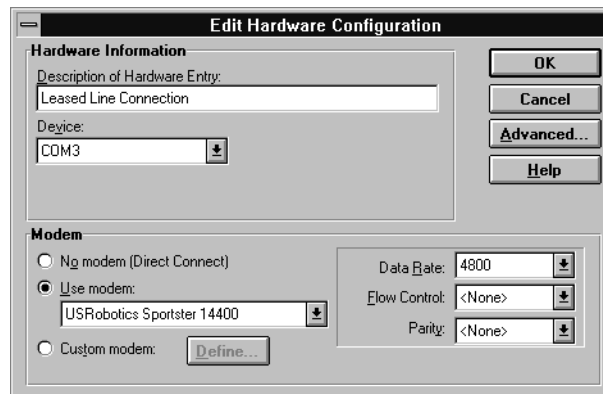
A leased line is a dedicated line between two modems. Normally this type of line is offered and maintained by local or long distance telephone companies. One characteristic of leased lines is that the telephone line over which the two modems are connected has no dial tone. The most common use of leased lines is between multiplexers. For more information on multiplexers, see Appendix A, “Technical Information.”

NOTE: It is important that this type of hardware configuration be tried with modems that are leased-line compatible. Some modems on the market are not leased-line compatible. If you are not certain whether your modem is leased-line compatible, refer to your modem's manual or contact your modem's manufacturer.

To create a leased-line hardware configuration:

- 1 Choose SYSTEM HARDWARE... from the Configure menu.
The Configure System Hardware dialog box appears (see Figure 3-2).
- 2 Click the New... button.
The Edit Hardware Configuration dialog box appears (Figure 3-7).

Figure 3-7 The Edit Hardware Configuration dialog box lets you modify some basic hardware settings.



- 3 Select the communications port to which your modem is attached, (COM1 through COM4) from the Device drop-down list in the Hardware Information group box.

NOTE: Windows and DOS standards for serial ports are not always identical. You may need to modify the Windows SYSTEM.INI file to change how Windows handles COM3 and COM4 if you want to use either of these two ports. For more information on Windows, see Appendix A, “Technical Information.”

- 4 Click the Use Modem option button in the Modem group box.

- 5 Select the name of your modem from the Use Modem drop-down list box.

NOTE: If the name of your modem does not appear in the list, consult your modem's manufacturer for an alternative choice or see "Customizing the Command Set for Your Modem," later in this chapter.

Norton pcANYWHERE automatically sets the remaining modem options to default settings. You may modify any of the communications parameters whenever you want. For more information on modem and communications options, refer to your modem's manual.

- 6 Click the Advanced... button in the Edit Hardware Configuration dialog box (see Figure 3-7).

The Advanced Hardware Options dialog box appears (Figure 3-8).

Figure 3-8 Advanced hardware options are set automatically.

*Leased Line option
must be selected by
both host and
remote*

- 7 Check the Leased Line check box. This must be checked on both remote and host Norton pcANYWHERE computers.
- 8 Click OK to save the settings and return to the Edit Hardware Configuration dialog box.

NOTE: This configuration instructs Norton pcANYWHERE to initialize the modems and wait for both the remote and host users to press Enter to begin the connection. If this is not desired, there is an alternative way to set up the remote and host computers. For more information on leased lines, see Appendix A, “Technical Information.”

To start a connection with this hardware configuration, proceed to Chapter 6, “Starting a Remote Control Session.”

Creating an Interrupt 14 Hardware Configuration

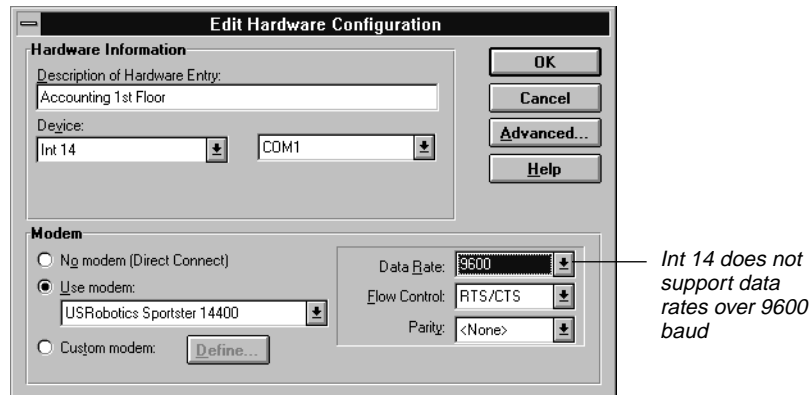
Some network communications products use Interrupt 14 (Int 14), a standard serial port support built into PCs. Most modem-sharing products provide an Int 14 interface to enable other communication programs, such as Norton pcANYWHERE, to access the modems. The Int 14 driver must be loaded before you run Norton pcANYWHERE. Refer to the manual for your network communications product for more information on installing and configuring the Int 14 software.

NOTE: Norton pcANYWHERE does not come with an Int 14 driver. You can obtain these drivers from stores or third-party distributors.

To create an Interrupt 14 hardware configuration:

- 1 Choose SYSTEM HARDWARE... from the Configure menu.
The Configure System Hardware dialog box appears (see Figure 3-2).
- 2 Click the New... button.
The Edit Hardware Configuration dialog box appears (Figure 3-9).

Figure 3-9 Norton pcANYWHERE supports Int 14 speeds of up to 9600.



- 3 Select Int 14 from the Device drop-down list box in the Hardware Information group box. A new drop-down list box appears to the right of the Device field.
- 4 Select the communications port (COM1 through COM16) to which the modem is attached. For more information on Int 14 COM port addressing, refer to your Int 14 manual.
- 5 Select the Use Modem option button in the Modem group box.
- 6 Select the name of the modem to use from the Use Modem drop-down list box.

NOTE: If the name of your modem does not appear in the list, consult your modem's manufacturer for an alternative choice or see "Customizing the Command Set for Your Modem," later in this chapter.

Norton pcANYWHERE automatically sets the remaining modem parameters to default settings. You may modify any of the communications parameters at any time. When using Int 14, Norton pcANYWHERE only supports speeds up to 9600. Flow Control and Parity should remain at their default settings, as shown in Figure 3-9 for remote computing sessions, but may be adjusted as necessary for online service sessions. For more information on modem and communications parameters, refer to your modem's manual.

- 7 Click OK to save the settings and return to the Configure System Hardware dialog box.

When you select a device in the Edit Hardware Configuration dialog box, the settings in the Advanced Hardware Options dialog box change to use the most common settings for that device. You probably do *not* need to adjust the Advanced Hardware Options for remote computing sessions. However, if you have difficulty connecting with online services, you may need to alter one or more of the settings. If you have selected Manual modem in the Use Modem list box, you should enter the initialization string recommended by your modem's manufacturer in the Additional Modem String text box in the Advanced Modem Options group box. For more information on Manual modem, see Appendix A, "Technical Information."

To access advanced Int 14 options:

- 1 Click the Advanced... button on the Edit Hardware Configuration dialog box (see Figure 3-9).

The Advanced Hardware Options dialog box appears (see Figure 3-8).

- 2 Change the settings as necessary.
- 3 Click OK to save the settings and return to the Edit Hardware Configuration dialog box.

To start a connection with this hardware configuration, proceed to Chapter 6, "Starting a Remote Control Session."

Creating Network Hardware Configurations

Network hardware configurations can be used only by PCs that are attached to a network. For example, your PC can connect to other computers on that network or use network communication devices such as a pcANYWHERE Gateway, Novell Asynchronous Communications Server (NACS), Novell NetWare Connect, or the Telebit ACS to connect to computers that are not on the network.

You may need several network hardware configurations for your PC. For example, the hardware configuration used to connect two computers on the network is different from the configuration used to make off-LAN connections. An off-LAN connection made with a gateway requires a different configuration from an off-LAN connection made with an ACS.

Creating a Node Hardware Configuration

A PC attached to a network is often referred to as a *node* on that network. You use node hardware configurations to connect your PC to another node on the same LAN or to use a gateway to access off-LAN computers. Before you create your node hardware configuration, you must know what type of communications device is required by your network. If you are not sure what network you are on, ask your system administrator or refer to Appendix A, “Technical Information.”

NOTE: Depending on how your system administrator configured Norton pcANYWHERE during installation, you may or may not be able to create or edit hardware configurations. Contact your system administrator if you experience problems creating or editing a hardware configuration.

Norton pcANYWHERE is supplied with eight different communications device drivers. Six of the eight can be used for node connections across a network:

- NetWare IPX
- NetBIOS
- Banyan VINES
- TCP/IP
- Telebit ACS
- NASI/NCSI

Select one of these device drivers, depending on which network Norton pcANYWHERE is installed. NetWare IPX is used for the examples that follow.

To create a node hardware configuration:

- 1 Choose SYSTEM HARDWARE... from the Configure menu.

The Configure System Hardware dialog box appears (see Figure 3-2).

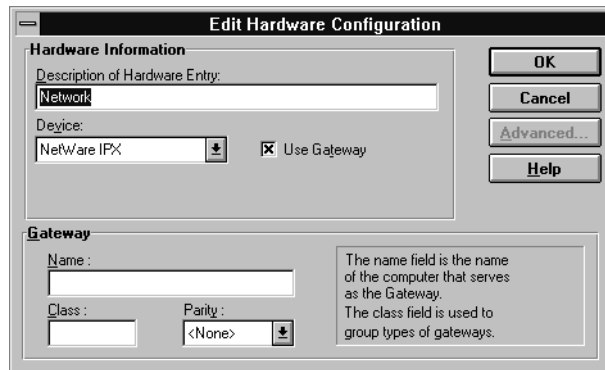
- 2 Select the existing Network entry in the Hardware Configuration List box and click Edit... if you want to update this entry.

Or,

Click New... to configure a new entry.

The Edit Hardware Configuration dialog box appears (Figure 3-10).

Figure 3-10 Use the Edit Hardware Configuration dialog box to create a node hardware configuration.



- 3 Enter a new name for this hardware configuration in the Description of Hardware Entry text box. Make sure the name describes the type of connection for which the configuration is created (see Figure 3-10).
- 4 Select the communications device supported by your network from the Device drop-down list box in the Hardware Information group box.

Norton pcANYWHERE supports NetWare IPX, NetBIOS, and Banyan VINES. If you are unsure which communications driver to choose, please contact your system administrator.

- 5 Check the Use Gateway check box found to the right of the Device field if you plan to use a gateway for communicating out of the network through an outbound gateway.

Or,

Leave Use Gateway unchecked when not using a gateway or if you are a host node waiting for a connection. For more information on gateways, see Chapter 4, “Gateways.”

If Use Gateway is checked, the following options appear in the Gateway group box:

- Name—Enter the gateway name to make Norton pcANYWHERE select that gateway automatically. If no name is entered, a list of available gateways is presented. Enter an asterisk (*) to allow Norton pcANYWHERE to select any gateway.
- Class—Enter the gateway class if several gateways exist with different classes. If no class is entered, a list of available gateways and classes is presented. Enter an asterisk (*) in the Class text box to allow pcANYWHERE to select any class.

- **Parity**—Click the Parity prompt button to select a parity different from that set up under the gateway's outgoing hardware configuration. Parity should be set to None for pcANYWHERE remote control connections. Connections to online services may require different parity settings. For example, CompuServe requires that parity be set to Even. Setting parity from the remote node's hardware configuration is easier than changing the gateway parity.

NOTE: No advanced hardware options exist for node connections using NetWare IPX, NetBIOS, and Banyan VINES. The Advanced... command button is therefore grayed.

- 6 Click OK to save the settings and return to the Configure System Hardware dialog box.

To start a connection with this hardware configuration, proceed to Chapter 6, "Starting a Remote Control Session."

Creating ACS Hardware Configurations

Another kind of network hardware configuration allows users to communicate through an asynchronous communications server (ACS) for dial-in and dial-out sessions. An ACS is similar to a file server, but instead of storing files for all the users on a network, an ACS directs serial communications for all users on a network. Normally an ACS has several communications ports on a multiport serial card. Several of these cards can be added to an ACS, creating an enormous bank of serial connections. Norton pcANYWHERE does not come with an ACS driver. pcANYWHERE communicates to an ACS via a third-party device driver. A user on a network can access the ACS through Norton pcANYWHERE as long as there is a third-party ACS driver loaded on the network node. See your network administrator or ACS documentation for configuration and driver information.

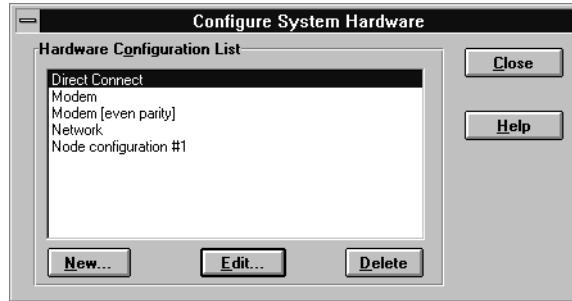
Using a NASI-Compliant ACS

When the ACS in use is compatible with a NACS (Novell Asynchronous Communications Server) or is NASI-compliant (Novell Asynchronous Services Interface), you specify a NASI/NCSI hardware configuration. You can specify its server, service, and port as part of the hardware configuration or specify that they will be selected as part of the connection process.

To create a hardware configuration for an ACS:

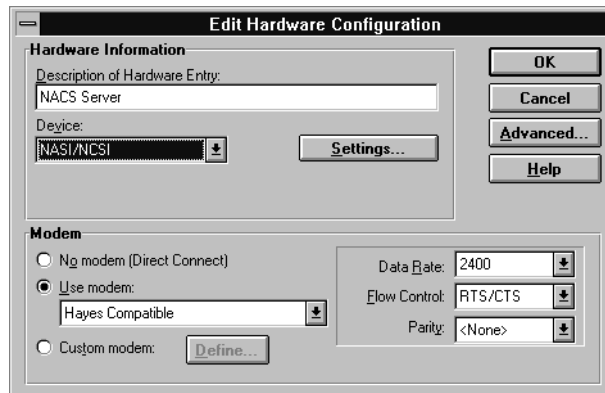
- 1 Choose SYSTEM HARDWARE... from the Configure menu.
The Configure System Hardware dialog box appears (Figure 3-11).

Figure 3-11 Use the Configure System Hardware dialog box to create an ACS hardware configuration.



- 2 Click the New... button.
The Edit Hardware Configuration dialog box appears (Figure 3-12).

Figure 3-12 Specify the type of network connection you are creating in the Device drop-down list box. Click Settings... for additional options.

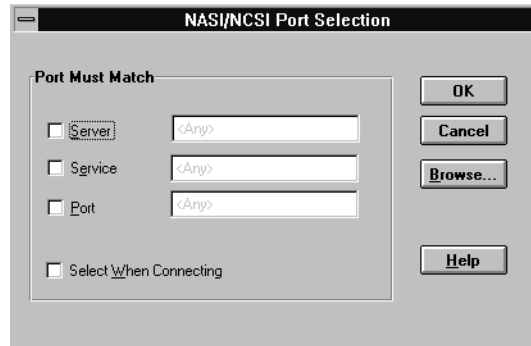


- 3 Enter a name for this hardware configuration in the Description of Hardware Entry text box.
- 4 Select NASI/NCSI in the Device drop-down list.
Advanced hardware options are set automatically by Norton pcANYWHERE.

- 5 Click the Settings... button.

The NASI/NCSI Port Selection dialog box appears (Figure 3-13).

Figure 3-13 Click the Browse... button to select from currently available network devices.



- 6 Specify how the ACS port is to be selected.

By default, the Server, Service, and Port show <Any>. This causes Norton pcANYWHERE to attach to any available server, service, and port. Leave the check boxes unchecked to attach to any device. To specify a server, service, and port, check the box directly to the left of each field and click the Browse... button. A list of available servers, services, and ports appears.

- **Server**—Check to enter a server name. Click the Browse... button to select from a list of currently available servers. Select <Any> to have pcANYWHERE select the first available server.
- **Service**—Check to enter the name of the multiport serial card to use within the ACS. Click the Browse... button to select from a list of currently available services. Select <Any> to have pcANYWHERE select the first available service.
- **Port**—Check to enter a port name. Click the Browse... button to select from a list of currently available ports. Select <Any> to have pcANYWHERE select the first available port.
- **Select When Connecting**—Allows the remote caller to select the server, service, and port at the time of connection.

NOTE: The <Any> options work only if you are a remote dialing out of an ACS. If you plan to wait for a call as a host, Norton pcANYWHERE requires that you preselect a specific server, service, and port.

- 7 Click OK to save the settings and return to the Edit Hardware Configuration dialog box.
- 8 Specify modem settings for the ACS modem with which you are connecting. For more information on modem settings, see Chapter 3, “Hardware Configurations.”
- 9 Click OK to save the settings and return to the Configure System Hardware dialog box.

Using a Telebit ACS

The Telebit Asynchronous Communications Server (ACS) uses a slightly different port selection method than the standard NASI/NCSI. The port selection criteria vary according to the port selection method you choose. See your Telebit documentation for more information. The Telebit ACS Port selection dialog boxes (Figures 3-14 through 3-16) display choices corresponding to the option button selected in the Select By group box.

NOTE: The <Any> options work only if you are a remote dialing out of an ACS. If you plan to wait for a call as a host, Norton pcANYWHERE requires that you preselect a specific server, service, and port.

Figure 3-14 Select by Pool.

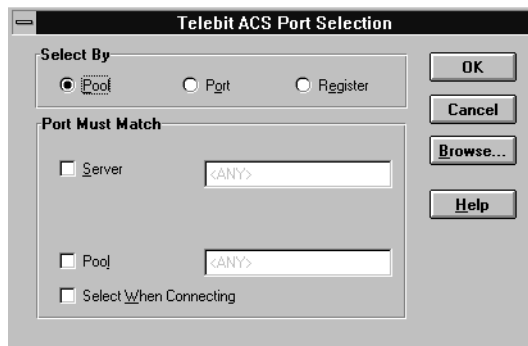


Figure 3-15 Select by Port.

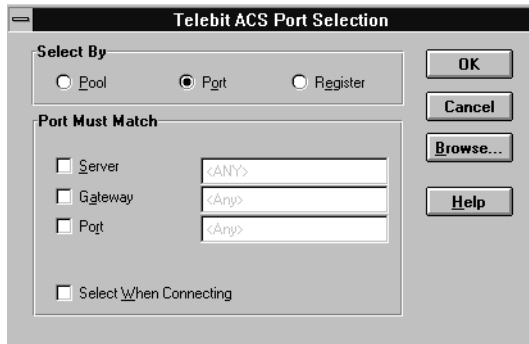
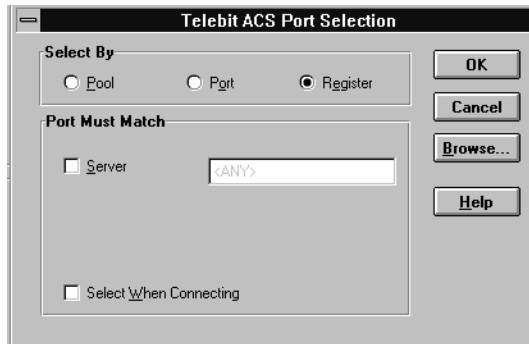


Figure 3-16 Select by Register.



NOTE: Since Norton pcANYWHERE is bundled with the Telebit ACS, refer to the Telebit ACS manual for configuration details.

To create a hardware configuration for a Telebit ACS:

- 1 Choose SYSTEM HARDWARE... from the Configure menu.
The Configure System Hardware dialog box appears (see Figure 3-11).
- 2 Click the New... button.
The Edit Hardware Configuration dialog box appears (see Figure 3-12).
- 3 Enter a name for this hardware configuration in the Description of Hardware Entry text box.
- 4 Select Telebit ACS in the Device drop-down list.

- 5 Click the Settings... button.

The Telebit ACS Port Selection dialog box appears (see Figures 3-14, 3-15, 3-16).

- 6 Specify how the Telebit ACS port is to be selected.

You can select a port by pool, by port, or by register.

The Telebit ACS selections include the following:

Pool

- **Server**—Check to enter a server name. Click the Browse... button to select from a list of currently available servers. Leave the check box unchecked to have pcANYWHERE select the first available server.
- **Pool**—Check to enter a pool name. Click the Browse... button to select from a list of currently available pools. Leave the check box unchecked to have pcANYWHERE select the first available pool.
- **Select When Connecting**—Check to select the pool name at the time of connection.

Port

- **Server**—Check to enter a server name. Click the Browse... button to select from a list of currently available servers. Leave the check box unchecked to have pcANYWHERE select the first available server.
- **Gateway**—Check to enter a gateway name. Click the Browse... button to select from a list of currently available gateways. Leave the check box unchecked to have pcANYWHERE select the first available gateway.
- **Port**—Check to enter a port name. Click the Browse... button to select from a list of currently available ports. Leave the check box unchecked to have pcANYWHERE select the first available port.
- **Select When Connecting**—Check to select the port at the time of connection.

Register

- **Server**—Check to enter a server name. Click the Browse... button to select from a list of currently available servers. Leave the check box unchecked to have pcANYWHERE select the first available server.
- **Select When Connecting**—Check to select the register at the time of connection.

- 7 Click OK to save the settings and return to the Edit Hardware Configuration dialog box.

Using TCP/IP Protocol

Transmission Control Protocol/Internet Protocol (TCP/IP) is a set of network protocols developed to allow PCs on networks to communicate with other PCs, as well as with a variety of non-PC systems such as mini-computers and mainframes. Using the TCP/IP protocols, Norton pcANYWHERE supports *only PC connections*.

NOTE: Norton pcANYWHERE does not come with TCP/IP drivers. You can obtain these drivers from stores or third-party distributors.

See Chapter 5, “Configuring Norton pcANYWHERE,” for information on setting up TCP/IP hosts.

Customizing the Command Set for Your Modem

This section explains the alternatives available to you when your modem is not found in the list of supported modems, and it introduces the Custom Modem feature, a new feature that allows you to define your own modem command set.

When your modem is not on the list of supported modems, do one of the following:

- Ask your modem’s manufacturer which modem in the list has a similar command set and select that modem.
- Choose the default modem (Hayes-compatible) and experiment with some of its settings.
- Choose Manual modem and type a string of commands after the Additional Modem Initialization String. You can find these commands by contacting the modem manufacturer’s technical support department.
- Define a custom modem. This is preferable to using Manual modem because Custom Modem allows you to specify more settings that give precise control over the modem’s behavior.

To create a custom modem configuration:

- 1 Choose SYSTEM HARDWARE... from the Configure menu.
The Configure System Hardware dialog box appears (see Figure 3-11).
- 2 Select the Modem entry and click the New... button.
The Edit Hardware configuration dialog box appears (see Figure 3-12).

- 3 Enter a name for your hardware configuration.
- 4 Select the Custom Modem option button.
- 5 Click the Define... button.

The Custom Modem Settings dialog box appears (Figure 3-17).

Figure 3-17 You can change the default settings for a custom modem as needed.

Custom Modem Settings		
Modem Name:	Acme 14.4	OK
Modem Control Strings		Cancel
Initialization:	AT&F%C1S0=0	Help
Dial Prefix:	ATDT	
Dial Suffix:		
Answer:	ATS0=1	
Disconnect:	~+++~ATS0=0H	
Modem Responses		
Connect:	CONNECT *	No Answer:
Error:	ERROR	No Connect 1:
No Carrier:	NO CARRIER	No Connect 2:
Busy:	BUSY	No Connect 3:
No Dialtone:	NO DIALTONE~	

- 6 Use your modem's manual to determine what settings to use for each option. You must type in all the settings in the Custom Modem Settings dialog box (see Figure 3-17). The data rate, flow control, and parity options are selected from a drop-down list box in the Edit Hardware Configuration dialog box (see Figure 3-12).
- 7 Click OK to save the Custom Modem settings and return to the Edit Hardware Configuration dialog box.

Gateways

4

Norton pcANYWHERE's gateway feature allows network users to share a communications device, usually a modem, attached to any one of the nodes on the network. The gateway provides dial-in and dial-out services that allow network users access to off-LAN systems and allows off-LAN users to access the network. For example, a network user can call someone who is connected to a different network—even if neither user has a modem—as long as both networks have gateways.

The gateway TSR runs in the background on a PC and can be configured so that it does not interfere with the activities of the user at that PC. The only difference for the user at the gateway PC is that he or she cannot access the modem directly—only via the gateway using the node hardware configuration. See Chapter 3, “Hardware Configurations.”

The gateway can be either unidirectional or bidirectional. A *unidirectional gateway* waits for either incoming calls from the modem or for outgoing calls from the network, but not both types. A *bidirectional gateway* accepts calls from either the network or the modem.

This chapter covers:

- Gateway concepts
- Setting up a gateway and modifying it
- Loading the gateway TSR
- Removing the gateway TSR

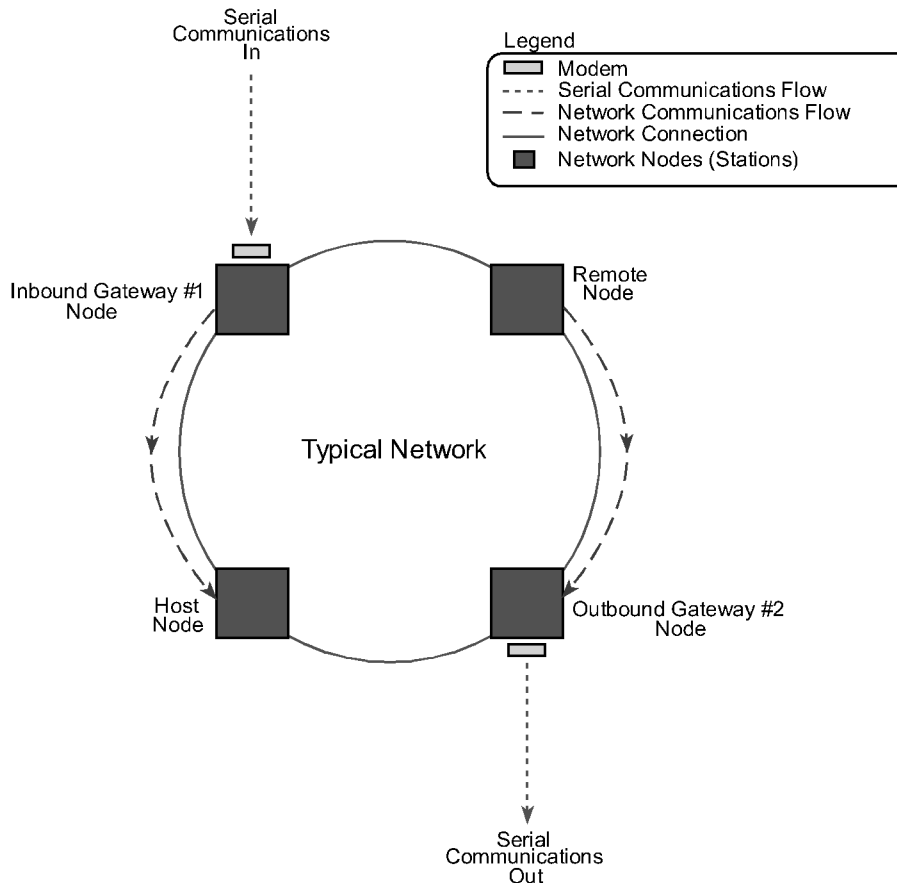
Gateway Concepts

A *gateway* is a small memory-resident program (TSR) that resides on a PC which is both on a network and has a modem (or another communications device that is compatible with Norton pcANYWHERE). The gateway takes the information from one communications device, converts it, and sends it out through the other communications device. The gateway TSR is designed to operate completely in the background. This allows network users at gateway stations to continue operating their PCs without interruption.

For the gateway to work properly, you must specify two hardware configurations: one for the network and one for the modem (or other communications device). Which configuration you designate as the incoming configuration and which you designate as the outgoing configuration is not important unless the gateway is to be unidirectional instead of bidirectional.

For a *unidirectional gateway*, the incoming configuration indicates what device the gateway accepts data from and the outgoing configuration indicates what device the gateway sends data to. Figure 4-1 shows an inbound gateway that accepts calls from the LAN and sends data over a modem.

Figure 4-1 Unidirectional gateways allow users to communicate across two different devices but in only one direction.



Using *bidirectional gateways* on the network allows outside users access to the network and network users access to host PCs and online services. Using two unidirectional gateways, each sending data in the opposite direction, also provides this functionality; however, this requires two PCs.

A single unidirectional gateway allows you to restrict calls to only incoming or only outgoing calls. For example, with a unidirectional gateway that receives calls from the network and sends data over the modem, you allow network users to make connections to each other and call off-LAN but prevent any outsiders from accessing (dialing into) the network.

Configuring Gateways

To configure a gateway, you must first determine which hardware configuration to use for the incoming and outgoing configurations. The incoming configuration specifies the device the gateway uses to receive calls and the outgoing configuration specifies the device it uses to forward or route calls.

For example, if users on a network want to access a gateway PC on the network to use its modem to dial an online service such as a BBS, the gateway PC should be set up with *network* as the *incoming* hardware configuration (because the gateway receives calls from users on the network) and *modem* as the *outgoing* hardware configuration (because the the gateway's modem is used to dial the online service).

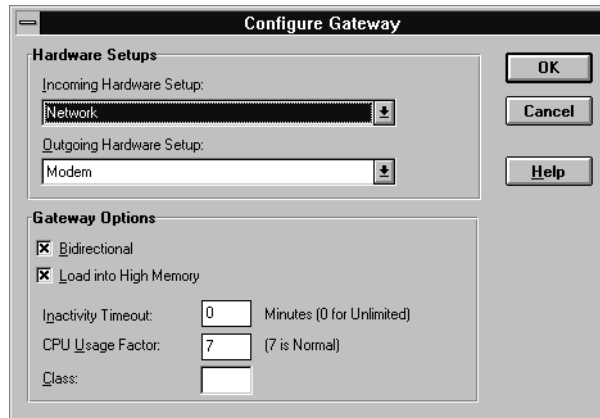
To configure the gateway:

- 1 Create the necessary hardware configurations if you have not previously done so. See Chapter 3, "Hardware Configurations," for information on how to create hardware configurations.

NETWORK USERS: Sometimes the network administrator specifies that the hardware configuration file and/or the session configuration file is to be shared by all network users. If the file is shared, you must use the predefined configurations set by your network administrator.

- 2 Choose GATEWAY... from the Configure menu.
The Configure Gateway dialog box appears (Figure 4-2).

Figure 4-2 Create a gateway by specifying the incoming and outgoing hardware configurations. Group gateways by assigning them to a class.



- 3 Click the Incoming Hardware Setup prompt button to display a list of available hardware configurations. For a unidirectional gateway, choose the device from which the gateway receives information.
- 4 Select the hardware configuration used to receive the incoming information.
- 5 Click the Outgoing Hardware Setup prompt button to display a list of available hardware configurations. For a unidirectional gateway, choose the device to which the gateway sends information.
- 6 Select the hardware configuration used to send the outgoing information.
- 7 Specify the appropriate gateway options:
 - Bidirectional—Designates whether the gateway allows both incoming and outgoing calls. Unchecked, the gateway restricts calls to only incoming or only outgoing.
 - Load into High Memory—Loads the gateway TSR into high memory giving the gateway PC more efficient use of the available memory.
 - Inactivity Timeout—Specifies the maximum period of inactivity allowed before the gateway automatically ends the idle session.
 - CPU Usage Factor—Specifies the percentage of the amount of the computer's processing time dedicated to gateway operations. The default value is 7, which would rarely interfere with the normal use of the PC. A value of 10, however, is the best choice for PCs that are dedicated solely to gateway operations.

- Class—Specifies this gateway as part of a group of gateways. Classes are commonly based on the speed of the modem. For example, a network administrator might create a class of 9600-bps gateways called 9600.
- 8 Click OK to save the settings and return to the Norton pcANYWHERE main window.

Modifying Gateway Settings

After making the changes, the gateway must be reactivated. See “Loading the Gateway TSR” later in this chapter.

To modify gateway settings:

- 1 Choose GATEWAY... from the Configure menu.
- 2 Follow the procedures in the previous section for selecting the Hardware Setups and Gateway Options.
- 3 Click OK to save the new settings and return to the Norton pcANYWHERE main window.
- 4 Exit pcANYWHERE and Windows and re-load the gateway (see “Loading the Gateway TSR” later in this chapter).

NOTE: If the gateway TSR is already loaded using a previous configuration, you must remove it from memory before reactivating it with the modified settings (see the procedure “To remove the gateway TSR from memory” later in this chapter).

Loading the Gateway TSR

Once the gateway settings have been configured, you can load the gateway and make it available to all network users running Norton pcANYWHERE. pcANYWHERE does not load the gateway automatically from within the program. You must enter the gateway load command at the DOS command line or have it loaded automatically from a batch file.

NOTE: When using the network as part of the gateway’s device configurations, make sure you have all Norton pcANYWHERE compatible network drivers loaded. If you do not have the network drivers loaded, the gateway TSR will not operate properly. If you are using a modem, make sure the modem is installed correctly and is turned on.

To load the gateway TSR:

- 1 Exit Windows completely. Do not run DOS in a Windows DOS box.
- 2 For standalone installations of Norton pcANYWHERE, at the DOS prompt type:

```
pathname\AW_GATE
```

Or,

If you have a network installation of Norton pcANYWHERE, at the DOS prompt type:

```
pathname\AW_GATE /I:userid
```

Replace *pathname* with the name of the directory that contains the Norton pcANYWHERE program files. Replace *userid* with the pcANYWHERE user ID for the user on whose PC the gateway resides.

TIP: To load the gateway automatically when the computer is started or rebooted, place the gateway's DOS command line in the AUTOEXEC.BAT file. Because the Norton pcANYWHERE program files are located on the network, make sure you have access to the network drive where Norton pcANYWHERE is installed when not logged in. For example, on Novell networks, users can access the F:\LOGIN drive with read-only rights without being logged in.

Once the gateway is loaded, users on the gateway PCs can continue using their computers as usual. If the gateway user needs to use Norton pcANYWHERE to receive or initiate calls, he or she must set up pcANYWHERE as a node hardware configuration and access the gateway the same way as other network users. Although the modem is attached to the gateway user's station, the gateway TSR must have control over it. If control of the modem is interrupted by pcANYWHERE or another communications package, the gateway will not operate correctly.

For more information on using gateways to start a remote computing session, see Chapter 6, "Starting a Remote Control Session."

To remove the gateway TSR from memory:

- 1 Exit Windows completely. Do not run DOS in a Windows DOS box.
- 2 Type `AW_GATE -c` at the DOS prompt.
The TSR is removed from memory.

Configuring Norton pcANYWHERE

5

This chapter explains how to configure general program options and how to set up a Norton pcANYWHERE remote and host computer. You should create one or more hardware configurations as described in Chapter 3, “Hardware Configurations,” before proceeding.

For information on configuring terminal emulation options for accessing online services see Chapter 7, “Online Services.” For information about file transfer options see Chapter 8, “Managing Remote Control and Online Sessions.”

This chapter covers:

- Assigning a computer name
- Setting the master password
- Creating a dialing prefix/suffix list
- Setting host options
- Defining default caller entry
- Creating a caller list
- Setting remote options
- Creating a Host PC directory
- Drive mapping

Setting Options in the Configure Menu

This section explains four of the options available from the Configure menu. The settings you select affect every remote or host session you start from your computer.

The configuration options covered in this chapter include:

- SYSTEM SETUP
- PREFIX/SUFFIX
- HOST OPERATION
- REMOTE OPERATION

Defining Your Computer's Name and Security Level

SYSTEM SETUP defines the name and security for your Norton pcANYWHERE computer. You already assigned a name to your computer when you started Norton pcANYWHERE for the first time. If you do not want to change the name you assigned, skip ahead to “Setting the Master Password.”

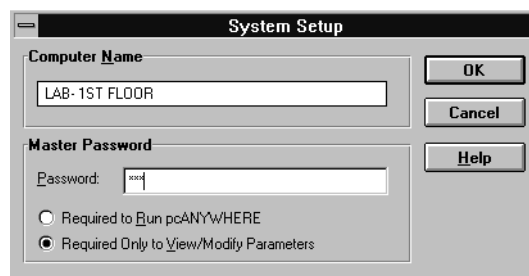
Assigning a Computer Name

You assign a name to your computer to distinguish it from other computers running Norton pcANYWHERE. pcANYWHERE's Smart Setup prompts you to name your computer the first time you launch Norton pcANYWHERE. Choose a name for your PC that is meaningful and easy to remember. You can use up to 24 characters. You can change this computer name as often as you like.

To change your computer name:

- 1 Choose SYSTEM SETUP... from the Configure menu.
The System Setup dialog box appears (Figure 5-1).

Figure 5-1 The Master Password is an optional security feature.



- 2 Enter a computer name of up to 24 characters in the Computer Name text box.
- 3 Click OK to save the computer name and return to the Norton pcANYWHERE main window.

Setting the Master Password

You can restrict access to your Norton pcANYWHERE installation. There are two levels of security. The higher of the two requires the master password to run the program. The other requires the password only for configuration

changes. Users that you allow to control your computer remotely have full access to Norton pcANYWHERE and its configuration files unless you enable the master password.



WARNING: Use caution when setting the master password. Once you have set it, there is no way to access the protected areas if you forget the password. Be sure to write down the master password you have selected and keep it in a secure place. For maximum security do not select a password that can be found in any dictionary. Instead use meaningful but nonstandard words or a combination of words and punctuation.

To set the master password:

- 1 Choose SYSTEM SETUP... from the Configure menu.
The System Setup dialog box appears (see Figure 5-1).
- 2 Enter a master password of up to 16 characters in the Password text box.
- 3 Click an option button for the level of security you want to implement.
 - Required to Run pcANYWHERE—Norton pcANYWHERE does not load on a PC if this button is selected unless the master password is entered.
 - Required Only to View/Modify Parameters—If this button is selected, users can load Norton pcANYWHERE and make connections; however, users cannot change any of the configurations without entering the master password first.
- 4 Click OK.

Creating a Prefix/Suffix List

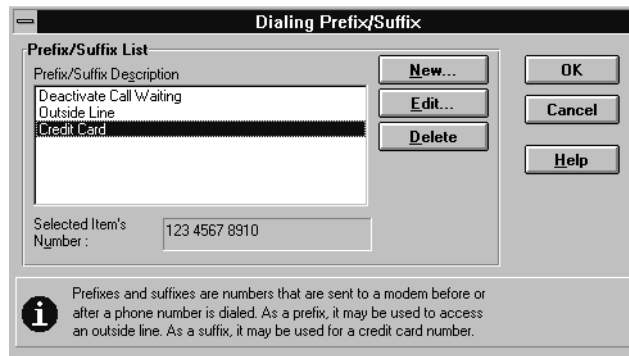
A *prefix* is an optional number or group of numbers added to the beginning of a phone number. Entering 9 to dial out of an office telephone system is an example of using a prefix. A *suffix* is an optional number or group of numbers appended to the end of a telephone number. A calling card number is an example of a suffix. Before you can use a suffix or prefix for host or remote dial-out operations, you must create a Dialing Prefix/Suffix List. You enter the numbers and codes and associate each with a descriptive name. Then, to use a prefix or suffix you simply specify it by name in the host or remote dialing instructions. For more information on entering dialing instructions, see Chapter 6, "Starting a Remote Session," or Chapter 7, "Online Services."

To enter prefix and suffix information:

- 1 Choose PREFIX/SUFFIX... from the Configure menu.

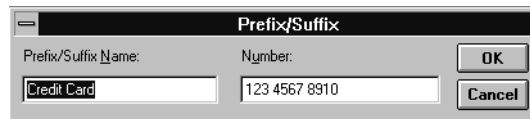
The Dialing Prefix/Suffix dialog box appears (Figure 5-2). If you specified a master password, you are prompted to enter it before the Dialing Prefix/Suffix dialog box appears.

Figure 5-2 You can edit or add to the Prefix/Suffix List at any time.



- 2 Click New... to create a new entry.
- Or,
- 3 Highlight an existing entry and click Edit....
- The Prefix/Suffix dialog box appears (Figure 5-3).

Figure 5-3 Give each prefix or suffix a unique descriptive name.



- 4 Enter a descriptive name in the Prefix/Suffix Name text box and the associated numbers or codes in the Number text box.
 - 5 Click OK.
- The new prefix or suffix appears in the Prefix/Suffix list.

Setting Up Host Operations

Before you can begin a remote computing session with a host, the host must be configured.

Host configurations include:

- Host options—Establishing security, timeout, and other options.
- Caller information—Establishing a list of callers allowed to control your host computer.
- Hardware configuration—Selecting hardware and communications parameters for your host. pcANYWHERE asks you to identify what communications port and modem you are using the first time you run pcANYWHERE. You can change this hardware configuration as often as required. (See Chapter 3, “Hardware Configurations.”)

Configuring Host Options

As the host user, you can place restrictions on the remote user and modify certain host functions. Host options determine how much control remote callers have on the host PC as well as how the host PC behaves. For example, you can configure the host PC so that the screen blanks upon each connection. This prevents the activities taking place on the host from being observed by anyone who is near the host. Host options affect *every* remote control session using the PC as a host.

Host options fall into three categories:

- GENERAL...
- SECURITY...
- DOS TSR OPTIONS...

Setting the Host's General Options

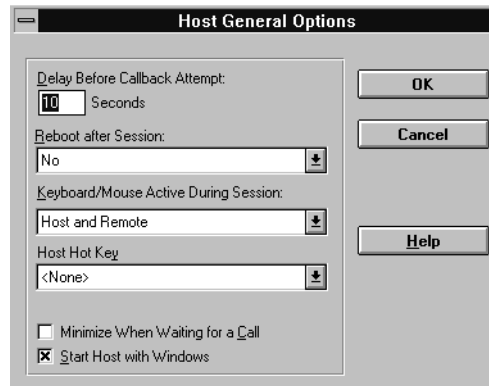
Use the general options to specify whether the host automatically reboots after each session, to designate which keyboard and/or mouse is active during a session, to assign the host PC's hotkey, and to instruct the host to minimize when waiting for a call.

To configure the general options:

- 1 Choose HOST OPERATION from the Configure menu.
- 2 Choose GENERAL... from the submenu.

The Host General Options dialog box appears (Figure 5-4).

Figure 5-4 The Host General Options dialog box allows you to set session preferences that affect the operation of the host PC.



- **Delay Before Callback Attempt**—You specify, in seconds, how long the host waits before making a callback to the remote PC. This setting is ignored if the Callback the Remote User option is not enabled in the Caller Entry menu. See “Configuring Caller Information” later in this chapter.
- **Reboot after Session**—Determines if the host reboots after every session or every abnormal disconnection. You can specify a cold boot (equivalent to turning the PC off and then back on) or a warm boot (equivalent to pressing Ctrl+Alt+Del or the reset button). For example, you can use this feature to ensure that users do not find someone else’s application running when their sessions start. To have the host launch automatically after reboot, check the Start Host with Windows check box in the Host General Options dialog box and run Windows from the AUTOEXEC.BAT file. To run the DOS Host TSR automatically after reboot, enter the RUN command in the AUTOEXEC.BAT file. (For information on DOS host commands, see Chapter 6, “Starting a Remote Session.”)

TIP: If you usually perform remote tasks on the host that have long processing times, such as operations on large database files, you may want to select No Reboot or Warmboot if Connection Lost. This allows you to end the current session after starting the remote task without interrupting the task. Later you can check its progress from another session. In addition, this prevents data loss if there is unsaved data at the time of an unexpected interruption.

- Keyboard/Mouse Active During Session—Allows the host to determine who has keyboard and mouse control during the session. The default setting is Host and Remote.
 - Minimize when Waiting for a Call—Causes the host to appear on the desktop as an icon when it is waiting for a connection. If this option is unchecked, pcANYWHERE displays a status dialog box.
 - Start Host with Windows—Causes the host to load and wait for a call automatically each time you run Windows.
- 3 Click OK to save the settings and return to the main Window.

Setting Security Options

Some security options determine if the remote user can blank the host screen or encrypt data. Others regulate input of passwords and the display of prompts. Still others control if the host is locked while waiting for a connection and if the session ends because of inactivity. The logging of failed connections is explained in detail in Chapter 10, “Utilities.”

To configure security options on the host:

- 1 Choose HOST OPERATION from the Configure menu.
- 2 Choose SECURITY... from the submenu.

The Host Security Options dialog box appears (Figure 5-5), in which you can check or uncheck the following security preferences:

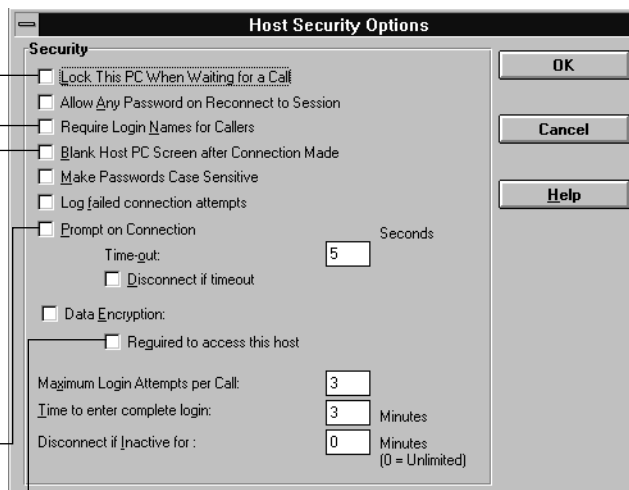
Figure 5-5 Host options control operation before, during, or after a remote computing session.

Locking the host prevents anyone from using the PC when it is waiting for a call

Checking or unchecking Login Names has an effect on user IDs already created

Blank the host screen after connections to prevent unauthorized viewing of confidential applications

Alerts the host to an incoming call and can authorize the connection



Remotes must use a version of Norton pcANYWHERE that supports data encryption

- **Lock This PC When Waiting for a Call**—Prevents others at the host site from using your host PC while it is waiting for a remote user to call.
- **Allow Any Password on Reconnect to Session**—Allows users to log in with any password after a remote computing session is unexpectedly disconnected.
- **Require Login Names for Callers**—Requires a user to have both a login name and a password when connecting to a host. (See “Caller Information” later in this chapter.) The Require Login Names... check box increases the level of host security by requiring a remote caller to use an assigned login name as well as a password. When login names are required by the host, the login name you assign for each caller must be unique, but the password does not have to be unique and can be one that is assigned to another caller. When login names are not required by the host, the passwords assigned to each caller must be unique.

CAUTION: Switching this option on and off affects caller IDs that have been set up previously. If the host configures remote callers with a login and a password and later disables (unchecks) the Require Login Names... option, a conflict could exist with duplicate passwords, because only the login name had to be unique. To avoid this conflict, the host automatically uses the previously assigned login name as the remote's password whenever the Require Login Names... option is disabled (unchecked).

- **Blank Host PC Screen After Connection Made**—Improves the security of unattended host sessions by blanking the host PC monitor display.
- **Make Passwords Case Sensitive**—Specifies that passwords must be entered with the correct combination of uppercase and lowercase letters.
- **Log Failed Connection Attempts**—Causes the host to create a log file containing information on unsuccessful attempts to connect.
- **Prompt on Connection**—Sends a message to the host operator that a connection is being requested by a remote. When this option is checked and a remote user attempts a connection, the host user receives an alert of the impending connection and provides a Yes/No prompt from which the host can choose to allow the connection or not.

Time-out—Specifies how long the host operator has to respond to the Yes/No prompt. If the Disconnect if Timeout box is unchecked, a connection is made automatically after the timeout expires. If checked, the remote caller is disconnected after the expiration of the specified timeout period. This option is grayed if Prompt on Connection is left unchecked.

- **Data Encryption**—Enables data encryption for the host for all data transmitted during a remote control session. Both the host and remote must have Norton pcANYWHERE for Windows, version 2.0, or Norton pcANYWHERE for DOS, version 5.0, to use encryption.

Data Encryption Required to Access this Host—Causes the host to accept only calls from remotes using Norton pcANYWHERE for Windows, version 2.0, or Norton pcANYWHERE for DOS, version 5.0, eliminating the risk of data being transmitted without encryption. This option is grayed if Data Encryption is left unchecked.

- **Maximum Login Attempts per Call**—Specifies how many attempts the user may make to log in correctly. The default value is three attempts; zero indicates an unlimited number of retries is allowed.
 - **Time to Enter Complete Login**—Specifies the time a user has to log in successfully. The default value is three minutes; zero indicates unlimited time to complete the login.
 - **Disconnect if Inactive for**—Specifies the timeout period. Norton pcANYWHERE disconnects the session when no screen data has changed or no keystrokes have been entered for the number of minutes specified. Establishing an inactivity timeout period keeps the telephone line free in case the remote user forgets to end the session. The default value is zero, which indicates an unlimited amount of time. This timeout can be enforced on an individual caller basis by selecting the Caller Subject To Inactivity Timeout check box in the Advanced Caller Options dialog box. See “Advanced Caller Options” later in this chapter.
- 3 Click OK to save the settings and return to the main window.

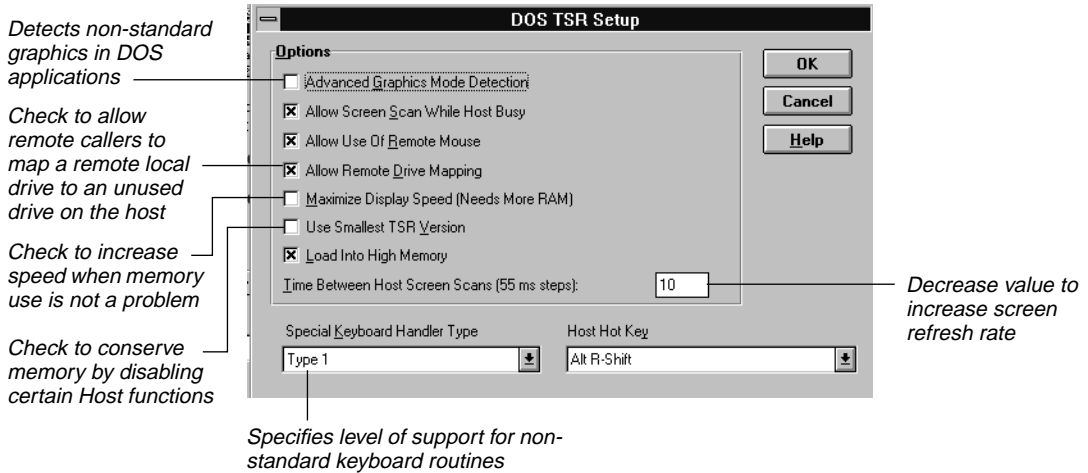
Configuring the DOS TSR

The Norton pcANYWHERE DOS host TSR program allows remote users to maintain or begin a connection to a DOS session without running Windows.

To configure the DOS TSR setup:

- 1 Choose HOST OPERATION from the Configure menu.
- 2 Choose DOS TSR OPTIONS from the submenu.
The DOS TSR Setup dialog box appears (Figure 5-6).

Figure 5-6 DOS TSR options affect full-screen DOS remote sessions only.



3 Check or uncheck the DOS TSR options as desired. Options include the following:

- **Advanced Graphics Mode Detection**—Allows the host to detect non-standard graphics within a DOS application. Checking this check box slows down the remote display, and it should be left unchecked unless the graphics from a host application are difficult to view.
- **Allow Screen Scan While Host Busy**—Keeps remote’s screen as current as possible by scanning host’s screen while it is busy. If unchecked, the host does not allow scanning while it is busy, and the remote screen is updated only after the host has completed its task.
- **Allow Use of Remote Mouse**—Allows the remote user to use his or her mouse in DOS applications run on the host. This feature requires 1K of extra memory.
- **Allow Remote Drive Mapping**—Allows the remote PC to map its drives to the host. Using this feature requires 2K of extra memory, but it allows you to use files on the remote PC as though they were on the host. See “Mapping Drives” later in this chapter.
- **Maximize Display Speed**—Improves the speed of the transfer of the host screen’s data to the remote PC for DOS graphics applications by using an advanced compression technique. (This feature has no effect on Windows or on DOS text mode applications.) It increases the size of the host TSR by 46K.

- Use Smallest TSR Version—Reduces the size of the DOS TSR to conserve memory. This option saves memory by disabling the connection status messages, the Chat Window, pop-up windows, and auditing of connections.

NOTE: Besides checking the smallest TSR version, the host must set the Host Hot Key option to None, and deselect the Prompt on Connection option in the Host Security Options dialog box.

- Load into High Memory—Causes the host to load as many segments of the host TSR as possible into upper memory blocks.
 - Time Between Host Screen Scans (55 ms steps)—Controls the refresh rate of the screen. Each step is equivalent to 55 milliseconds. The smaller the value entered here, the more frequently the screen refreshes. The default value is 10.
 - Special Keyboard Handler Type—Increases the host's ability to handle keystrokes in specific applications (most notably, many 3270 terminal emulation programs). Norton pcANYWHERE offers two types of keyboard handlers. For most of these applications, the Type 1 handler is appropriate and is, therefore, the default choice. The Type 2 handler writes keyboard codes to the keyboard. Although it is faster than Type 1, it may not function on all host PCs. For more information on special keyboard handlers see "Remote Operations" later in this chapter and Appendix B, "Terminal Emulation."
 - Host Hot Key—Specifies the keystroke sequence the host uses to open the Online Menu during a session.
- 4 Click OK to save the settings and return to the main window.

NOTE: You must run pcANYWHERE and configure your hardware and computer name before attempting to load the HOST TSR.

For instructions on how to launch the DOS TSR, see Chapter 6, "Starting a Remote Session."

Configuring Caller Information

The settings available in the caller information dialog boxes allow the host to set privileges or place restrictions on remote callers. In addition, you can assign passwords to maintain host security. Privileges and passwords can be set as defaults that affect all remote callers or they can be set differently for

each caller, allowing the host to specify different privileges for each remote caller. Password-protection increases when you set privileges on an individual basis, because each remote caller uses a unique password.

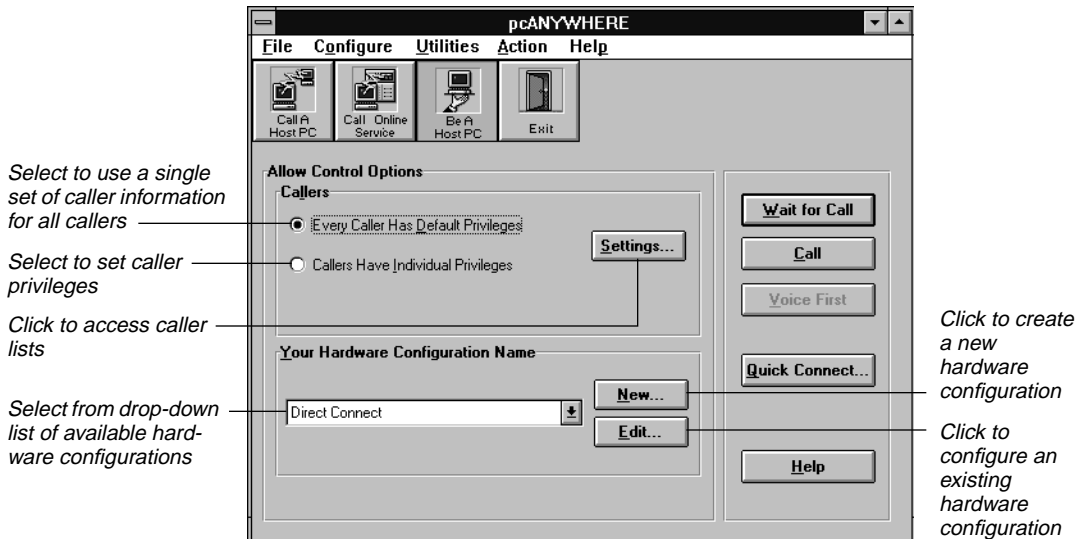
NETWORK USERS: Sometimes the network administrator specifies that the Caller Information file is to be shared by all network users. Ask your network administrator, “Is the Caller Information File *shared* or *personal*?” If it is personal, the host may create a custom list of callers. If the file is shared, the host must use the predefined list of callers set by the network administrator.

To set default privileges:

- 1 Click the Be A Host PC load button.

The host main window appears (Figure 5-7).

Figure 5-7 The host main window lets the host user define a caller information list.



- 2 Select the Every Caller Has Default Privileges option button.
- 3 Click the Settings... button. The Edit Caller Entry dialog box appears (Figure 5-8).
- 4 Click the Login Name text box and type in a login name for this caller.

NOTE: The Login Name text box appears only if the check box was checked in the Host Security Options dialog box (see “Setting Security Options” earlier in this chapter).

- 5 Type a password in the Password text box if one is desired.

Figure 5-8 Passwords may be up to 16 characters in length.

Login Name is required in addition to password if Require Login Names is also checked in the Host Options dialog box

Check to enable remote callback

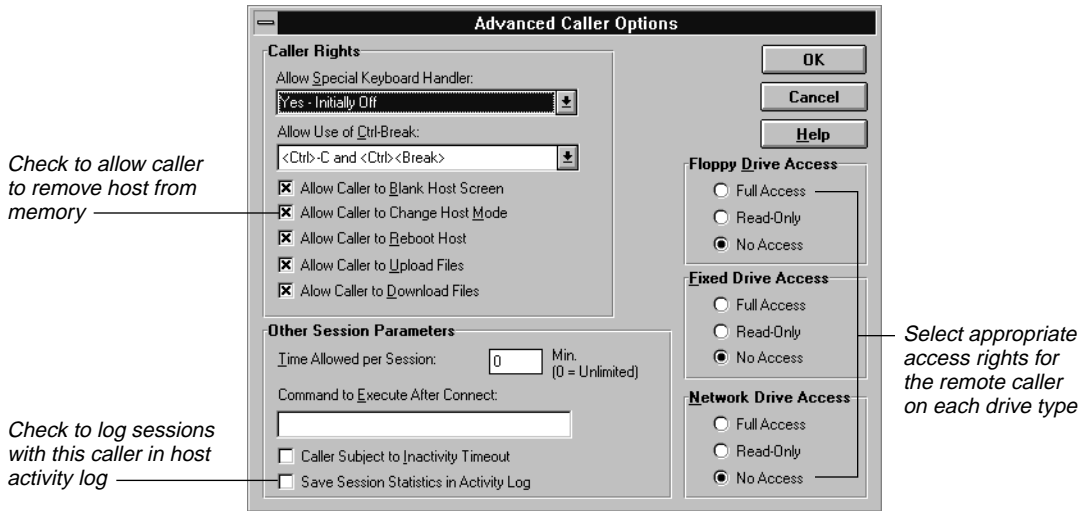
Check to use selected prefix or suffix

Define a password for all callers to use

Select prefix or suffix name

- 6 Enter callback information if the callback operation is desired. When the callback feature is enabled, the host hangs up upon connection with the remote and dials the caller back at the specified telephone number.
- 7 Click the Advanced... button to access additional caller information. The Advanced Caller Options dialog box appears (Figure 5-9) in which you can check or uncheck the following caller options:

Figure 5-9 You can click the Advanced... button to specify optional information. Some options are preset to a default value but can be modified.



- **Allow Special Keyboard Handler**—Specifies whether caller may use special keyboard handling required to run some mainframe terminal emulators. You can block access to such systems by selecting Not Allowed. To allow special keyboard handling select Yes—Initially Off, or specify a default level of support. Level 1 works well for most applications. (See Appendix B, “Terminal Emulation,” for additional information.)
- **Allow Use of Ctrl+Break**—Allows the remote user to use the Ctrl+C or Ctrl+Break key combinations to halt certain applications running on the host.
- **Allow Caller to Blank Host Screen**—Allows the remote user to blank the host screen. The remote user can use this option to prevent others from viewing the activities occurring on the host.
- **Allow Caller to Change Host Mode**—Allows the remote user to change the state in which the host is left when a session ends. The remote caller can end the session and either have the host wait for another call, or disable the host, prohibiting other connections.
- **Allow Caller to Reboot Host**—Allows the remote user to reboot the host machine remotely. The remote user can select the method of reboot from within the Remote Online Menu. Refer to Chapter 8, “Managing Remote Control and Online Sessions,” for more Online Menu information.

- Allow Caller to Upload Files—Allows the remote user to send files to the host PC. If this option is not enabled, the remote caller is also prohibited from performing any operation that modifies the host drive, such as synchronization and cloning.
- Allow Caller to Download Files—Allows the remote user to retrieve files from the host PC. If this option is not enabled, the remote caller is also prohibited from performing any operation that modifies the host drive, such as synchronization and cloning.
- Time Allowed per Session—Specifies the maximum length of a remote session in minutes. Setting this value to anything other than zero causes Norton pcANYWHERE to gracefully end a remote computing session at the time specified. Enter a value between 1 and 9999 minutes. By default, the value is set to zero, which indicates that the caller has an unlimited time to remain online.
- Caller Subject to Inactivity Timeout—Enforces the timeout set in the Disconnect If Inactive For text box of the Host Security Options dialog box. (See “Setting Security Options” earlier in this chapter.) If the remote caller is inactive for the specified period, the host disconnects the remote computing session.
- Save Session Statistics in Activity Log—Enables the host Activity Log. For more information see Chapter 10, “Utilities.”
- Drive Access Options—Restricts the remote caller’s access to drives on the host PC. Select the appropriate option buttons to indicate availability of host drives. For example, the host can allow the remote user no access to the network drives, read-only access on the fixed drives, and read/write access to the floppy drives.

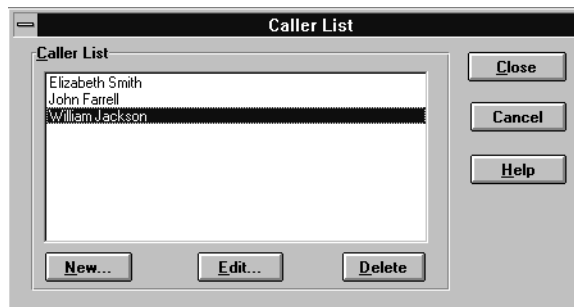
NOTE: A remote caller must have a minimum of read access capability to the directory in which pcANYWHERE is installed.

- 8 Click OK to save the caller options settings and return to the Edit Caller Entry menu.
- 9 Click OK to accept all settings and return to the host main window.

To set individual privileges:

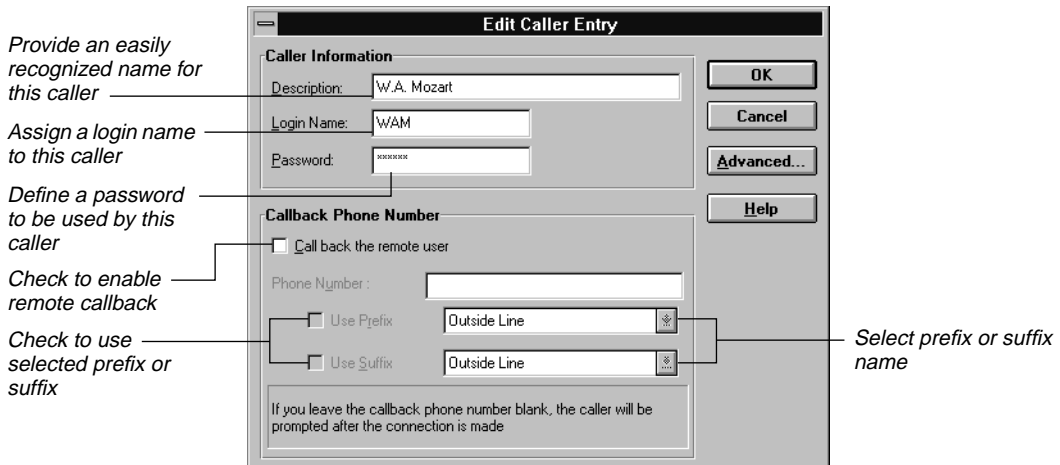
- 1 Click the Be A Host PC load button.
The host main window appears (see Figure 5-7).
- 2 Select the Callers Have Individual Privileges option button.
- 3 Click the Settings... button.
The Caller List dialog box appears (Figure 5-10).

Figure 5-10 The Caller List dialog box contains the names of any callers you have defined.



- 4 Click the New button to add an entry.
The Edit Caller Entry dialog box appears (Figure 5-11).

Figure 5-11 Notice the Description field does not contain <Default Caller>. Enter a descriptive name for this caller.



- 5 Enter a descriptive name for this caller in the Description text box.
- 6 Continue to configure the caller entry and advanced settings just like the default caller entry. Repeat this for as many callers as you wish to list. The number of caller entries that can go into this list is limited only by the space on your disk.
- 7 Click OK to save the settings and return to the Caller List dialog box.

NETWORK USERS: Sometimes the network administrator specifies that the Caller Information file is to be shared by all network users. Ask your network administrator, “Is the Caller Information file *shared* or *personal*?” If it is personal, you may create a custom list of callers. If the file is shared, you must use the predefined list of callers set by your network administrator.

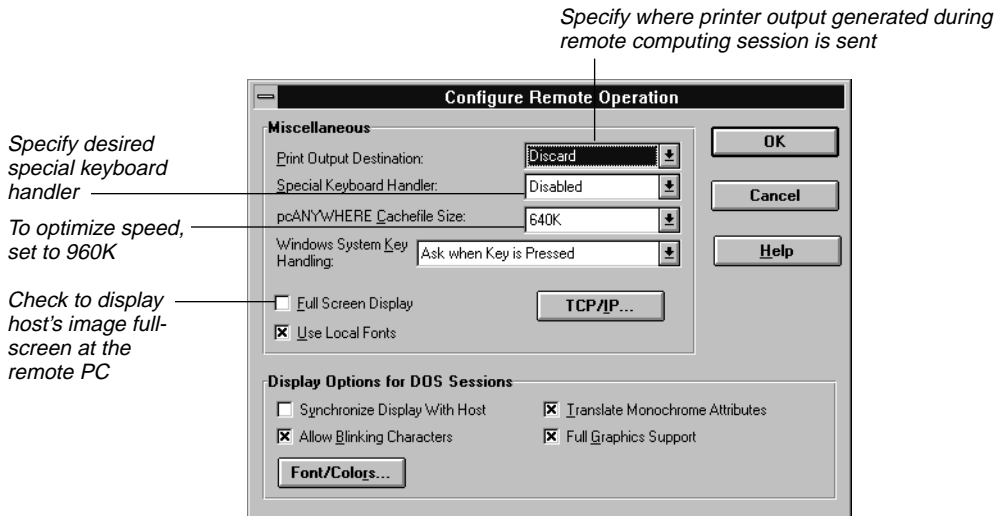
Remote Operations

Remote operations control how the remote interacts with the host. Once set, these options establish a default for *every* remote computing session started from your computer. However, you can change these defaults during a remote computing session if needed; for more information, see Chapter 8, “Managing Remote Control and Online Sessions.”

To specify remote operations:

- 1 Choose REMOTE OPERATION from the Configure menu.
The Configure Remote Operation dialog box appears (Figure 5-12).

Figure 5-12 The Configure Remote Operation dialog box lets you control how the remote interacts with the host.



2 Change the remote options in the Miscellaneous group box as desired.

- **Print Output Destination**—Directs the host's printed output to either the host or remote, or to both host and remote, or discards it completely.
- **Special Keyboard Handler**—Specifies which special keyboard handler to use during a session. This option can be changed during a session by accessing the Remote Online Menu. For more Online Menu and Keyboard Handling information, see Chapter 8, "Managing Remote Control and Online Sessions."
- **pcANYWHERE Cachefile Size**—Specifies the amount of disk space Norton pcANYWHERE uses when caching icon information during a remote control session. This cache file is used only when accessing another Norton pcANYWHERE computer running Windows. It stores icon information locally on the remote computer, thus increasing Windows' display speed.
- **Windows System Key Handling**—Specifies where pcANYWHERE should execute Windows system keystrokes, when used.

Ask when Key is Pressed—Asks the remote user where to execute the system key information each time the system keys are used.

Always Execute Locally—Sends the system key information to Windows on the remote computer.

Always Send to Host—Sends the system key information to Windows on the host computer.

- Full Screen Display—Displays the host image full-screen on the remote PC. If unchecked, the host screen appears in a window.
 - Use Local Fonts—Improves the performance of the session by having the remote use a local font that closely matches the font used at the host. This option is checked by default. If text is not displayed correctly on the remote, uncheck this check box.
 - TCP/IP—Specifies which TCP/IP host to connect to. See the next procedure for instructions on adding TCP/IP hosts.
- 3** Check or uncheck the following Display Options for DOS Sessions:
- Synchronize Display with Host—Slows the host application to the rate at which the remote can display screen activity. If this option is unchecked, some lines of text may scroll off the screen before the remote is able to display them. If the speed of the application is more important than a complete display of all characters, such as with a lengthy database indexing procedure, uncheck this option.
 - Allow Blinking Characters—Controls character blink attributes. Check to allow blinking characters.
 - Translate Monochrome Attributes—Determines which black-and-white colors to use to represent the host color screen. Check when using a remote with a monochrome display to control a DOS application running on a host with a color display.
 - Full Graphics Support—Provides the best possible representation of DOS graphics. Uncheck to improve speed, when an approximation of graphics is acceptable.
 - Fonts/Colors—Determines the background and foreground colors to use during the session as well as the font style and size.
- 4** Click OK to accept the settings and return to the main window.

Adding TCP/IP Hosts

If you want to connect to TCP/IP hosts, only those hosts that are listed in the TCP/IP vendor-provided host list file are available. If you do not have access to this file, ask your system administrator for assistance. See Chapter 3, “Hardware Configurations,” for more information on TCP/IP.

To add TCP/IP hosts:

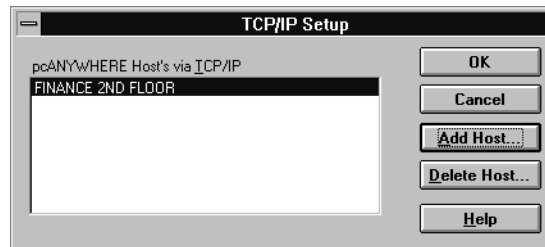
- 1 Choose REMOTE OPERATION... from the Configure menu.

The Configure Remote Operation dialog box appears (see Figure 5-12).

- 2 Click the TCP/IP... button.

The TCP/IP Setup dialog box appears (Figure 5-13).

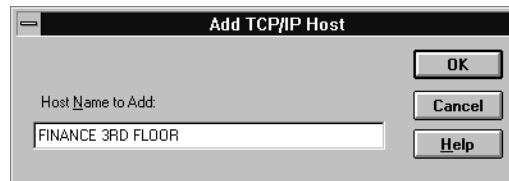
Figure 5-13 The TCP/IP Setup dialog box lists the TCP/IP hosts available.



- 3 Click the Add Host... button to add a new host.

The Add TCP/IP Host dialog box appears (Figure 5-14).

Figure 5-14 The host name must exist in the host list file.



- 4 Enter the name of the TCP/IP host in the Host Name to Add text box. This name is obtained from the TCP/IP vendor-supplied host list file.
- 5 Click OK to add the host and return to the TCP/IP Setup dialog box.
- 6 Click the Add Host button to add additional hosts.

Or,

Click OK to return to the Configure Remote Operation dialog box.

Creating a List of Host PCs

The first time you start the Norton pcANYWHERE remote, you must establish a list of one or more host computers for remote access. Each entry in this list contains dialing instructions and other parameters that the remote uses to connect to the host. You may add to or modify this list at any time.

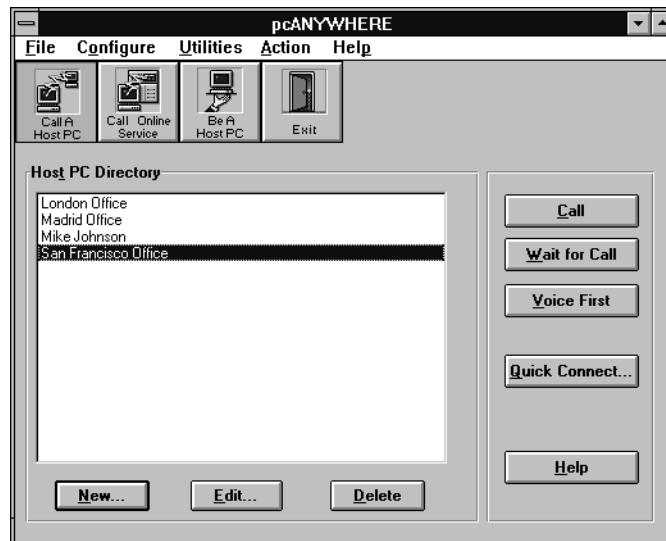
NETWORK USERS: If your network administrator specified a *shared* “Host PC Directory” file during network installation, you cannot add to or modify the host list. In this case you may access only the hosts specified by your network administrator. For more information, see Chapter 2, “Installation and General Setup.”

To create a list of hosts to call:

- 1 Click the Call A Host PC load button.

The Norton pcANYWHERE remote main window appears (Figure 5-15).

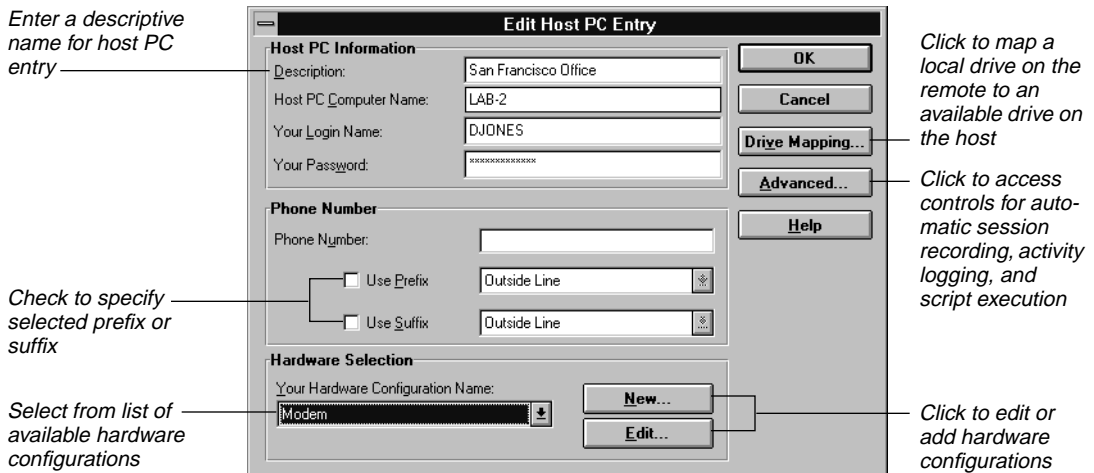
Figure 5-15 Enter Host PC information before clicking the Call button.



- 2 Click New... to add a host PC entry.

The Edit Host PC Entry dialog box appears (Figure 5-16).

Figure 5-16 Optional Host PC Computer Name and Host PC Login and Password entries help automate the connection.



- 3 Type a descriptive name for this host in the Description text box.
- 4 Type the host telephone number in the Phone Number text box if you use a modem to connect to this host.
- 5 Select a hardware configuration from the Your Hardware Configuration drop-down list box. See Chapter 3, “Hardware Configurations,” for additional information.
- 6 Click Advanced... if you need Norton pcANYWHERE to record the session, run a script, or log the session statistics. For information on all the utilities in the Advanced Host Options dialog box, see Chapter 10, “Utilities.”
- 7 Click OK.
- 8 Repeat steps 2 through 7 for each host PC you want to add to the list.

Optional Host PC Name and Password

You can automate connections to network hosts and gateways by entering the host PC’s computer name and any login name or password the host PC is expecting from you. The remote’s settings for the host computer name, login name, and host password options must match those defined on the host PC.

If you leave this field blank, the host PC presents you with a list of available hosts or gateways from which to choose at the time of connection.

If you leave the login name or password field blank and the host requires one, the host prompts you for a password upon connection. (See “Setting Security Options” earlier in this chapter.)

Mapping Drives

Drive mapping allows easy accessibility to a remote’s drives during a remote control session. You can map remote drives to unused drives on the host. The remote drives appear as additional drives on the host. For example, if the host has drive T: available, you could map the remote’s C: drive as the host’s T: drive. Then, as the remote user in a remote control session, selecting drive T: on the host gives you access to the files on drive C: of the remote PC.

Mapping allows an application running on the host to access data on the remote PC. For example, you can attach a file from the remote PC to an electronic mail message on the host PC without transferring the file to the host first.

To map remote drives to the host PC:

- 1 Click the Call A Host PC load button.

The Norton pcANYWHERE remote main window appears (see Figure 5-15).

- 2 Click the New... button to add a host PC entry.

Or,

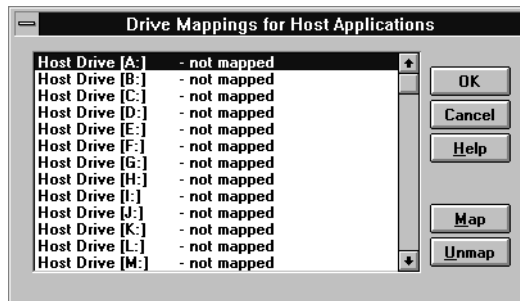
Click the Edit... button to edit an existing entry.

The Edit Host PC Entry dialog box appears (see Figure 5-16).

- 3 Click the Drive Mapping... button.

The Drive Mappings for Host Applications dialog box appears (Figure 5-17).

Figure 5-17 Check with the host user to determine what drive letter is available to use on the host.



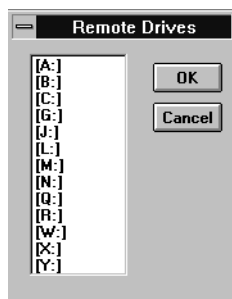
- 4 Select an available host drive to which you will map your remote drive.

NOTE: The host drive availability depends on the LASTDRIVE = statement in the Host's AUTOEXEC.BAT file. For example, if the LASTDRIVE statement is equal to F:, the host has up to drive E: available for mapping.

- 5 Click the Map button.

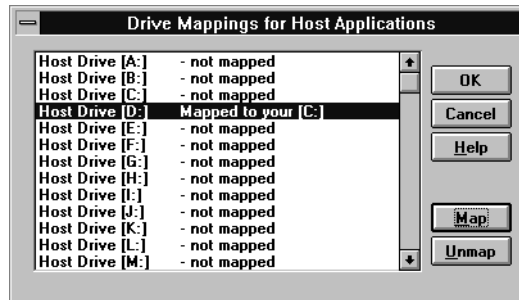
The Remote Drives dialog box appears (Figure 5-18).

Figure 5-18 Select the remote's drive letter you wish to map to the host's available drive.



- 6 Select the drive on the remote that you wish to have mapped to the host drive selected in step 4 above.
- 7 The Drive Mappings list box in the Drive Mappings for Host Applications dialog box now shows the host drive mapping (Figure 5-19).

Figure 5-19 The Drive Mappings dialog box displays the mapped drives.



- 8 Click OK to accept the mapping and return to the Edit Host PC Entry dialog box.

To unmap drives:

- 1 Click the Call A Host PC load button.
The Norton pcANYWHERE remote main window appears (see Figure 5-15).
- 2 Click the Edit... button to edit the host entry containing the drive mapping.
The Edit Host PC Entry dialog box appears (see Figure 5-16).
- 3 Click the Drive Mapping... button.
The Drive Mappings for Host Applications dialog box appears (see Figure 5-19).
- 4 Click the mapped host drive you want to unmap.
- 5 Click the Unmap button.
- 6 Click OK to accept the unmapping and return to the Edit Host PC Entry window.

NOTE: If the host is using the host DOS TSR, drive mapping may not be available to the remote caller. The host user can disallow the use of drive mapping. See “Configuring the DOS TSR” earlier in this chapter.

Starting a Remote Control Session

6

This chapter explains how to start a Norton pcANYWHERE remote control session in which one PC remotely controls another. Whether you are connecting over phone lines to a computer in another city, or over a local area network to a computer down the hall, the connect procedures are very similar. The host screen appears on the remote PC and, in general, the remote user can access any of the host's files and applications.

Norton pcANYWHERE makes the connection using information from the hardware configuration on each PC, the session configuration used by the remote PC, and any caller privileges used by the host PC. Be sure to complete the necessary installation and configuration procedures described in Chapter 3, "Hardware Configurations," and Chapter 5, "Configuring Norton pcANYWHERE," before beginning.

This chapter covers:

- Initiating a remote control session from either the host or remote PC while the other waits
- Starting the host
- Starting the remote
- Using gateways for a remote control session

Starting the Host PC

The host is the PC that is controlled by the remote after making a connection. Before loading the host, be sure to follow the configuration procedures described in Chapter 5, "Configuring Norton pcANYWHERE."

Running the host loads the Norton pcANYWHERE host program into memory with the selected session and program options. Once the host has been loaded, you are ready to begin a remote control session.

There are five ways to load a host:

- Wait for Call—Causes the host to wait for a remote user to call.
- Call—Causes the host to dial a remote that is waiting for a connection.
- Voice First—Allows the host to establish a voice connection with the remote user first and then activate your remote control session without disconnecting.
- Quick Connect—Allows the host user to quickly load the host without first establishing hardware configurations or caller privileges.
- Auto Start—Loads the host automatically each time Windows is run (see Chapter 5, “Configuring Norton pcANYWHERE”).

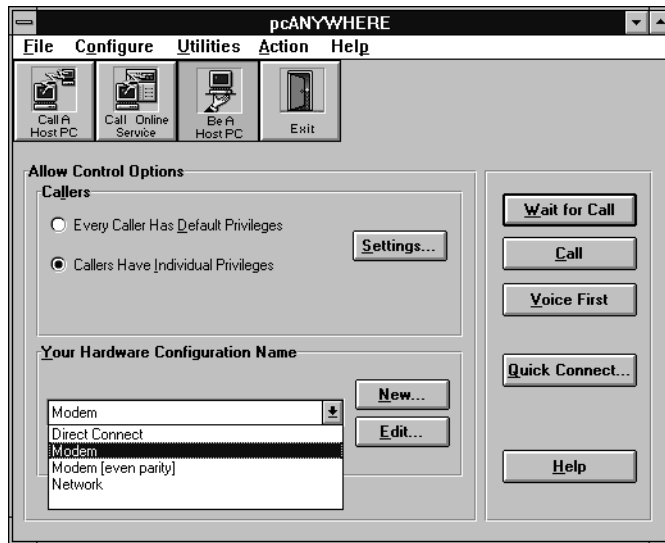
CAUTION: Whatever method you use to load the host, be sure you have first selected an appropriate hardware configuration from the Your Hardware Configuration Name group box (see Figure 6-1). If your hardware or communications device changes, select a new hardware configuration. See Chapter 3, “Hardware Configurations,” for more information.

To have the host wait for a call:

- 1 Click the Be A Host PC load button.

The Norton pcANYWHERE Host main window appears (Figure 6-1).

Figure 6-1 You can edit the existing default hardware configurations or create new ones.



- 2 Click the Wait for Call button.

The pcANYWHERE Waiting... dialog box appears and the main Norton pcANYWHERE window closes. The current status of the connection is displayed. Upon connection, a prompt appears asking the remote user to enter a password. After the password is entered correctly, the host image appears in a pcANYWHERE Session window on the remote display, and the remote computing session begins. For information on session control see Chapter 8, "Managing Remote Control and Online Sessions." For information on file transfer, see Chapter 9, "File Transfer."

NOTE: If you have checked the Minimize When Waiting for a Call check box in the Host General Options dialog box, the pcANYWHERE Waiting dialog box appears as an icon.

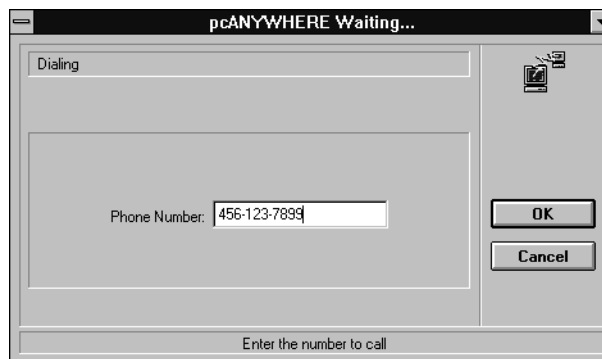
Initiating the Session from the Host PC

The host PC usually is set up to wait for the connection from a remote PC. The host can also initiate the phone call to the remote. After connecting, however, it is still the remote PC that takes control over the host.

To call a remote:

- 1 Click the Be A Host PC load button.
The Norton pcANYWHERE Host main window appears.
- 2 Click Call.
The pcANYWHERE Waiting dialog box appears and the main pcANYWHERE window closes (Figure 6-2).

Figure 6-2 The pcANYWHERE Waiting... dialog box on the host screen waits for the host user to enter the phone number of the remote PC.



- 3 Type the remote's telephone number in the Phone Number text box.
- 4 Click OK.
- 5 The host dials the remote. The current status of the connection is displayed while waiting for the remote to answer. If the host has been configured to require login names and passwords from remote callers, upon connection a prompt appears asking the remote user to enter them.

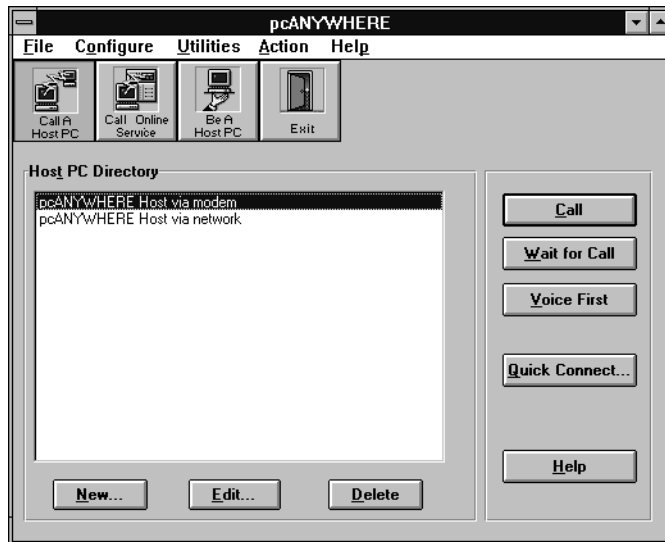
NOTE: Although the host PC called the remote, after connecting, the remote PC takes control of the session.

The host image appears in a pcANYWHERE Session window on the remote display, and the remote computing session begins. For information on session control, see Chapter 8, "Managing Remote Control and Online Sessions." For information on file transfer, see Chapter 9, "File Transfer."

To call a remote with voice confirmation:

- 1 Click the Be A Host PC load button.
The Norton pcANYWHERE Host main window appears.
- 2 Pick up your telephone, dial the remote, and establish a voice connection.
- 3 Instruct the remote user to start Norton pcANYWHERE remote, then click Voice First in the remote's main window (Figure 6-3).

Figure 6-3 You can edit the default host entries or create new ones.



- 4 Hang up the voice telephone receiver when prompted. The remote user does the same.

Norton pcANYWHERE displays the current status of the connection while waiting for the session to begin. If the host has been configured to require login names and passwords from remote callers, upon connection, a prompt appears asking the remote user to enter them. After the password is correctly entered, the host's image appears in a pcANYWHERE Session window on the remote, and the remote computing session begins. For information on session control, see Chapter 8, "Managing Remote Control and Online Sessions." For information on file transfer, see Chapter 9, "File Transfer."

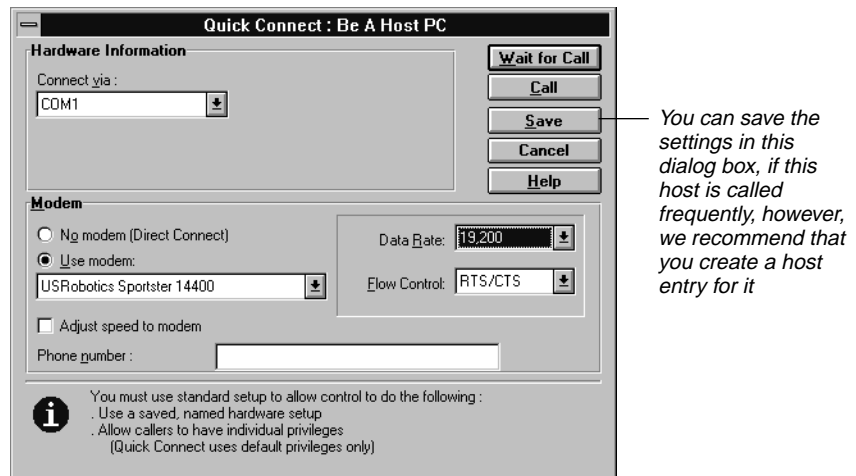
Using Quick Connect to Load a Host

Quick Connect gives you the ability to quickly load the host without creating hardware configurations or caller privileges. In the Quick Connect dialog box, you only need to specify the modem port if you are using a modem, or the network drivers if you are on a LAN. Depending on which connect device you select, other options appear. For example, if you select COM1 as your connect device, data rate, flow control, and modem options appear. If you select NetWare IPX as your connect device, no other options appear.

To load a host using Quick Connect:

- 1 Click the Be A Host PC load button.
The Norton pcANYWHERE Host main window appears.
- 2 Click the Quick Connect... button.
The Quick Connect: Be A Host PC dialog box appears (Figure 6-4).

Figure 6-4 The Quick Connect dialog box includes the minimum settings needed to make a connection.



- 3 Select the device to use for the connection from the Connect Via drop-down list box.

If you select any of the network devices such as NetWare IPX, NetBIOS, or Banyan VINES, no other settings are required.

If you select NASI/NCSI, Telebit ACS, or TCP/IP, refer to Chapter 3, “Hardware Configurations,” for information on available settings.

If you select a serial connection type (COM1 through Int 14) you need to set the following:

- Use modem—Select this button if you are making a serial modem connection and select your modem from the drop-down list box. If your modem does not appear in the list, refer to your modem's manual to determine a compatible selection, or select Hayes Compatible.

Or,

No modem—Select this button if your PCs are directly connected by a null modem cable (see Appendix A, "Technical Information" for information on cables).

- Adjust Speed to Modem—Check if you want the serial port speed to adjust to match the connect speed of the modem. Check this option if remote callers are connecting at various speeds.
 - Data Rate—A default data rate is set depending on the modem selected. You can raise or lower this speed as necessary.
 - Flow Control—RTS/CTS is the default setting and in most cases, does not need to be changed. XON/XOFF is only used in connections with online services. Do not select this option if you are making a pcANYWHERE remote control connection.
 - Phone Number—Type the phone number of the host.
- 4 Click the Save button if you want to save the Quick Connect dialog box selections. The selected parameters appear the next time you access Quick Connect.

NOTE: Quick Connect is a convenience provided to make one or two calls to a particular host or remote. Each time you save new settings in the Quick Connect dialog box, the previous settings are overwritten. If you intend to call a particular host or remote more than once, we recommend that you configure an entry for that host. See Chapter 5, "Configuring Norton pcANYWHERE" for information on creating a host entry.

- 5 Click Wait For Call to load the host and wait for a remote to call.
- Or,
- Click Call to load the host and call a remote.

Canceling a Host Session

If you change your mind after loading a host, you can disable or cancel the host session. Disabling the session deactivates the host, but leaves the host in memory. Canceling the session removes the host from memory.

To disable a waiting host:

- 1 Click the Cancel button in the pcANYWHERE Waiting... status window.

Or,

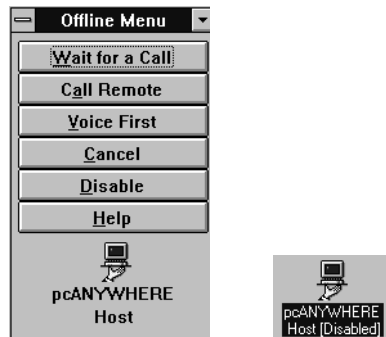
Double-click the pcANYWHERE Waiting icon to open the status window, then click Cancel.

The pcANYWHERE Host confirmation box appears asking you if you wish to Cancel pcANYWHERE.

- 2 Click No.

The Offline Menu appears (Figure 6-5).

Figure 6-5 You can reload, cancel, or disable the host from the Offline Menu.



- 3 Click DISABLE.

The host is disabled and minimized as an icon (see Figure 6-5).

To reload a disabled host:

- 1 Double-click the Host [Disabled] icon.

The Offline Menu appears (see Figure 6-4).

- 2 Choose one of the following:
 - **WAIT FOR A CALL**—Causes the host to wait for a remote user to call.
 - **CALL REMOTE**—Causes the host to dial a remote waiting for a connection.
 - **VOICE FIRST**—Enables the host to establish a voice connection first with the remote user before activating the remote control session.

To cancel a disabled host:

- 1 Double-click the Host [Disabled] icon.
The Offline Menu appears (see Figure 6-4).
- 2 Click **CANCEL**.
A confirmation box appears asking if you want to cancel pcANYWHERE.
- 3 Click **Yes**.
The host is removed from memory and you are returned to the Windows main menu.

Loading the DOS Host TSR

The Norton pcANYWHERE DOS Host TSR is only required to support DOS sessions from the command line outside of Windows. Starting the TSR is not necessary to run the host's DOS applications on a remote within a window. The DOS Host options are configured within Norton pcANYWHERE for Windows. You can load the TSR from the DOS command line or from your AUTOEXEC.BAT file.

NOTE: The DOS TSR cannot be loaded from within a window's DOS box. You must exit Windows completely to load the DOS TSR.

To start the DOS Host TSR from the command line:

- 1 Run pcANYWHERE for Windows and set up the host with the correct hardware configuration and DOS TSR options. See Chapter 5, "Configuring Norton pcANYWHERE" for information on how to configure your host.
- 2 Exit Windows.

- 3 To cause the TSR to wait for an incoming call, at the DOS prompt type:

```
pathname/AW_HOST -W=winpath -P=configpath -M=W
```

Or,

To cause the TSR to wait in the background for an incoming call and allow the host PC to be used for other applications while waiting, type:

```
pathname/AW_HOST -W=winpath -P=configpath -M=A
```

Replace *pathname* with the full path and name of the directory you selected for Norton pcANYWHERE during installation or the network path specified by your network administrator. Replace *winpath* with the full path and the name of the directory where Windows is located on your computer. Replace *configpath* with the name of the directory that contains your pcANYWHERE configuration files. See Appendix A, “Technical Information,” for details.

NETWORK USERS: If Norton pcANYWHERE has been installed on a network, be sure to include the `-I=userid` command-line option as part of the command line. Replace *userid* with the same ID you used to start the network installation of Norton pcANYWHERE; for example: `pathname/AW_HOST -W=winpath -p=configpath -I=userid -M=W`

Starting the Remote

Start the Norton pcANYWHERE remote on the computer that you are using to control a host. Before starting the remote, be sure to follow the configuration procedures described in Chapter 5, “Configuring Norton pcANYWHERE.”

Initiating the Session from the Remote PC

As the remote user, you can initiate the remote control session from the remote PC. You can connect to the host using a variety of hardware configurations. If you are using a modem hardware configuration, you can also switch from voice communication to data communication. See the procedure “To call a host with voice confirmation,” later in this section.

Loading the remote connects you to a host and begins the remote computing session. There are four ways to load the remote:

- Call Host PC—Causes the remote to dial a host. This is the most commonly used method.

- Wait for Call—Causes the remote to wait for a host to call.
- Voice First—Allows the remote user to establish a voice connection first before activating the remote control session.
- Quick Connect—Allows the remote user to quickly connect to a host without configuring hardware settings or host information.

To call a host:

- 1 Click the Call A Host PC load button.
- 2 Select the name of a Host PC in the Host PC Directory list box (see Figure 6-3).
- 3 Click the Call button.

The remote dials the host. The current status of the connection appears on the remote's screen while the remote waits for the host to answer.

If the host has been configured to require login names or passwords, a prompt appears asking you to enter them at the time of connection.

- 4 Enter your login name and password if required.
- 5 Click OK.

The host's image appears in a pcANYWHERE Session window on the remote display, and the remote computing session begins. For information on session control, see Chapter 8, "Managing Remote Control and Online Sessions." For information on file transfer, see Chapter 9, "File Transfer."

NOTE: If your password or login name was specified in the Host PC Directory entry for the host you are calling, they are entered automatically upon connection, and the remote user is not prompted for them. The host image appears in a pcANYWHERE remote Session window and the remote computing session begins. For more information on host password settings see Chapter 5, "Configuring Norton pcANYWHERE."

To wait for a call:

- 1 Click the Wait for Call button (see Figure 6-3).

The pcANYWHERE Waiting... dialog box appears and the remote PC waits for the host to call.

If the host configuration requires login names and passwords, you are prompted to enter them upon connection.

- 2 Enter your password and login name if required.

3 Click OK.

The host image appears in a pcANYWHERE Session window on the remote, and the remote computing session begins. For information on session control see Chapter 8, “Managing Remote Control and Online Sessions.” For information on file transfer see Chapter 9, “File Transfer.”

To call a host with voice confirmation:

- 1** Pick up your telephone, dial the host, and establish a voice connection.
- 2** Instruct the host user to click the Be A Host PC load button and to click the Voice First button on the host’s main window.
- 3** Click Voice First in the remote’s main window.
- 4** Click OK when you are finished with the voice conversation and ready to begin the remote computing session.

The current status of the connection appears in the window while the remote waits for the connection to be made. If the host is configured to require login names and passwords, the remote user is prompted to enter them upon connection. The host’s image appears in a pcANYWHERE Session window on the remote, and the remote computing session begins. For information on session control, see Chapter 8, “Managing Remote Control and Online Sessions.” For information on file transfer, see Chapter 9, “File Transfer.”

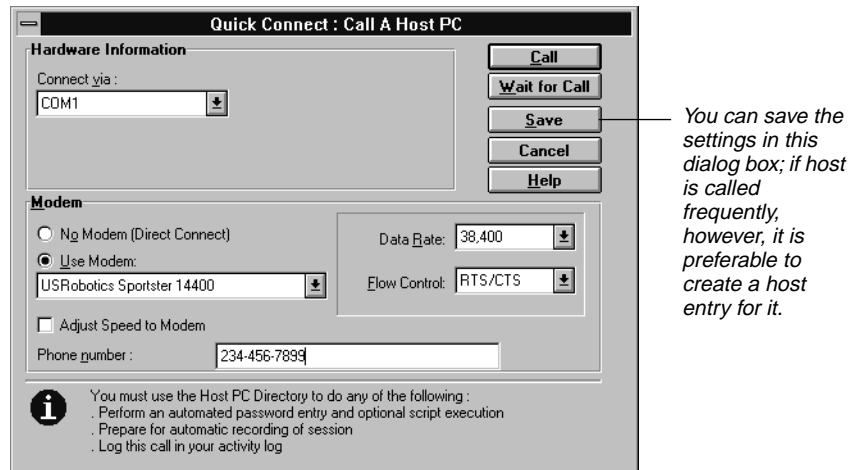
Using Quick Connect to Connect with a Host

Quick Connect gives you the ability to quickly connect to a host without first configuring hardware or host information. In the Quick Connect screen, you only need to specify the connect device from the Connect Via drop-down list box. Depending on which connect device you select, other options appear. For example, if you select COM1 as your connect device, data rate, flow control, and modem options appear. If you select NetWare IPX as your connect device, no other options appear.

To call a host with Quick Connect:

- 1** Click the Call A Host PC load button.
The Norton pcANYWHERE main window appears.
- 2** Click Quick Connect....
The Quick Connect: Call A Host PC dialog box appears (Figure 6-6).

Figure 6-6 The Quick Connect dialog box includes the minimum settings needed to connect.



- 3 Select the device to use for the connection from the Connect Via drop-down list box.

If you select any of the network devices such as NetWare IPX, NetBIOS, or Banyan VINES, no other settings are required.

If you select NASI/NCSI, Telebit ACS, or TCP/IP, refer to Chapter 3, “Hardware Configurations,” for information on available settings.

If you select a serial connection type (COM1 through Int 14) you need to set the following:

- Use Modem—Select this button if you are making a serial modem connection and select your modem from the drop-down list box. If your modem does not appear in the list, refer to your modem’s manual to determine a compatible selection, or select Hayes Compatible.

Or,

No Modem—Select this button if your PCs are directly connected by a null modem cable (see Appendix A, “Technical Information” for information on cables).

- Adjust Speed to Modem—Check if you want the serial port speed to adjust to match the connect speed of the modem. Check this option if remote callers are connecting at various speeds.
- Data Rate—A default data rate is set depending on the modem selected. You can raise or lower this speed as necessary.

- Flow Control—RTS/CTS is the default setting and in most cases, does not need to be changed. XON/XOFF is only used in connections with online services. Do not select this option if you are making a pcANYWHERE remote control connection.
 - Phone Number—Type the phone number of the host.
- 4 Click the Save button if you want to save the Quick Connect dialog box selections. The selected parameters appear the next time you access Quick Connect.

NOTE: Quick Connect is a convenience provided to make one or two calls to a particular host. Each time you save new settings in the Quick Connect dialog box, the previous settings are overwritten. If you intend to call a particular host more than once, we recommend that you configure a host entry for that host. See Chapter 5, "Configuring Norton pcANYWHERE" for information on creating a host entry.

- 5 Click Call to have the remote begin the call to a host.
Or,
Click Wait for Call to have the remote wait for a call from a host.

Connecting through a Gateway

A Norton pcANYWHERE Gateway allows network users to share a single communications device attached to a network station. Because the gateway operates in the background, the CPU on which the gateway is configured can devote at least 90 percent of its processing time to other tasks.

Using an Incoming Gateway

To use an incoming gateway, create a gateway configuration and load it as described in Chapter 4, "Gateways."

Starting the Host

Start the Norton pcANYWHERE Host on the network station that you want to control remotely. Before loading the host, you must set certain session options. These options specify host operations that affect the remote computing session. For more information see "Setting Up A Host" in Chapter 5, "Configuring pcANYWHERE."

NOTE: The callback feature is not available through gateway connections.

To start the host for a gateway connection:

- 1 Click the Be A Host PC load button.
The pcANYWHERE Host main window appears.
- 2 Click the Your Hardware Configuration Name prompt button and select the name of a network configuration. For more information on network hardware setups see “Creating a Node Hardware Configuration” in Chapter 3, “Hardware Configurations.”
- 3 Click the Wait For Call button.
pcANYWHERE prepares your computer to be remotely controlled by initializing the selected communications device.

Starting the Remote

Start the remote on your computer. In most cases, the remote uses a modem to call the gateway, which in turn connects to a host.

To connect to a host using an incoming gateway:

- 1 Click the Call A Host PC load button.
The pcANYWHERE remote window appears.
- 2 Select the host PC name from the Host PC Directory list. For information on creating a host PC entry, see Chapter 5, “Configuring Norton pcANYWHERE.”
- 3 Click the Call button.
The remote dials the gateway. Upon connection, a list of available hosts appears. If you specified a Host PC Computer Name in the Edit Host PC Entry dialog box, the gateway automatically connects to the named host, and you will not have to select a host from the list.
If the host is configured to require login names and passwords, the remote user is prompted to enter them upon connection. If the remote user specified the password and login name in the Edit Host PC Entry dialog box, they are entered automatically upon connection. For more information on editing the Host PC Entry, see “Creating a List of Host PC’s” in Chapter 5, “Configuring Norton pcANYWHERE.”
- 4 Enter the login name and password if required.

- 5 Click OK to begin the remote computing session.

The host's image appears in a pcANYWHERE Session window on the remote's screen, and the remote computing session begins. For information on session control, see Chapter 8, "Managing Remote Control and Online Sessions." For information on file transfers see Chapter 9, "File Transfers."

Using an Outgoing Gateway

To use an outgoing gateway, create a gateway configuration and load it as described in Chapter 4, "Gateways."

Starting the Host

Start the Norton pcANYWHERE Host on the computer that you want to control remotely. Before loading the host, you must set certain session options. These options specify host operations that affect the remote computing session. For more information see "Setting Up A Host" in Chapter 5, "Configuring Norton pcANYWHERE." For more information on gateways, see Chapter 4, "Gateways."

To start the host :

- 1 Click the Be A Host PC load button.

The pcANYWHERE Host main window appears.

- 2 Click the Your Hardware Configuration Name prompt button and select the name of a modem hardware configuration from the drop-down list. For more information see Chapter 3, "Hardware Configurations."

- 3 Click the Wait For Call button.

The pcANYWHERE Waiting... status box appears or the pcANYWHERE Waiting Icon appears if the host user checked the Minimize While Waiting for a Call option in the host's configuration.

Starting the Remote

A gateway is a PC on a network that is dedicated to routing incoming and outgoing calls. To access a gateway PC, the remote uses a node (network) hardware configuration. Be sure you have checked the Use Gateway check box in the Edit Hardware Configuration Entry dialog box before you try to call out of a gateway. The Use Gateway option allows you to access one or

more Norton pcANYWHERE Gateways on the local area network. (For more information on node hardware configurations see “Creating a Node Hardware Configuration” in Chapter 3, “Hardware Configurations.”)

To connect to a host using an outgoing gateway:

- 1 Click the Call A Host PC load button.

The pcANYWHERE remote window appears.

- 2 Select the host name in the Host PC Directory list box.

The host entry should have the network node hardware configuration selected. The hardware configuration must have the Use Gateway check box checked.

- 3 Click the Call button.

If your hardware configuration specifies a particular gateway, the process of connecting through the gateway is handled automatically by pcANYWHERE.

Enter a login name and password, if prompted to. If the remote user specified the password and login name in the Edit Host PC Entry dialog box, they are entered automatically upon connection. For more information on editing the Host PC Entry, see “Creating a List of Host PCs” in Chapter 5, “Configuring Norton pcANYWHERE.”

- 4 Click OK.

The host’s image appears in a pcANYWHERE Session window on the remote display, and the remote computing session begins. For information on session control, see Chapter 8, “Managing Remote Control and Online Sessions.” For information on file transfers, see Chapter 9, “File Transfers.”

Online Services

7

This chapter explains how to start a Norton pcANYWHERE online service session. An online service is a service such as CompuServe, Dow Jones, MCI Mail, or an electronic bulletin board service (BBS). The service may be on another PC, a mainframe, or a minicomputer. Online services offer information on a vast variety of topics. Each service usually has its own set of procedures by which you identify yourself and log in. During an online session, your PC mimics (emulates) the type of terminal that the service uses to communicate. Norton pcANYWHERE provides several terminal emulation types and file transfer protocols commonly used by online services. Each service will tell you which of these to use.

Whether you are using an online session to connect directly to a mainframe computer or to connect to a BBS over telephone lines, the procedures are very similar. Norton pcANYWHERE makes the connection using information from the hardware configuration as well as information provided in the Edit Online Service Entry dialog box. If you are using a gateway and the modem for your PC is part of that gateway, be sure to use a node hardware configuration.

This chapter is for users who need to:

- Connect to a BBS or other dial-up information service.
- Connect to a minicomputer, mainframe, or other multi-user system.
- Connect through a Norton pcANYWHERE Gateway to a BBS, information service, minicomputer, or mainframe.

Customizing Terminal Emulation

Norton pcANYWHERE offers default settings for quick and easy startup, along with customization options to adapt to the most demanding circumstances. These customization options allow you to tailor terminal emulation performance to your exact needs and preferences.

Customization options include:

- Terminal emulation settings—Includes options that control how data is displayed on your monitor

- Macro keys—Assigns predefined actions to specified key combinations
- Translation tables—Redefines incoming and outgoing character codes

Configuring Terminal Settings

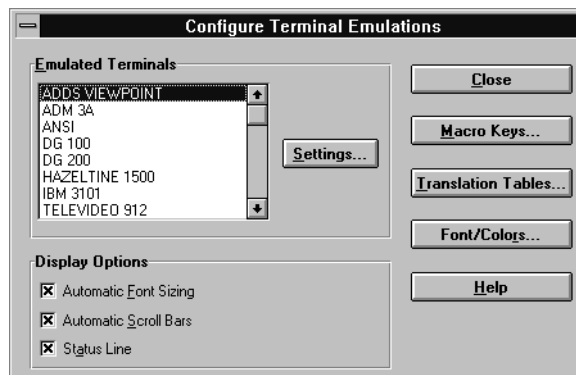
Norton pcANYWHERE includes a wide variety of the most commonly used terminal emulators. Although most users do not need to adjust terminal settings, you can customize each of the terminal emulators to your needs and preferences. Terminal settings specify how each type of emulation operates on your computer. These settings involve both display and keyboard performance.

To configure a terminal emulator:

- 1 Choose TERMINAL EMULATIONS... from the Configure menu.

The pcANYWHERE Configure Terminal Emulations dialog box appears (Figure 7-1).

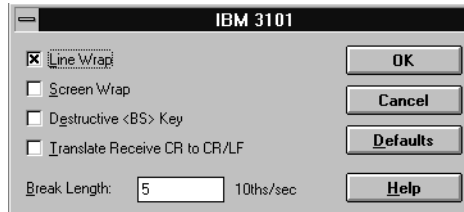
Figure 7-1 Terminal emulation settings fine-tune performance.



- 2 Select the name of the emulation type that you want to configure. For a list and description of Norton pcANYWHERE terminal emulation types see Appendix B, "Terminal Emulation."
- 3 Click Settings....

The configuration dialog box for the selected emulation type appears (Figure 7-2).

Figure 7-2 To restore the original settings, click the Defaults button.



Select terminal configuration options.

- **Line Wrap**—Determines how your monitor displays lines that exceed the width of the terminal display window. If Line Wrap is checked, lines that exceed the width of the display window continue on the next line. When the cursor reaches the far right side of the screen, the next character appears in the first position on the next line. If Line Wrap is unchecked, the cursor remains on the same line until a line feed is received.
 - **Screen Wrap**—Controls what happens when the entire screen is filled. If Screen Wrap is unchecked, the display scrolls, discards the top line of the display, and displays the new line at the bottom of the screen. If Screen Wrap is checked, the next line overwrites the top line when the cursor reaches the last position on the last line of the terminal display window.
 - **Destructive <BS> Key**—Causes the backspace key to act as a destructive backspace, that is to delete characters as it passes over them. If this option is unchecked, the backspace key will move the cursor to the left without deleting characters.
 - **Translate Received CR To CR/LF**—Causes the cursor to move to the left side of the terminal display window and to advance one line each time a carriage return character is received. Check this option only if the display does not scroll vertically as expected.
 - **Break Length**—Specifies the length of the break signal used to interrupt programs running on a mainframe or minicomputer. (This break should not be confused with the Ctrl+Break key combination, which sends a control character. This break is a sustained low signal used in online communications.) Do not alter the default break length setting of 5 unless required to by a specific online service.
- 4 Click OK to save the changes and return to the Configure Terminal Emulation dialog box to configure remaining options.

- 5 Check or uncheck the following Display Options:
 - Automatic Font Sizing—Causes Norton pcANYWHERE to automatically select the font size displayed on the remote screen, based upon the size of the terminal window.
 - Automatic Scroll Bars—Causes the screen to display horizontal and vertical scroll bars.
 - Status Line—Causes display of a status line at the bottom of the screen. This status line contains the terminal type, communication port, data rate, parity, and flow control being used.

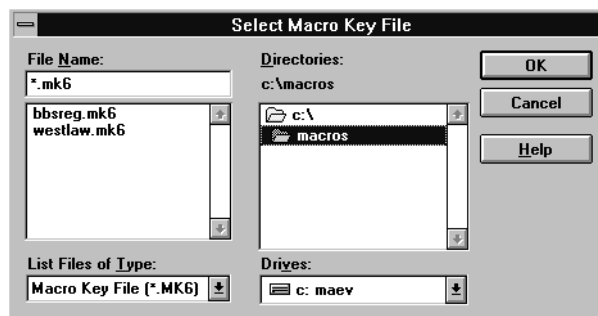
Setting Up Macro Keys

Macro keys are key combinations used for user-defined functions associated with them, such as keyboard commands, to run a script file, or to execute a program. You may specify up to ten different macro keys for use during Norton pcANYWHERE terminal emulation sessions. Macro keys are stored in files with the extension .MK6.

To set up a macro key:

- 1 Choose **TERMINAL EMULATIONS...** from the Configure menu.
The pcANYWHERE Configure Terminal Emulations dialog box appears (see Figure 7-1).
- 2 Click the **Macro Keys...** button.
The Select Macro Key File dialog box appears (Figure 7-3).

Figure 7-3 Select a macro key file from the File Name list box.



- 3 Select a path for the macro key files. You can accept the default directory (where Norton pcANYWHERE is installed) or enter a new directory.

- 4 If a macro file has been defined, select the name of the file you wish to enable from the File Name list box.

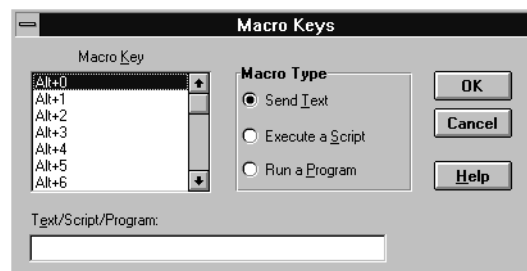
Or,

If you wish to create a macro file, type a filename in the File Name text box.

- 5 Click OK.
- 6 Click Yes to create a macro.

The Macro Keys dialog box appears (Figure 7-4).

Figure 7-4 Up to 10 macros can be assigned for use online.



- 7 Select a key combination from the Macro Key list box.
- 8 Select an option button in the Macro Type group box to specify the macro type:
 - Send Text—Indicates the macro is a command or group of keystrokes to be transmitted.
 - Execute a Script—Indicates the macro is a pcANYWHERE script to be executed.
 - Run a Program—Indicates the macro is a program to be executed.
- 9 In the Text/Script/Program text box, enter macro keystrokes, or a complete path and filename for the Norton pcANYWHERE script to run or the program to execute.
- 10 Click OK to save the macro key settings and return to the Configure Terminal Emulations dialog box.

Setting Up Translation Tables

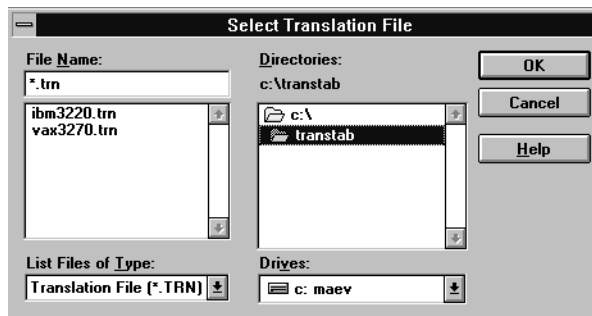
Translation tables translate one character to another. You can translate characters you are sending, receiving, or both. Translation tables are stored in files with the extension .TRN. You can have several .TRN files, and you can assign the same .TRN file to more than one session configuration. See Appendix B, “Terminal Emulation,” for more information on the use of translation tables.

CAUTION: This is an advanced feature intended for users who are experienced with communication programs. You probably do not need to edit translation tables. This feature is used only when the keyboard does not behave as expected because of an incompatibility between an online service and a Norton pcANYWHERE terminal emulator, or to filter certain codes sent by the host.

To set up a translation table:

- 1 Choose TERMINAL EMULATIONS... from the Configure menu.
The Configure Terminal Emulations dialog box appears (see Figure 7-1).
- 2 Click Translation Tables... to display the Select Translation File dialog box (Figure 7-5).

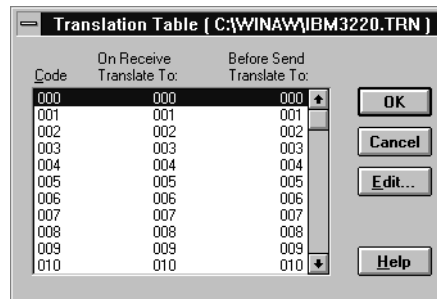
Figure 7-5 Set up a Translation Table only if your keyboard does not work properly with terminal emulation.



- 3 Enter a name for the translation file or select the name of an existing file.
- 4 Click OK.

The Translation Table dialog box appears (Figure 7-6).

Figure 7-6 The Translation Table dialog box displays the translation table for the file you selected.



If you enter a new filename for the translation table, Norton pcANYWHERE loads a default translation table. Until you edit it, this table does not specify any translations.

- 5 Select the code you want to change and click the Edit... button.

The pcANYWHERE Translation Tables dialog box appears (Figure 7-7).

Figure 7-7 You can edit both incoming and outgoing character translations.



- 6 Enter hexadecimal translation values and click OK. For more information on hex translations, see Appendix B, "Terminal Emulation."
- 7 Repeat steps 5 and 6 until you are finished.
- 8 Click OK to return to the Translation Table dialog box.

TIP: To filter out an incoming or outgoing character, clear the appropriate field. This eliminates unwanted characters from being sent or received.

Customizing Font and Colors

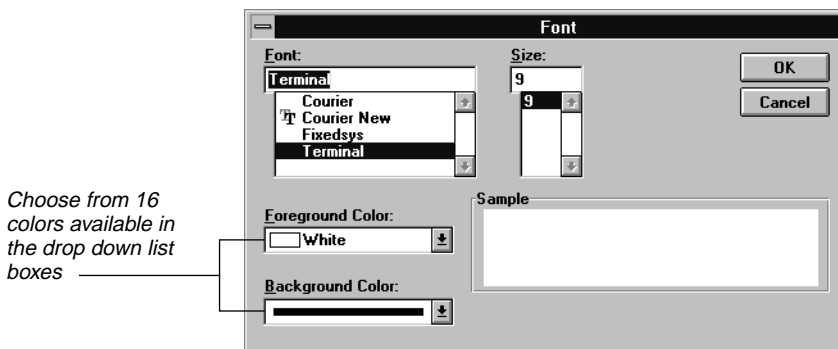
You can select your preference of background and foreground colors your monitor uses during a connection with an online service, as well as choose a font and size to improve the readability of the text on your screen.

To customize your display's color and font:

- 1 Choose TERMINAL EMULATIONS... from the Configure menu.
- 2 Click the Font/Colors... button in the Configure Terminal Emulations dialog box.

The Font dialog box appears (Figure 7-8).

Figure 7-8 The Font dialog box allows you to customize font style and colors for your session.



- 3 Select a font style and size to use from the Font and Size drop-down list boxes.
- 4 Select the colors to use from the Foreground Color and Background Color list boxes.
- 5 Click OK to save the settings and return to the Configure Terminal Emulations dialog box.
- 6 Click Close to save all settings and return to the Norton pcANYWHERE main window.

Calling an Online Service

This section explains how to use Norton pcANYWHERE to call an information service or connect to a mainframe or minicomputer. Both of these connections involve terminal emulation. Whether you are connecting directly to a mainframe or connecting with a BBS over telephone lines, the connect procedures are virtually identical. Norton pcANYWHERE handles the routing of the connection automatically according to the selected hardware configuration. For information on how to transfer files to and from the online service, see Chapter 8, “Managing Remote Control and Online Sessions.”

Creating a List of Online Services

Norton pcANYWHERE uses terminal emulation to connect to online services. The first time you use pcANYWHERE terminal emulation, you need to create one or more entries in the Online Service Directory. Each entry in this list contains dialing instructions and other parameters that are used to connect to the specified service. You can modify or add to this list at any time.

NETWORK USERS: If your network administrator specified a *shared* Online Service Directory file during network installation, you may not be able to modify or add to the Online Service Directory. In this case you can access only the online services specified by your network administrator. For more information on shared data files, see “Specifying Shared Data Files” in Chapter 2, “Installation and General Setup.”

Online service directory information includes:

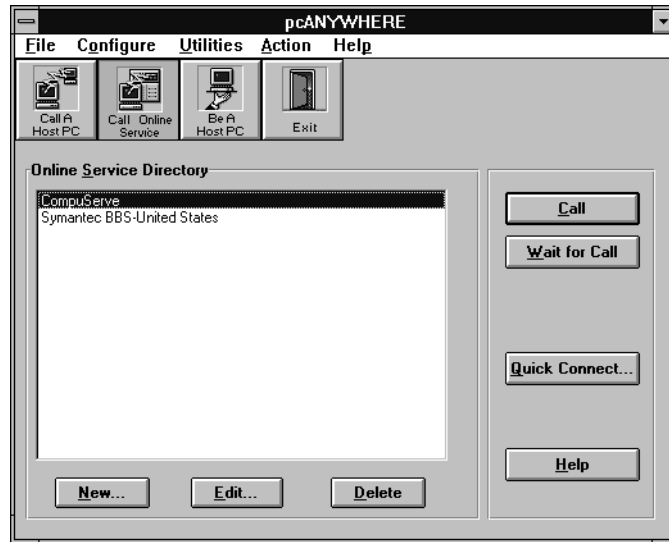
- Description—Specifies the name of the online service
- Hardware configuration—Specifies what hardware is used to connect to the online service
- Terminal Emulation—Specifies the type of terminal emulation used
- File Transfer Protocol—Specifies the protocol used for uploading (sending) and downloading (receiving) files

To create a list of online services to call:

- 1 Click the Call Online Service load button.

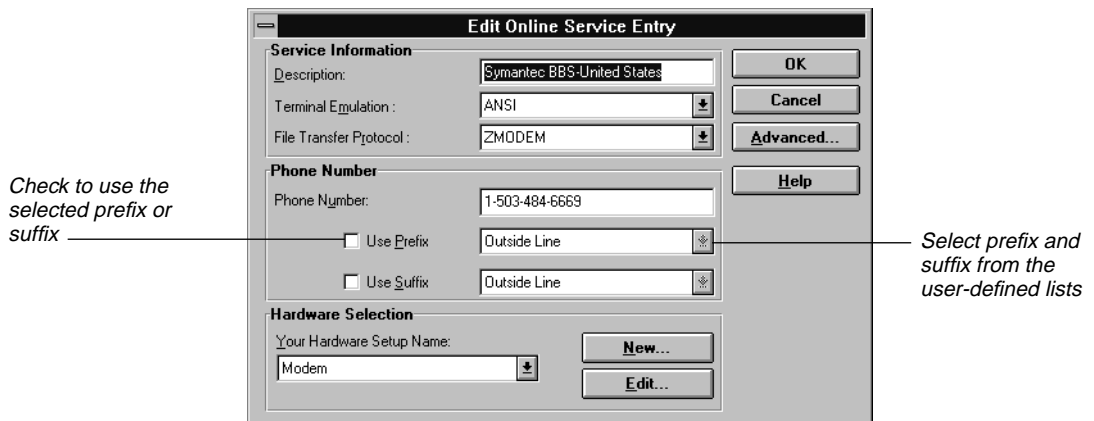
The online service main window appears (Figure 7-9).

Figure 7-9 Enter Online Service Directory information before clicking the Call button.



- 2 Click New... to add an online service entry to the directory. The Edit Online Service Entry dialog box appears (Figure 7-10).

Figure 7-10 Norton pcANYWHERE supports most popular terminal emulations and file transfer protocols.



- 3 Enter a descriptive name for this online service entry in the Description text box.

- 4 Click the Terminal Emulation prompt button to display a drop-down list of terminal emulations.
- 5 Select the name of a terminal emulation type.
ANSI and VT100 are the most commonly used emulation types. You may want to check with your system administrator to determine which type to use.
- 6 Click the File Transfer Protocol prompt button to display a drop-down list of protocols.
- 7 Select the name of a file transfer protocol to establish it as the default for transferring files to and from this online service. XMODEM is a very commonly used protocol, but many systems also support such protocols as ZMODEM and Kermit. You may want to check with your system administrator to determine which type to use.
- 8 Enter the online service telephone number in the Phone Number text box.
- 9 Click the Your Hardware Setup Name prompt button to display a drop-down list of available hardware configurations.
- 10 Select a hardware configuration for use in calling this online service. For more information on hardware configurations, see Chapter 3, "Hardware Configurations."
- 11 Click OK.
Repeat this procedure for each online service you want to add to the list.

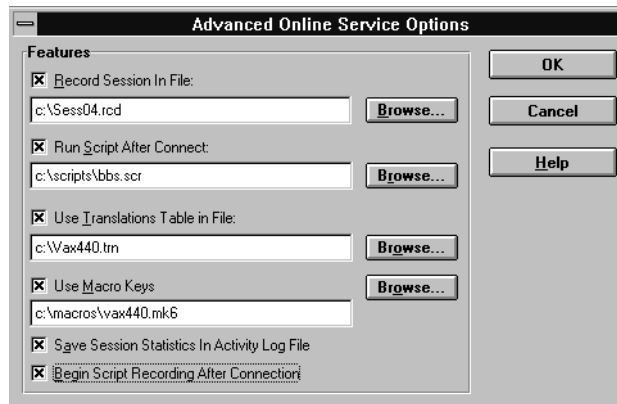
Advanced Online Session Options

The advanced settings allow you to automate certain functions you may use during your session, such as recording the session to a file, running a script after a connection is established, and enabling translation tables, or running macros.

To set advanced features:

- 1 Click the Advanced... button in the Edit Online Service Entry dialog box.
The Advanced Online Service Options dialog box appears (Figure 7-11).

Figure 7-11 The Advanced Online Service Options dialog box allows automatic enabling or execution of features.



- 2 Check or uncheck the following advanced options as desired:
 - Record Session in File—Causes recording of the activities of the session to a file for playback later. You can type in a new filename in the text box or you can use the Browse... button to locate and use an existing record file. The new session is appended to the end of this file. See Chapter 10, “Utilities,” for more information on session recording and playback.
 - Run Script after Connect—Causes execution of a script file when the session starts. Use the Browse... button to display the Scripts dialog box from which you can select a script to run. See Chapter 8, “Managing Remote Control and Online Sessions,” for more information on running scripts.
 - Use Translation Table in File—Enables a translation table to use for this session. Use the Browse... button to view and select from available translation (.TRN) files. See “Setting Up Translation Tables” in this chapter and Appendix B, “Technical Information,” for more information on translation tables.
 - Use Macro Keys—Enables special macro keys to be used during the session. Use the Browse... button to view and select from available macro (.MK6) files. See “Setting up Macro Keys” earlier in this chapter.
 - Save Session Statistics in Activity Log File—Causes session statistics to be saved in a log file. See Chapter 10, “Utilities,” for more information on log files and reports.
 - Begin Script Recording after Connection—Creates a script file automatically from the activities occurring during this session.

Refer to the *Creating Norton pcANYWHERE Scripts* manual for information on creating scripts.

- 3 Click OK to save the settings and return to the Edit Online Service Entry dialog box.

Starting an Online Session

Once you have established one or more entries in the Online Service Directory, starting a session with an online service is easy. There are two options for connecting.

Connection methods include:

- Call—Norton pcANYWHERE dials an information service, mainframe, or minicomputer.
- Wait for Call—Norton pcANYWHERE waits for an online service to call back.

To call an online service:

- 1 Click the Call Online Service load button.
The online service main window appears (see Figure 7-9).
- 2 Select the name of an online service from the Online Service Directory list.
- 3 Click the Call button to initiate the call.

Norton pcANYWHERE connects to the online service (Figure 7-12).

Figure 7-12 The online service screen appears in the Terminal window after a connection is made.

```

pcANYWHERE Terminal
File Edit Session Transfers Help
All Rights Reserved

800 Direct Dial Access
rates now in effect.
GO RATES for current information

What's New This Week(FREE)  NEW-1

1 Enter Military Forum D-Day Contest
2 Der Spiegel Magazin Online
3 Attend Conference with New Order
4 Discuss D-Day in Gaming World
5 Win Tickets, Trip to "The Shadow"
6 Get CompuServe Mail(sm) for Powertalk(tm)
7 More Symantec Support in Network Forum
8 Timeslips Corporation Forum Opens
9 Florida Governor's Race News Online
10 Visit Benchmark & STDS Forum
11 Neuer CompuServe-Knoten in Hannover

Enter choice or <CR> for more ?_
ANSI  COM1  38,400  Even  RTS/CTS  XMODEM

```

- 4 Log on to the online service and enter any required password.
The online service session begins.

NOTE: Log-on procedures vary from system to system. You can automate the log-on procedure by creating a custom script file that logs you onto the specified online service. Refer to the *Creating Norton pcANYWHERE Scripts* manual supplied with your software for information on creating scripts.

To wait for a call:

- 1 Select the name of an online service from the Online Services Directory list box (see Figure 7-9).
- 2 Click Wait for Call.
Norton pcANYWHERE initializes your modem and waits for a call.

Connecting Through a pcANYWHERE Gateway

A Norton pcANYWHERE Gateway provides shared access to a local network station modem. One or more gateways can be established on a local area network to connect network users to online services. Inbound and outbound gateways allow network users to dial in and out of the local area network without the need for modem hardware at each network station. For information on setting up and using a Norton pcANYWHERE network gateway, see Chapter 4, “Gateways.” For more information on connecting through a gateway, see “Connecting Through a Gateway” in Chapter 5, “Configuring Norton pcANYWHERE.”

Specifying a Gateway Connection

To use a Norton pcANYWHERE Gateway to connect to an online service, the Online Service Directory entry for that service must reference a special type of hardware configuration. The node hardware configuration specifies connection through a gateway. For more information on hardware configurations see “Creating a Node Hardware Configuration” in Chapter 3, “Hardware Configurations.”

NETWORK USERS: If your network administrator specified a *shared* Online Service Directory file during network installation, you may not be able to modify or add to the Online Service Directory. In this case you may access only the online services previously set up by your network administrator. For more information see “Specifying Data File Sharing” in Chapter 2, “Installation and General Setup.”

To specify a remote-to-gateway hardware configuration:

- 1 Click the Call Online Service load button.
The online service main window appears (see Figure 7-9).
- 2 Select from the Online Service Directory the name of an online service you want to access through a gateway.
- 3 Click Edit...
The Edit Online Service Entry dialog box appears (see Figure 7-10).
- 4 Click the Your Hardware Setup Name prompt button to display a drop-down list of available hardware configurations.
- 5 Select the name of a node hardware configuration. For more information on node hardware configurations, see “Creating a Node Hardware Configuration” in Chapter 3, “Hardware Configurations.”
- 6 Click OK to save the specified online service settings.

For information on other online service settings, see “Creating a List of Online Services” earlier in this chapter.

Calling an Online Service Using a Gateway

Once you have specified a node hardware configuration, connecting through a gateway is easy. If your hardware configuration specifies a particular gateway, Norton pcANYWHERE handles the process of connecting through the gateway automatically. Otherwise, a list of available gateways appears when you click Call or Wait For Call.

To call an online service through an outbound gateway:

- 1 Click the Call Online Service load button.
- 2 Select an online service to call from the Online Service Directory list box.
- 3 Click Call.

- 4 If the correct gateway name is specified in the hardware configuration, pcANYWHERE dials out of the gateway modem automatically.
Or,
If the name is not specified, a list of gateways appears. Select a gateway and click OK. The gateway modem dials the selected online service.
- 5 Log on to the online service and enter any required password.
The online service session begins.

NOTE: You can create a script file to log you onto a specific online service automatically. For information on creating script files, consult the *Creating Norton pcANYWHERE Scripts* manual included with your software.

Using Quick Connect for Online Sessions

The Norton pcANYWHERE Quick Connect feature allows you to quickly configure and start up a session using the minimum required parameters. This is not a replacement for full configuration, but is a handy tool to help both experienced and novice users connect to an online service quickly.

Starting a Quick Connect Online Session

Unlike other Norton pcANYWHERE components, Quick Connect does not use hardware configurations. Instead, the minimum required communications options are configured in a single dialog box. While this limits your choices, the Quick Connect feature provides adequate control for most sessions without overwhelming you with a large number of selections.

Connection methods include:

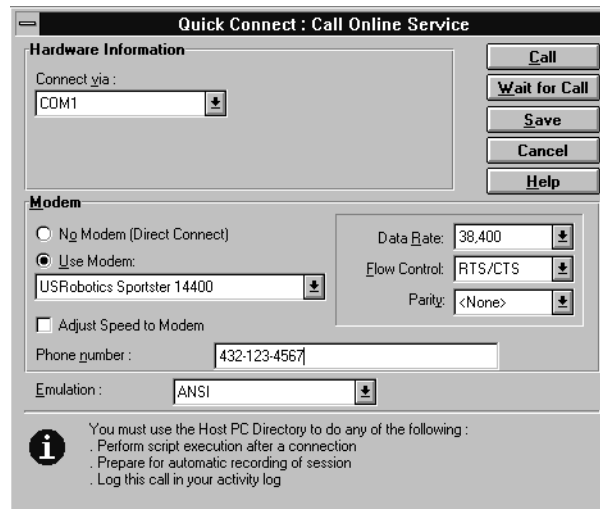
- Call Online Service—Norton pcANYWHERE dials an information service, mainframe, or minicomputer.
- Wait for Call—Norton pcANYWHERE waits for an information service, mainframe, or minicomputer to initiate a connection.

To use Quick Connect to call an online service:

- 1 Click Quick Connect... in the online service main window (see Figure 7-9).

The Quick Connect: Call Online Service dialog box appears (Figure 7-13).

Figure 7-13 The Quick Connect dialog box includes the minimum parameters needed to make a connection.



- 2 Select communications options in the Quick Connect dialog box.

The communications port and modem settings are filled in automatically based upon the information you provided the first time you used pcANYWHERE after installing. The Data Rate is set automatically based upon the recommended speed for the modem selected. Flow Control, Parity, and Emulation depend upon the online service to which you are connecting. Most online services provide you with this information. For more information on communications options, see Chapter 3, “Hardware Configurations.”

- 3 Click Save if you want to save the dialog box settings. The saved settings will appear the next time you use Quick Connect.

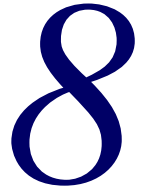
NOTE: If you are going to call this online service regularly, you should add it to your Online Service Directory. (See “Creating a List of Online Services” earlier in this chapter.) Quick Connect is generally used for infrequently called online services.

- 4 Click Call to call an online service.

Or,

Click Wait for Call to wait for a call from an online service.

Managing Remote Control and Online Sessions



This chapter explains how to change session options and access pcANYWHERE program functions during remote computing and online sessions. It also explains how pcANYWHERE remotely handles Windows system keys during sessions with a host. This chapter is for all users who need to access program features or change session options during a session, or to end a session.

This chapter covers:

- Accessing online session options
- Accessing terminal session options
- Using the chat window to type a conversation with the host user
- Changing session options during a session
- Controlling Windows system keys during a remote computing session
- Switching to voice/data connection during a session
- Starting a script during a session
- Enabling special keyboard handling
- Printing remotely
- Setting DOS session options

Managing the Remote Control Session

Using Online Menu Options Available to Host and Remote

Once the connection to the host PC is made, both the host and remote user can execute commands and run applications on the host PC. Both users have access to an *online menu*. An online menu is accessible only after a connection is made. The remote PC has a different online menu from the one on the host PC.

Both host and remote users are able to initiate a typed conversation and end the session. These shared options are explained first.

To access the Online Menu:

- 1 Begin a remote computing session. For more information on starting a session, see Chapter 6, “Starting a Remote Computing Session.”
- 2 Open the session window’s Control-menu box and choose ONLINE MENU.

Or,

Double-click the Norton pcANYWHERE session icon.

Depending on whether you are the remote or host user, either the Remote Online Menu or the Host Online Menu appears (Figures 8-1 and 8-2).

Figure 8-1 You can access the Remote Online Menu by double-clicking the session icon.



Figure 8-2 The Host Online Menu allows the host to initiate some control over the session.



Any changes you make from the Online Menu affect the *current session only*. The default settings you see in the Online Settings dialog box are the settings that have been configured for the host and remote. The default settings return for your next session.

Chatting with the Other User

During a *chat*, a typed conversation initiated by either the host or remote user, the same dialog box appears on both the host and remote screens. This feature is particularly helpful for sending or receiving brief messages or instructions.

The host user's keystrokes automatically appear in the upper chat window while the remote user's keystrokes appear in the lower chat window. Either user can use the scroll bars to move to the bottom or top of either window.

To use the chat window:

- 1 Open the session window's Control-menu box and choose ONLINE MENU.

Or,

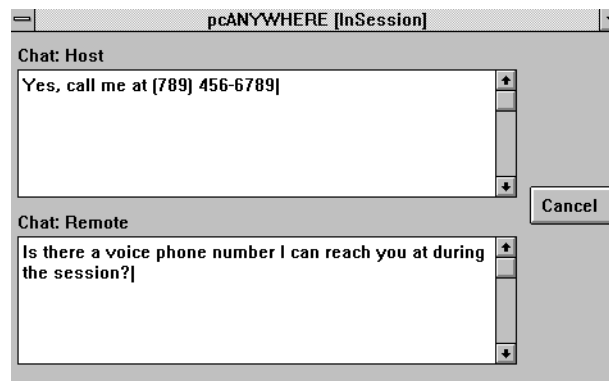
Double-click the Norton pcANYWHERE session icon.

The Online Menu appears (see Figures 8-1 and 8-2).

- 2 Choose CHAT from the Online Menu.

The Norton pcANYWHERE chat windows appear on both the host and remote screen (Figure 8-3).

Figure 8-3 Identical chat windows appear on the host and remote PCs.



- 3 Type your conversation.
- 4 Click Cancel when the conversation is done.

Ending the Remote Control Session

Either the host or remote user can end the session. The remote caller can change the mode to which the host returns, providing the caller was granted this privilege. See “Creating a Caller List” in Chapter 5, “Configuring Norton pcANYWHERE.”

To end the session from the remote:

- 1 Open the Session window’s Control-menu box and choose ONLINE MENU.

Or,

Double-click the Norton pcANYWHERE session icon.

The Remote Online Menu appears (see Figure 8-1).

- 2 Choose END SESSION.

The remote’s End Session dialog box appears (Figure 8-4).

The Host Accepts Another Call check box appears only if the caller has been granted the right to change the host’s mode. See “Creating a Caller List,” in Chapter 5, “Configuring Norton pcANYWHERE.”

Figure 8-4 The remote user can instruct the host to wait for another call.

This check box appears only if the remote caller was granted the right to change the host mode



NOTE: If the remote does not choose to have the host accept another call, the host operation on the host PC is canceled. The host user must load pcANYWHERE and wait for another call.

To end the session from the host:

- 1 Double-click the Norton pcANYWHERE session icon.

The Host Online Menu appears (see Figure 8-2).

- 2 Choose END SESSION.

The host's End Session dialog box appears (Figure 8-5).

Figure 8-5 When ending a session from the host, the host user can disable or cancel the host.



- 3 Select a disconnect option.
 - Host Accepts Another Call—Instructs the host to wait for another call.
 - Disable Host Operation—Instructs the host to disable itself. The session ends and the host minimizes. Double-click the pcANYWHERE host (disabled) icon to display the Offline Menu and click the Wait for a Call button to have a disabled host wait for another call.
 - Cancel pcANYWHERE—Removes the host from memory.
- 4 Click Yes to end the session.

NOTE: If the host is running the host DOS TSR, the host user accesses the Online Menu by pressing the hotkey specified in the host configuration. The default hotkey for the host is Alt+Right Shift. (See Chapter 5, “Configuring Norton pcANYWHERE.”)

Using Remote Online Menu Options

The next few sections describe options on the remote user's Online Menu. These are not privileges shared with the host user, although some of them are not available to the remote user without the host user's prior authorization. (See Chapter 5, “Configuring Norton pcANYWHERE.”)

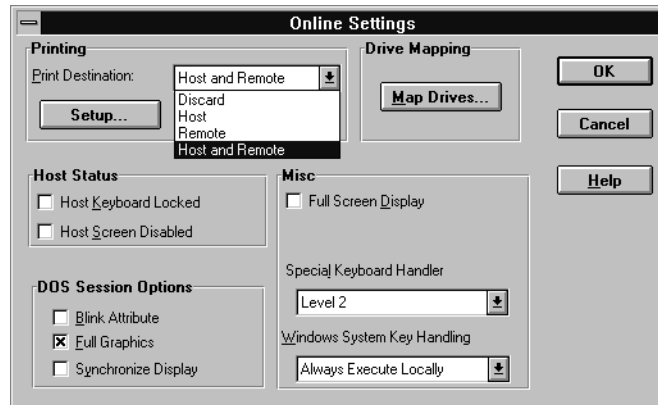
Remote online settings include options for printing, remote drive mapping, host screen and keyboard states, DOS session options, remote screen display, special keyboard handling, and Windows system key handling.

To access online settings:

- Choose ONLINE SETTINGS... from the Remote Online Menu (see Figure 8-1).

The Online Settings dialog box appears (Figure 8-6).

Figure 8-6 Use the Online Settings dialog box to change session options while you are connected.



Changing the Destination for Printed Output

The remote user can change the destination of any printed output during a session. The output can be printed on the active printer at the host, remote, or both host and remote PCs, or be discarded.

The Setup... button displays the Windows Print Setup dialog box for the local printer.

The destination of printed output also can be set as a remote option. See “Remote Operations” in Chapter 5, “Configuring Norton pcANYWHERE.”

To change the destination for printed output:

- 1 Choose ONLINE SETTINGS... from the Remote Online Menu (see Figure 8-1).
The Online Settings dialog box appears (see Figure 8-6).
- 2 Click the Print Destination prompt button.
- 3 Select the print destination of your choice from the drop-down list box.

Print Destinations include:

- Discard—Instructs pcANYWHERE to ignore all printed output from the host.
 - Host—Send host's printed output to the host printer only.
 - Remote—Send host's printed output to the remote printer only.
 - Host and Remote—Send host's printed output to both host and remote printers.
- 4 Click OK to save settings and return to the Remote Online Menu.

CAUTION: When selecting Remote as a print destination, the host must have a printer setup to match the remote's printer setup. If you want to print to both the host and remote, the host and remote PCs must have the same printer configuration.

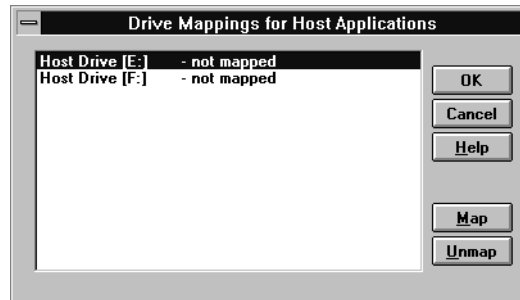
Accessing the Remote PC's Drives During a Session

As the remote user in a remote control session, you control the host PC. The remote's keystrokes and mouse movements take effect on the host PC—not the remote PC. At some point during a session, you may want to access files or applications on the remote PC. For example, you can attach a file from the remote PC to an electronic mail message on the host PC without transferring the file to the host first. You can map the remote PC's drives to available drives on the host PC, making your PC's drives available during the session.

To map remote drives to the host PC:

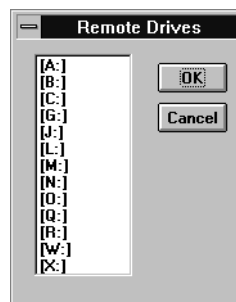
- 1 Choose ONLINE SETTINGS... from the Remote Online Menu.
The Online Settings dialog box appears (see Figure 8-6).
- 2 Click Map Drives....
The Drive Mappings for Host Applications dialog box appears.
(Figure 8-7).

Figure 8-7 Select a drive that the host will not be using during the session.



- 3 Select a host drive letter from the Drive Mappings window. This is the host drive that the remote will use to access files residing on the remote PC. Usually, you select a letter currently unused by the host PC.
- 4 Click the Map button.
The Remote Drives dialog box appears (Figure 8-8).

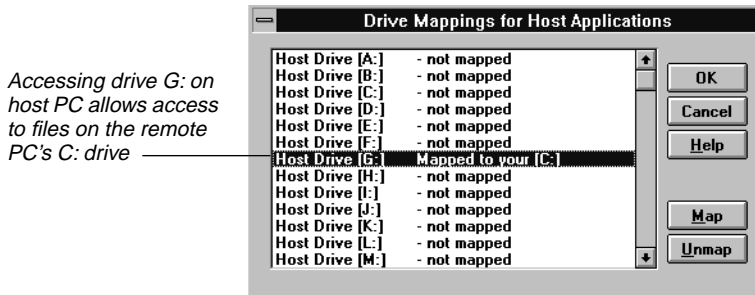
Figure 8-8 Select the remote drive to map to the host.



- 5 Select the drive letter representing the drive on the remote that you want to access from the host.

NOTE: If you want your local C: drive to be the host's T: drive, for example, in step 3 select T:, and in step 5 select C:.

- 6 Click OK.
The Drive Mappings for Host Applications dialog box reappears, indicating the current drive mapping status (Figure 8-9).

Figure 8-9 Select mapped host drive to access remote drive.

- 7 Click OK to save the drive mapping settings and return to the Online Settings dialog box.
- 8 Repeat steps 3 through 5 for each remote drive you want to map.

To unmap drives:

- 1 Click the Map Drives... button in the Online Settings dialog box (see Figure 8-6).
The Drive Mappings for Host Applications dialog box appears (see Figure 8-7).
- 2 Select the drive you want to unmap from the Drive Mappings window.
- 3 Click Unmap.
The Drive Mappings window indicates the unmapped status of the drives.
- 4 Click OK to return to the Online Settings dialog box.

Changing Host Status Options

When permitted by the host, the remote user can change the status of the host's screen, keyboard, and mouse by checking options within the Host Status group box in the Online Settings dialog box. These settings are in effect during the current session only and they return to the default settings after the connection ends. See Chapter 5, "Configuring Norton pcANYWHERE," for information on setting default values.

To change the host's status options:

- 1 Choose ONLINE SETTINGS... from the Remote Online Menu.
The Online Settings dialog box appears (see Figure 8-6).

- 2 Check the desired check boxes in the Host Status group box.

The available options are:

- Host Keyboard Locked—Allows you to disable the host's keyboard and mouse to prevent interruptions. The host user can only observe the remote control session.
- Host Screen Disabled—Disables (blanks) the host screen during the session to ensure your privacy. You use this option when the host PC is unattended and the remote is running confidential applications on it. As a host security option, the host user may configure the host screen to automatically blank upon connection. (See Chapter 5, "Configuring Norton pcANYWHERE.") If the host has not granted the remote user the privilege of blanking the host screen, this option is dimmed and cannot be checked.

- 3 Click OK to save the settings and return to the Online Menu.

Changing DOS Session Options

When the host is running DOS in a full-screen window, or when the host user has exited to DOS, the host screen may contain characters or graphics that differ from the screen display when the host PC is running Windows. The options available in the DOS Session Options group box allow the remote user to make adjustments to several DOS display characteristics if the remote PC experiences problems reading and displaying the host screen.

NOTE: These options also apply when the remote connects with a Norton pcANYWHERE 4.5 or 5.0 host.

To set DOS session options:

- 1 Choose ONLINE SETTINGS... from the Remote Online Menu.

The Online Settings dialog box appears (see Figure 8-6).

- 2 Check the desired check boxes in the DOS Session Options group box.

The available options are:

- Blink Attribute—Check this check box to allow the display of blinking characters.
- Full Graphics—Check this check box when you want the most accurate representation of DOS graphics possible. Uncheck to improve screen display speed if an approximation of graphics is acceptable.

- Synchronize Display—Check this check box to slow the host application to the rate at which the remote can display screen activity. If unchecked, some lines of text may scroll off the screen before the remote is able to display them. Uncheck if the speed of the application is more important than a complete display of all characters, such as with a lengthy database indexing procedure.
- 3 Click OK to save settings and return to the Online Menu.

Changing Miscellaneous Options

Options for displaying the host's screen full-screen on the remote, setting special keyboard handling levels, and selecting Windows system key handling are found in the Misc group box.

Full Screen Display

Full-screen display causes Norton pcANYWHERE to display the host's screen full-screen on your remote computer. When the host's screen is displayed full-screen at the remote, the Control-menu box is not available. To access the Online Menu, double-click the pcANYWHERE session icon or press Alt+Enter to change to window mode.

To change the remote display option:

- 1 Choose ONLINE SETTINGS... from the Remote Online Menu.
- 2 Check the Full Screen Display check box in the Online Settings dialog box to view the host full-screen on your remote computer.
- 3 Click OK to save the settings and return to the Remote Online Menu.

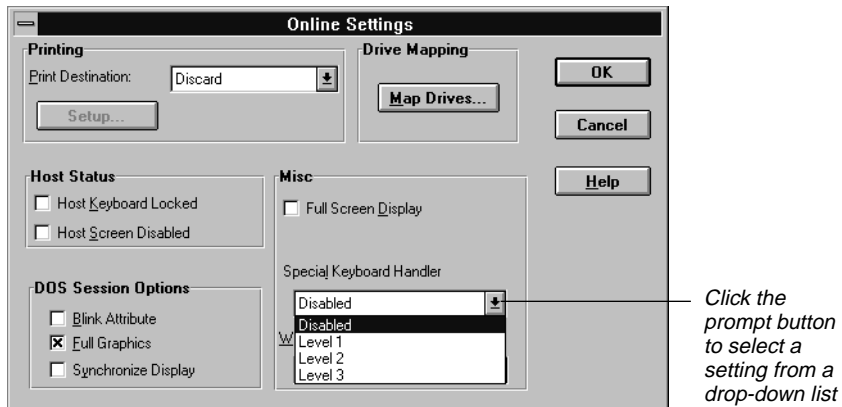
Special Keyboard Handling

Keyboard handlers allow the remote user to operate the host PC effectively while executing host applications that handle keyboard input in a non-standard fashion. Keyboard handlers are divided into two types, Type 1 and Type 2, and they are used only with the DOS TSR. Most applications use Type 1, the default setting. The host determines and sets the type of keyboard handler used. See Chapter 5, "Configuring Norton pcANYWHERE," for additional information.

Type 1 keyboard handler has three variations known as Level 1, Level 2, and Level 3. The remote user can select from the three levels during a session. Start with Level 1, and if you still experience keystroke difficulties, try Level 2 or Level 3.

To select the level of keyboard handling:

- 1 Choose ONLINE SETTINGS... from the Remote Online Menu.
- 2 Click the Special Keyboard Handler prompt button and select a keyboard handler level from the drop-down list box (Figure 8-10).

Figure 8-10 Select a level of keyboard handler from the list box.

- 3 Click OK to save the settings and return to the Remote Online Menu.

Windows System Key Handling

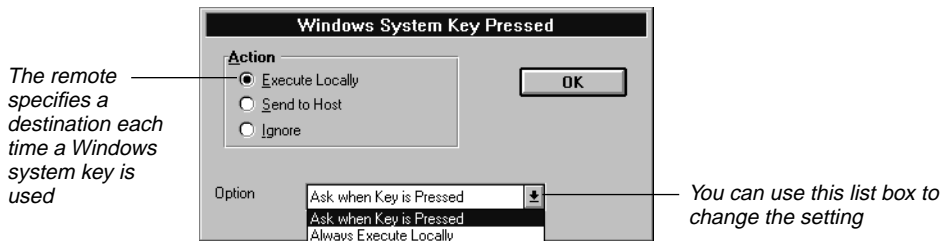
Windows system keys are special key combinations that control certain Windows functions. For example, Alt+Tab toggles between currently running applications. When you control a host computer that is running a Windows session, Norton pcANYWHERE needs to know whether to execute the Windows system key command locally or at the host. When set to the default, pcANYWHERE asks where to execute the keystroke. You also can configure these commands to execute automatically on one computer or the other.

To select a key handler:

- 1 Click ONLINE SETTINGS... in the Remote Online Menu.
- 2 Click the Windows System Key Handler prompt button (See Figure 8-10).
- 3 Select the key handler desired from the drop-down list box.
 - Ask When Key is Pressed—Instructs Norton pcANYWHERE to ask the user where to execute the system key each time a Windows system key is used (Figure 8-11).

- Always Execute Locally—Instructs Norton pcANYWHERE to execute the system key on the remote computer.
 - Always Send to Host—Instructs Norton pcANYWHERE to execute the system key on the host computer.
- 4 Click OK to save the settings and return to the Online Menu.

Figure 8-11 If Ask When Key is Pressed is selected, this dialog box will appear each time a Windows system key is used.



Switching from Data Communication to Voice

When both users are using a modem hardware configuration, the remote user can switch from a remote control session to a voice conversation over the telephone line. Norton pcANYWHERE prompts you through this activity. However, both users must have telephones that share the telephone lines with their modems.

To switch a session to voice:

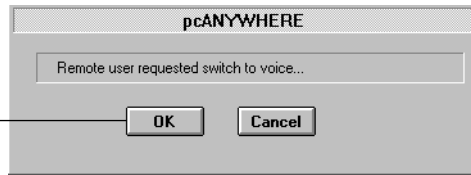
- 1 Choose VOICE from the Remote Online Menu (see Figure 8-1).
pcANYWHERE pauses the remote session and informs the host user. (Figures 8-12 and 8-13).

Figure 8-12 The remote's screen informs the remote user that it is waiting for acknowledgment from the host.



Figure 8-13 The host's screen informs the host user that the remote is requesting to use voice.

After host user clicks OK, both host and remote users receive instructions to pick up the phone



- 2 Pick up the telephone receiver when prompted and wait for host user to do the same.

To resume a suspended session:

- 1 Choose RESUME SESSION from the Remote Online Menu.
- 2 Hang up the telephone receiver and wait for host user to do the same.

The remote computing session continues.

Rebooting the Host PC

If the host PC crashes while performing some activity, the host or remote user may need to reboot it. The remote user can reboot the host PC providing the host has granted the caller the privilege to do so in the Advanced Caller Options dialog box. (See Chapter 5, “Configuring Norton pcANYWHERE.”)

To reboot the host from the remote PC:

- 1 Choose REBOOT HOST from the Remote Online Menu.

The Reboot Host? dialog box appears (Figure 8-14).

Figure 8-14 Click Yes if you want to reboot the host.

Cold Boot is equivalent to turning your computer off and on

Warm Boot is equivalent to pressing Ctrl+Alt+Del



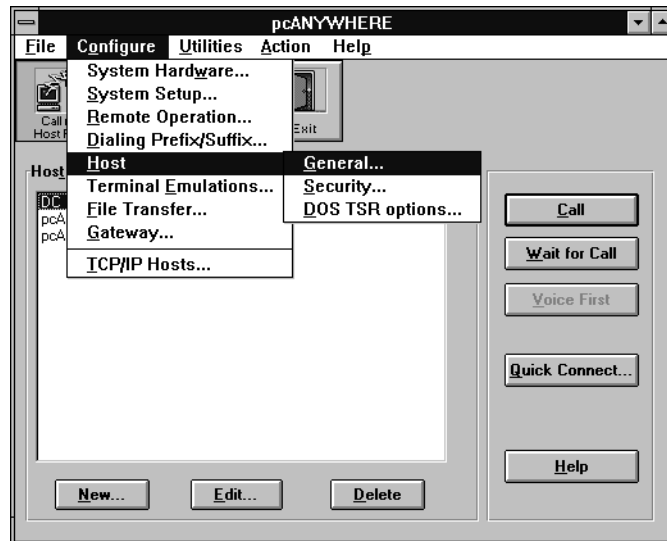
- 2 Click Yes to end the session and reboot the host PC.

NOTE: If you want to have the host wait for a call automatically after rebooting, you need to start Windows automatically by entering the windows load command (WIN) in your AUTOEXEC.BAT file and configuring the Norton pcANYWHERE Host to start automatically when Windows is loaded.

To run Norton pcANYWHERE Host automatically after reboot:

- 1 Choose HOST from the Configure menu in the pcANYWHERE main window (Figure 8-15).

Figure 8-15 Choose General from the submenu to open the Host General Options dialog box and configure the host to automatically start when Windows is run.



- 2 Choose GENERAL... from the submenu.
The Host General Options dialog box appears.
- 3 Check the Start Host with Windows check box.
- 4 Click OK to save the settings and return to the main window.
- 5 Enter the Windows load command (WIN) in the last line of your PC's AUTOEXEC.BAT file. See your DOS manual for information on how to edit the AUTOEXEC.BAT file.

Using Host Online Menu Options

Because hosts do not *control* remote control sessions, the Online Settings option in the Host Online Menu is significantly shorter than that of the remote, containing only two options—one to control the remote’s mouse and keyboard state and the other to blank the remote’s screen.

To access the Host Online Menu:

- 1 Double-click the pcANYWHERE session icon.

Or,

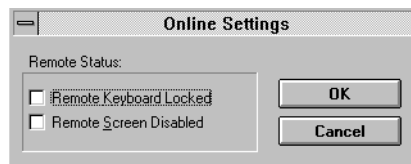
If using the Host DOS TSR, press the hotkey specified in the host configuration (the default is Alt+Right-Shift). For additional information on the host DOS TSR, see Chapter 5, “Configuring Norton pcANYWHERE” and Chapter 6, “Starting a Remote Computing Session.”

The Host Online Menu appears (see Figure 8-2).

- 2 Choose the ONLINE SETTINGS button from the Host Online Menu.

The Online Settings dialog box appears (Figure 8-16).

Figure 8-16 The host’s Online Settings dialog box allows the host to control the host’s screen, mouse, and keyboard.



- 3 Check one or both of the boxes to enable the functions.
 - Remote Keyboard Locked—Check this check box to lock the remote’s mouse and keyboard during the session.
 - Remote Screen Disabled—Check this check box to blank the remote’s screen during the session.
- 4 Click OK to save the settings and return to the Host Online Menu.

Transferring Files During a Remote Control Session

Both host and remote computers have the option of starting the Norton pcANYWHERE File Manager. The Norton pcANYWHERE File Manager can be used to transfer files from one computer to another using drag-and-drop. See Chapter 9, “File Transfer,” for information on file transfers during a remote

control session. See the following section, “Controlling Online Service Sessions,” for information on uploading and downloading files during a session with an online service.

Controlling Online Service Sessions

While you are connected to an online service, all session activities take place within the Terminal window. You can access the Online Terminal menu bar, which is located near the top of the window, anytime during and after completion of an online service session. These menus contain groups of related commands used to access program features and options during a session.

Running Scripts

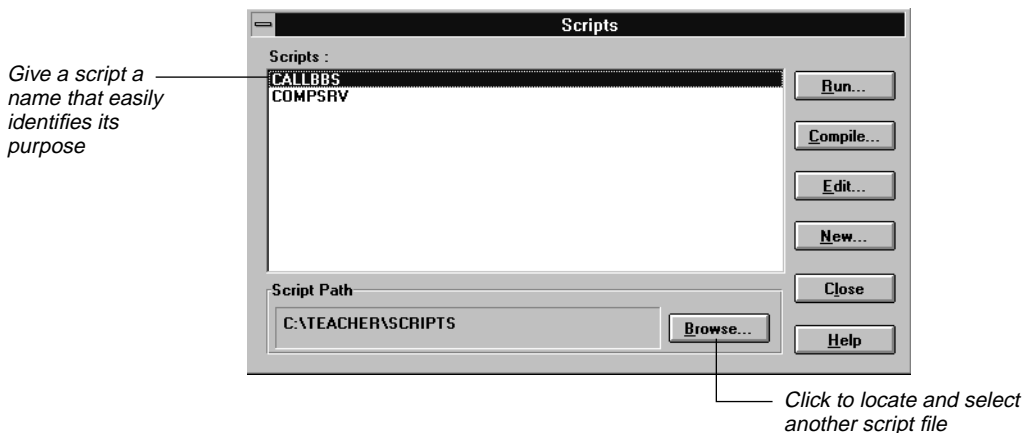
Norton pcANYWHERE scripts automate a variety of online service session activities. Scripts can be executed when a session starts or at anytime during a session. For more information, refer to the manual *Creating Norton pcANYWHERE Scripts*, included with your Norton pcANYWHERE software.

To start a script file during an online service session:

- 1 Begin an online service session. For details on starting a communications session with an online service, see Chapter 7, “Online Services.”
- 2 Choose SCRIPTS... from the File menu.

The Scripts dialog box appears (Figure 8-17).

Figure 8-17 Select a script file to run from the list box.



- 3 Select a script file to execute from the Scripts list box.
- 4 Click Run...
The selected script file executes.

Printing from the Terminal Window

Sometimes you need a printed copy of an online session or screen. Instead of using session recording to save the screen or session to a file, you can print directly from the Terminal window. (Recording sessions and screens is explained in Chapter 10, “Utilities.”)

To print from the terminal window:

- 1 Begin an online service session. For more information see Chapter 7, “Online Services.”
- 2 Choose PRINT ONLINE from the Sessions menu to enable session printing. Terminal window output is sent to your printer continuously during the session.

Or,

Choose PRINT SCREEN from the File menu to print only the current terminal display.

To end terminal window printing:

- Choose PRINT ONLINE from the Sessions menu to disable session printing.

NOTE: A checkmark appears next to the PRINT ONLINE menu choice when session printing is enabled. Printing a session is like using a camcorder or VCR in that you need to start and stop the recording. Alternatively, when you choose PRINT SCREEN from the File menu, the action is more like taking a snapshot.

Editing Terminal Window Text

The Terminal window supports the use of the Windows Clipboard. You can cut, copy, and paste text from the clipboard to the Norton pcANYWHERE Terminal window or you can upload it directly to the online service, providing the Windows application from which you are copying the text supports the Windows Clipboard.

You can copy clipboard text to the local Terminal window or you can upload it to the online service. You use standard Windows editing keys to edit text in the clipboard.

To copy and paste Clipboard text:

- 1 Switch to another Windows application (Alt+Tab).
- 2 Mark the text you want to copy or move by dragging the mouse cursor over it.
- 3 Choose COPY from the Edit menu of the other Windows application to copy the selected text to the Clipboard.

Or,

Choose CUT from the Edit menu of the other Windows application to move the selected text to the Clipboard.

- 4 Switch to the Norton pcANYWHERE Terminal window (Alt+Tab).
- 5 Choose PASTE from the Terminal window's Edit menu to place the text in the local terminal window.

Or,

Choose PASTE TO HOST from the Terminal window's Edit menu to send the text to the connected online service.

Adjusting Session Options

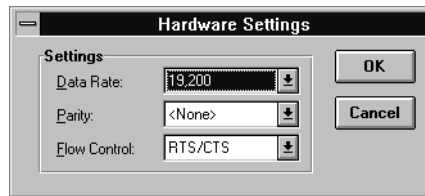
You can adjust hardware, terminal, and display options during a session with an online service. The ability to modify your settings during the session allows you to override settings previously configured from the Configure Terminal Emulation and Configure Hardware Setup dialog boxes. See Chapter 3, "Hardware Configurations." Check with your online service administrator or sysop for the correct session settings.

To adjust hardware settings during an online service session:

- 1 Begin a session with an online service. For details on connecting with an online service, see Chapter 7, "Online Services."
- 2 Choose HARDWARE... from the Session menu.

The Hardware Settings dialog box appears (Figure 8-18).

Figure 8-18 Click the prompt buttons to display options for data rate, parity, and flow control.

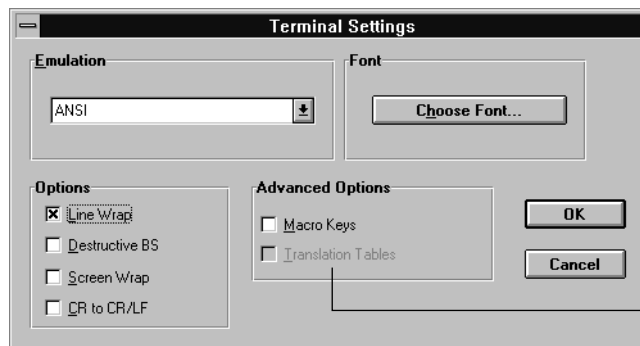


- 3 Select the desired hardware configuration. For a complete discussion of hardware configurations, see “Creating a Modem Hardware Setup” in Chapter 3, “Hardware Configurations.”
- 4 Click OK.

To adjust terminal emulation settings during an online service session:

- 1 Begin a session with an online service. For details on connecting with an online service, see Chapter 7, “Online Services.”
- 2 Choose TERMINAL... from the Session menu.
The Terminal Settings dialog box appears (Figure 8-19).

Figure 8-19 Consult your online service system administrator before adjusting Terminal Settings.



The Translation Table check box is grayed unless a table is selected in the Advanced Online Service Options dialog box

- 3 Select the desired terminal settings.
 - Emulation—Click the prompt button to select a different type of terminal emulation.
 - Choose Font—Click to display the Windows Font dialog box, which allows you to change the font, font style, and point size used to display characters in the Terminal window.

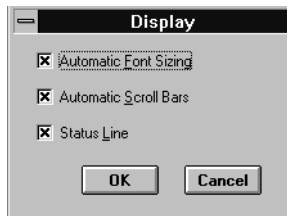
- **Line Wrap**—Check this check box to have the lines of text continue on the next line when the text exceeds the width of the display window. If unchecked, the cursor remains on the same line until a line feed is received.
- **Destructive BS**—Check this check box to cause the Backspace key to delete characters as it passes over them. If unchecked, the cursor moves to the left without deleting characters.
- **Screen Wrap**—Check this check box to control what happens when text fills the entire screen. When this option is checked, the next line overwrites the top line when the cursor reaches the last position on the last line of the terminal display window. If unchecked, the display scrolls, discards the top line of the display, and displays the new line at the bottom of the screen.
- **CR to CR/LF**—Check this check box if the display does not scroll vertically as expected. When this check box is checked, pcANYWHERE moves the cursor to the left side of the terminal window and advances one line when a carriage return is received.
- **Macro Keys**—Check this check box to enable macro keys defined in the Macro Keys dialog box. For information on defining macro keys, see “Setting Up Macro Keys” in Chapter 7, “Online Services.”
- **Translation Tables**—Check this check box to enable a translation table specified in the Advanced Online Services dialog box. For information on creating and editing translation tables, see “Setting Up Translation Tables” in Chapter 7, “Online Services.”

4 Click OK.

To adjust display settings:

- 1 Begin a session with an online service. For details on connecting with an online service, see Chapter 7, “Online Services.”
- 2 Choose DISPLAY... from the Session menu.
The Display dialog box appears (Figure 8-20).

Figure 8-20 You can add scroll bars and a status bar to your computer's Terminal window from the Display dialog box.



- 3 Check the desired display options.
 - Automatic Font Sizing—Norton pcANYWHERE selects a font size based upon the size of the terminal window.
 - Automatic Scroll Bars—Causes horizontal and vertical scroll bars to appear on the screen.
 - Status Line—Causes the status line to appear at the bottom of the screen. This status line contains the terminal type, communication port, data rate, parity, and flow control currently used.
- 4 Click OK to close the dialog box and save the changes.

Ending an Online Service Session

To end an online service session:

- Choose EXIT from the File menu in the pcANYWHERE Terminal Window.

Transferring Files to and from an Online Service

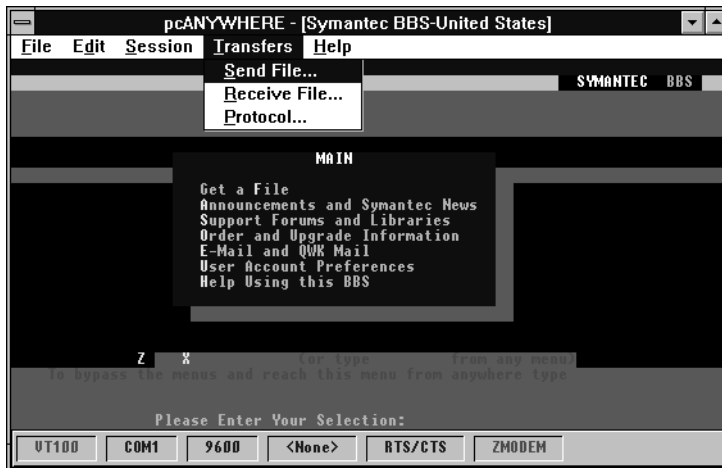
You can receive files from (download) or send files to (upload) an online service. To do so, you must follow the procedures for receiving or sending files, required by the online service and by Norton pcANYWHERE.

You must be sure that both the online service and your PC use the same file transfer protocol. Normally, you specify the name of the protocol as part of the session configuration. To change the protocol used by pcANYWHERE during the session, choose PROTOCOL... from the Terminal window's Transfers menu (Figure 8-21).

Norton pcANYWHERE Terminal mode offers a selection of the most popular file transfer protocols for use with online services. Most online services offer a number of different file transfer protocols, so it should be no problem finding a match.

Some online services let you register a preferred protocol that is used automatically whenever you download a file. Others prompt you to select from a list of available file transfer protocols. If you want to establish a protocol as the default for this online service, you can add this information to the File Transfer Protocol setting in the Edit Online Service Entry dialog box. See “Creating a List of Online Services,” in Chapter 7, “Online Services,” for instructions on establishing a default protocol.

Figure 8-21 Use the Transfers menu to access file transfer functions and protocol settings during a session.

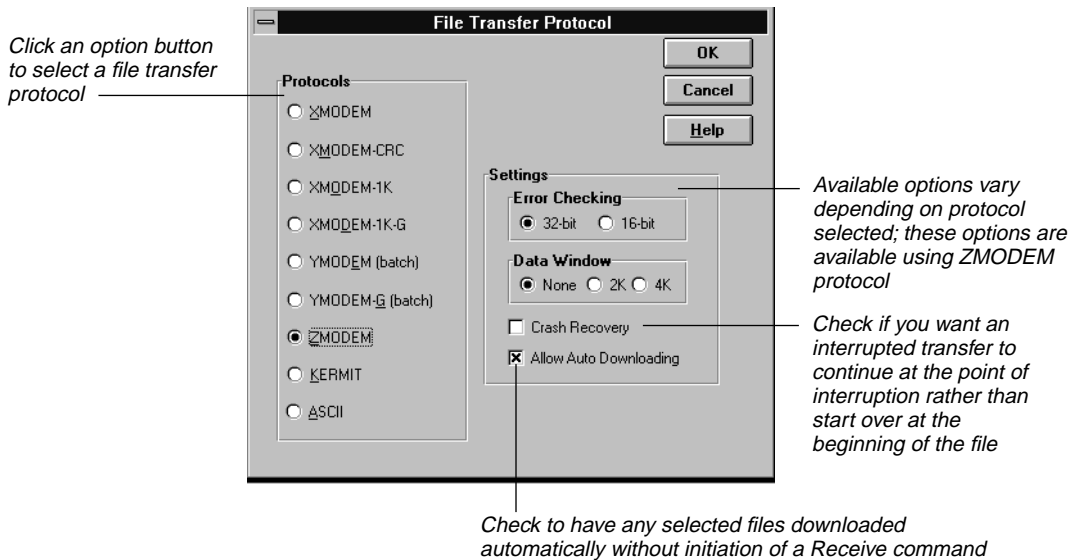


To change the default file transfer protocol during a session:

- 1 Choose PROTOCOL... from the Transfers menu in the pcANYWHERE Terminal window.

The File Transfer Protocol dialog box appears (Figure 8-22).

Figure 8-22 You can change file transfer protocols on the fly.



- 2 Select an option button to select the corresponding protocol.
- 3 Click OK to save the selections.

Selecting Protocol Options

You can customize the ZMODEM and ASCII protocols supported by Norton pcANYWHERE, although this is usually not necessary. For example, you can increase the level of error-checking the ZMODEM protocol uses.

Uploading and Downloading Files

Whether you are downloading (receiving files) or uploading (sending files), file transfer is a cooperative effort between two computers. To download files, first you establish a connection, then you select one or more files and initiate a file transfer using commands dictated by the online service. To complete the operation you need to initiate file receiving at your end of the connection. Uploading files is much the same, except for the direction of the data flow.

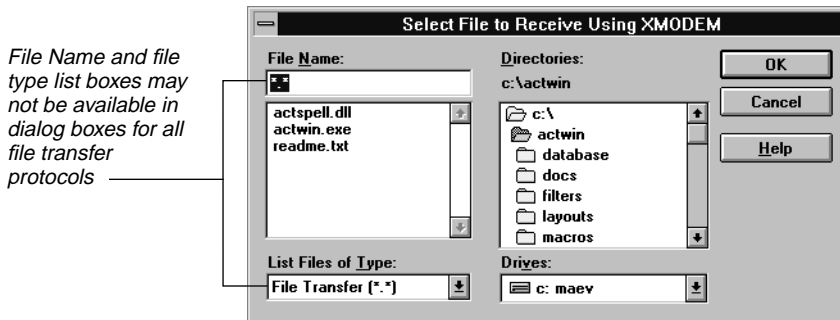
When you transfer files from online services, they are placed in the Norton pcANYWHERE program directory by default. You can change the default by specifying a download, or target, directory. The *target directory* is the directory that will receive the file, while the *source directory* is the directory from which the file is being sent.

To download files from an online service:

- 1 Begin an online service session.
For more information see Chapter 7, “Online Services.”
- 2 Select a file for transfer and initiate download by following the online service’s instructions.
- 3 Choose RECEIVE FILE... from the Transfer menu.

The Select File to Receive dialog box appears (Figure 8-23).

Figure 8-23 The XMODEM dialog box allows you to select a directory and name the incoming file.



- 4 Select the drive and directory in which you want the downloaded file to reside. If the protocol dialog box for the particular protocol you are using provides a File Name text box, you can provide a name for the downloaded file. Otherwise, the file will be downloaded with the original filename.

TIP: If the online service supports it you can use ZMODEM to automate file downloading by enabling the Norton pcANYWHERE Auto Download Protocol Option (see “Selecting Protocol Options” earlier in this chapter). When you use ZMODEM with this feature enabled, Norton pcANYWHERE anticipates incoming files and handles the download procedure automatically. Many online services that support this protocol also support automatic downloading of multiple files and optional automatic logoff upon completion of file transfer. For more information, contact your online service sysop or system administrator.

- 5 Change the target directory, if desired.

- 6 Click OK.

The file is transferred to the indicated download directory.

To upload files to an online service:

- 1 Begin an online service session.

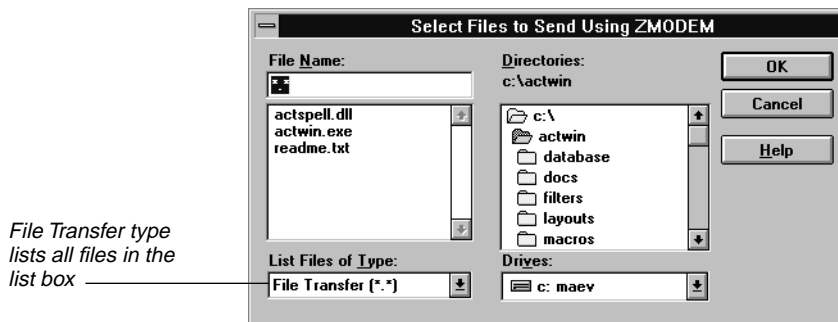
For more information see Chapter 7, “Online Services.”

- 2 Initiate upload according to the online service’s instructions.

- 3 Choose SEND FILE... from the Transfer menu.

The Select Files to Send dialog box appears (Figure 8-24).

Figure 8-24 Select directory and filename to send a file.



- 4 Select a file for uploading.
- 5 If desired, change the target directory or edit the filename.
- 6 Click OK.

The file is sent to the online service.

File Transfer

9

This chapter explains how to transfer files between the host and remote PCs, and manage the files and directories on either computer. You can initiate a file transfer from either the host or remote PC.

Norton pcANYWHERE also supports most popular file transfer protocols for use in sending files to and receiving files from online services such as BBSs and mainframes. See Chapter 8, “Managing Remote Control and Online Sessions,” for information on how to upload or download files during a session with an online service.

This chapter covers:

- Transferring files between pcANYWHERE host and remote computers
- Transferring clipboard contents
- Managing files and directories

Using the Norton pcANYWHERE File Manager

You can use the Norton pcANYWHERE File Manager to transfer files between a remote and a host during remote computing session, and to manage directories and files on both host and remote computers. Some of the more frequently used functions also can be accessed from the button bar at the bottom of the window.

To access the File Manager:

1 Begin a remote computing session. For more information see Chapter 6, “Starting a Remote Computing Session.”

2 Choose ONLINE MENU... from the remote’s Control-menu box.

Or,

Double-click the pcANYWHERE session icon.

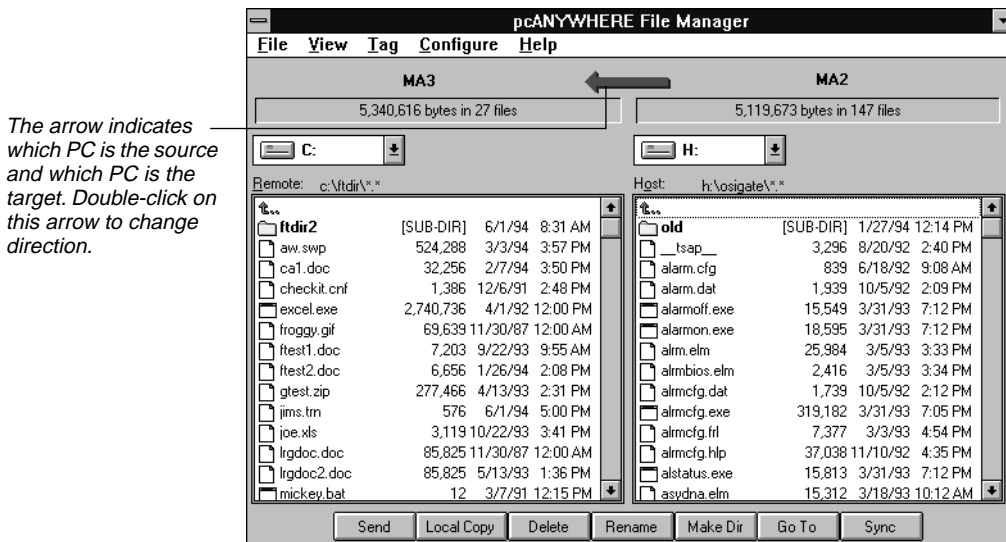
The Remote Online Menu appears.

3 Choose FILE TRANSFER from the Remote Online Menu.

The Norton pcANYWHERE File Manager appears (Figure 9-1).

Use the File manager to select files to transfer between the remote and host PCs, and to manage files and directories.

Figure 9-1 Remote and host files are listed side by side for easy file management.



- 4 Choose EXIT from the File menu to exit the File Manager and return to the host main window and the remote computing session.

Selecting Files and Directories

You must select one or more files or directories before performing file transfer or some file management operations. You can select from either the remote or host list box. Only one of the two list boxes may be active at a time.

The two drop-down list boxes in the File Manager window display the names of the currently selected remote and host drives. The contents of these drives appear in the remote and host list boxes.

Refer to online Help for additional keyboard selection techniques.

To select a different drive:

- Click the prompt button in the drive drop-down list box and select a drive letter from the list that appears.

Or,

- Choose CHANGE DIRECTORY... from the File menu and type the desired drive letter and directory in the New Directory text box.

To display directory contents:

- Double-click the name of the directory that you want to display.

Or,

- Press the UpArrow or DownArrow to highlight the desired directory and press Enter.

To select a single file or directory:

- 1 Click the name of the file or directory.
- 2 Click the name of a second file or directory. Note that the previously selected file is no longer selected.

To select two or more files in sequence:

- 1 Select the first file by clicking its filename.
- 2 Press Shift while clicking the last filename in the group you want to select: Shift+click.

All the files between the first selected file and the last are highlighted.

Or, to use the mouse:

- Select the first file by clicking the right mouse button, then hold the right mouse button down while you drag over the sequenced filenames.

To select multiple files not sequenced:

- 1 Click the first filename.
- 2 Press Ctrl while clicking each of the other filenames: Ctrl+click.
Only the files selected are highlighted.

Or, to use the mouse:

- Select each filename by clicking it with the right mouse button.

Using the Tag Menu to Select Files

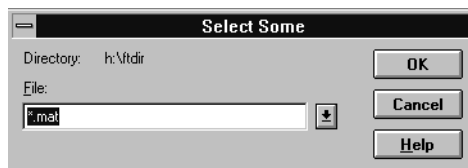
The Norton pcANYWHERE File Manager Tag menu lets you select all or some of the files or directories in the active file list box.

The options available in the Tag menu are:

- TAG ALL—Selects all files and directories in the active list box.
- TAG FILES—Selects all files in the active list box, omitting directories.

- TAG DIRS—Selects all directories in the active list box and the files contained within the directories. Files listed in the active file list box are not included in the selection.
- CLEAR TAGS—Clears all file and directory selections.
- REVERSE TAGS—Deselects the tagged files and directories while selecting the unselected files and directories.
- TAG BY...—Selects files and directories based on a filter you provide (Figure 9-2).

Figure 9-2 You can easily tag all files having the same extension.



Deselecting Files

Just as you can select files using the Ctrl+click or the right mouse button method, you can also deselect files and directories in the same manner.

Refer to online Help for additional keyboard selection techniques.

To deselect a file in a group of selected files:

- Press Ctrl while clicking the names of any selected files or directories you want to deselect.

Or,

- Deselect any selected filename by clicking it with the right mouse button.

Sending Files

This section explains how to transfer files between the host and remote PCs, and how to manage files and directories on either computer. You can initiate a file transfer from either PC. For information on setting file transfer options, see “Setting File Manager Options” later in this chapter.

To send files from a remote to a host:

- 1 Begin a remote computing session. For more information, see Chapter 6, “Starting a Remote Computing Session.”
- 2 Choose ONLINE MENU... from the Control-menu box on the remote.

Or,

Double-click the pcANYWHERE session icon.

The Remote Online Menu appears.

- 3 Choose FILE TRANSFER from the Remote Online Menu.

The Norton pcANYWHERE File Manager appears (see Figure 9-1).

- 4 Select the desired source files or directories in the remote file list box. For more information see “Selecting Files and Directories” earlier in this chapter.

NOTE: The number of selected files and their total size in bytes appears in the status bar above the drive drop-down list box. The arrow that appears between the remote and the host computer names indicates the direction of the file transfer.

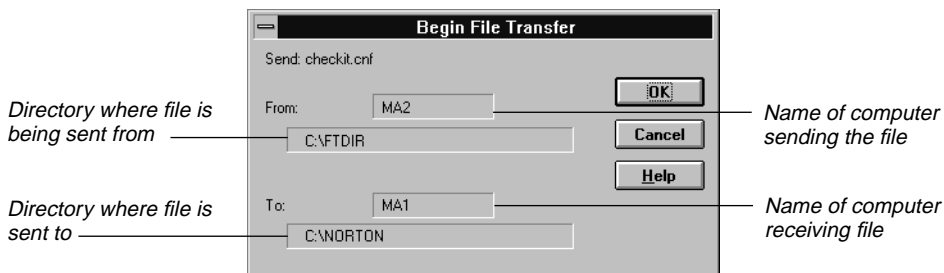
- 5 Select the desired destination directory in the host file list box (see Figure 9-1).
- 6 Click the Send button, or choose SEND from the File menu.

Or,

Use the mouse to drag and drop the selected files to the host list box.

The Begin File Transfer dialog box appears (Figure 9-3) listing the name of the file being transferred, the name of the computer sending the file, the name of the computer receiving the file, and the directory the file is sent to.

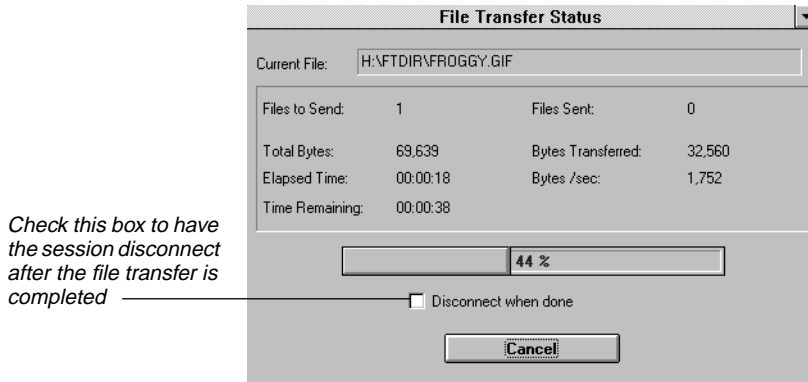
Figure 9-3 Confirm the file transfer before it begins by clicking OK.



- Click OK to confirm the selections.

The File Transfer Status dialog box appears (Figure 9-4), and file transfer begins.

Figure 9-4 The File Transfer Status dialog box monitors file transfer progress.



To send files from a host to a remote:

- Double-click the Norton pcANYWHERE session icon.
The Host Online Menu appears. See Chapter 8, “Managing Remote Control and Online Sessions,” for more details on online menus.
- Choose FILE TRANSFER in the Host Online Menu.
- Select the desired *source* files or directories in the host file list box.
- Select the desired *destination* directory in the remote file list box and click Send, or choose SEND from the File menu.

Or,

Use the mouse to drag and drop the selected files to the desired directory in the remote list box.

The Begin File Transfer dialog box appears (see Figure 9-3) listing the name of the file being transferred, the name of the computer sending the file, the name of the computer receiving the file, and the directory the file is being sent to.

- Click OK to confirm the selections.

The file transfer status dialog box appears and file transfer begins.

Transferring the Clipboard

The Windows Clipboard contains information that is cut or copied from another application. You can use the clipboard to transfer information to or from Windows and non-Windows applications. See your Microsoft Windows documentation for details.

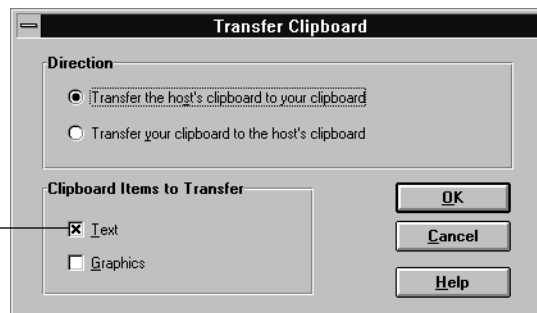
You can transfer text or graphics contained in the host's clipboard to the remote or the remote's clipboard to the host during a remote control session. Remember, copying information into the clipboard overwrites any existing information in the clipboard.

To copy clipboard text:

- 1 Begin a remote computing session. For more information see Chapter 6, "Starting a Remote Computing Session."
- 2 Choose TRANSFER CLIPBOARD... in the remote's Control-menu box. The Transfer Clipboard dialog box appears (Figure 9-5).

Figure 9-5 When you copy text in Windows applications, the information is placed in the Windows Clipboard.

You can choose to send both graphics and text; however, sending graphics slows down the speed of the transfer. Check Text only to improve transfer speed.



- 3 Select the option button to indicate the direction of the clipboard transfer: from host to remote, or from remote to host.
- 4 Check one or both check boxes in the Clipboard Items to Transfer group box to indicate the type of clipboard contents you want to transfer: text, graphics, or both types.

NOTE: Transferring graphic characters will slow down the speed of the transfer. If graphics are not important, uncheck this check box to send only text characters and improve the transfer's performance.

- 5 Click OK.

The clipboard information is transferred in the direction you selected.

Viewing Clipboard Contents

During a remote control session, your keystrokes are executed on the host PC. Clicking the Clipboard Viewer icon in the Windows Main program group displays the contents of the host PC's clipboard. To view the contents of the remote, or local PC, you must tell pcANYWHERE to execute your Windows system key locally.

To view the contents of the host's clipboard:

- While connected to the host, click the Clipboard Viewer icon in the Windows Main program group.

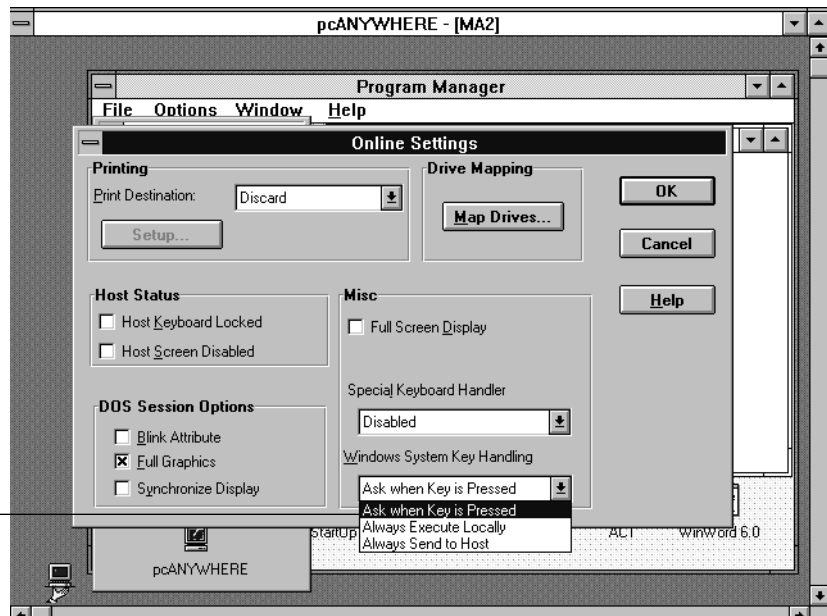
The Clipboard Viewer on the host PC opens, revealing the contents of the host clipboard.

To view the contents of the remote's clipboard:

- 1 Choose ONLINE MENU... from the Control-menu box on the remote. The Remote Online Menu appears.
- 2 Choose ONLINE SETTINGS... from the Remote Online Menu. The Online Settings dialog box appears (Figure 9-6).

Figure 9-6 You can change the Windows system key handling option during the remote control session to view the remote clipboard.

Change system key handling to cause the Alt+Tab Windows system key to execute on the remote PC instead of the host PC



- 3 Select Ask When Key is Pressed from the Windows System Key Handling drop-down list box.
- 4 Click OK to return to the Remote Online Menu.
- 5 Choose RESUME SESSION from the Remote Online Menu.
- 6 Press Alt+Tab to switch between pcANYWHERE and the Windows desktop.

The Windows System Key Pressed dialog box appears (Figure 9-7).

Figure 9-7 Select the Execute Locally option to access the Clipboard Viewer on the remote PC.



- 7 Select Execute Locally and click OK to cause the Alt+Tab key to execute on the remote PC.
- 8 Click the Clipboard Viewer icon in the Windows Main program group.
The contents of the remote's clipboard appear.
- 9 Choose EXIT from the File menu to exit the Clipboard Viewer.
- 10 Press Alt+Tab to return to the remote control session.

Managing Directories and Files

Norton pcANYWHERE File Manager gives you control over directories and files on both the host and the remote computers. This file management is useful when transferring files. For example, you may have connected to a host for the purpose of transferring one or more files to your remote computer, but once connected you realize that there is not a suitable subdirectory in which to place these new files. The MAKE DIR... command allows you to create a directory during a session. If you had been sending files to the host, you could just as easily have created a new directory on the host computer.

Making Directories

You can create a new directory anywhere on any host or remote drive with the MAKE DIR... command.

To create a new directory:

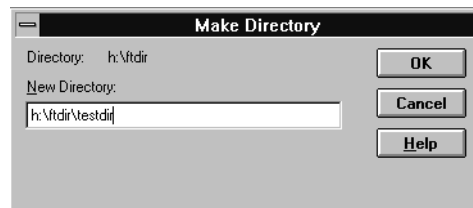
- 1 Start Norton pcANYWHERE File Manager at the remote or host computer. For more information see “Using Norton pcANYWHERE File Manager” earlier in this chapter.
- 2 Select the existing directory in which you would like to place the new directory.
- 3 Click the Make Dir button.

Or,

Choose MAKE DIR... from the File menu.

The Make Directory dialog box appears (Figure 9-8).

Figure 9-8 Use the Make Dir command to create new directories on the fly.



- 4 Type the path and name of the new directory.
- 5 Click OK.
The new directory appears in the active list box.

Deleting Files and Directories

You can delete files and directory contents anywhere on any host or remote drive with the DELETE... command.

To delete files or entire directories:

- 1 Start Norton pcANYWHERE File Manager at the remote or host computer. For more information see “Using Norton pcANYWHERE File Manager” earlier in this chapter.

- 2 Select the files or directories you want to delete. See “Selecting Files and Directories” earlier in this chapter for details.
- 3 Click the Delete button.

Or,

Choose DELETE... from the File menu.

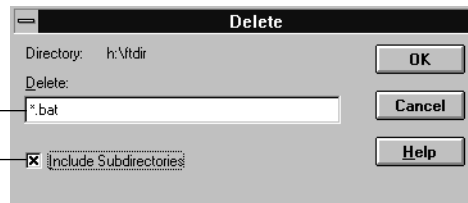
The Delete dialog box appears (Figure 9-9).

If you selected a single file or directory, its name appears in the Delete text box. If you selected multiple files or directories, the text box is replaced with an information line that indicates the number of selected files.

Figure 9-9 You can delete files on remote or host drives.

Entering this text deletes all files in the selected directory having the extension .BAT

Check when deleting directories if you want to delete the contents of all subdirectories



- 4 Click OK.

The file or directory selected is deleted.

Renaming Files and Directories

You can rename files and directories anywhere on any host or remote drive with the RENAME... command.

To rename a file or directory:

- 1 Start Norton pcANYWHERE File Manager at the remote or host computer. For more information see “Using Norton pcANYWHERE File Manager” earlier in this chapter.
- 2 Select the file or directory you want to rename. See “Selecting Files and Directories” earlier in this chapter for details.
- 3 Click the Rename button.

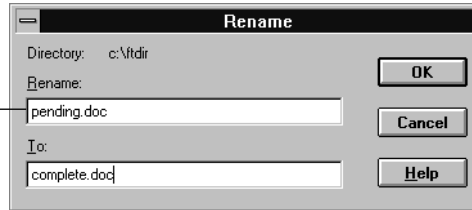
Or,

Choose RENAME... from the File menu.

The Rename dialog box appears (Figure 9-10). The name of the selected file or directory appears in the Rename text box.

Figure 9-10 Rename a file or directory on host or remote drives.

You can use wildcards in the Rename and To text boxes to specify a group of files to rename



- 4 Type the new file or directory name in the To text box.
- 5 Click OK.

Copying Files

You can make a local copy of files anywhere on any host or remote drive with the COPY... command. The new copy of the file can be given a new name or be located in a different directory or drive on the local system.

NOTE: The term *local copy* refers to the fact that this procedure does not transfer files between host and remote computers, thus the file stays local. You can, however, make a local copy on a distant system. That is, you can use a remote to make a local copy of a file that resides on a host.

To copy files and directories:

- 1 Start Norton pcANYWHERE File Manager at the remote or host computer. For more information see “Using Norton pcANYWHERE File Manager” earlier in this chapter.
- 2 Select the file you want to copy. See “Selecting Files and Directories” earlier in this chapter for details.
- 3 Click the Local Copy button.

Or,

Choose LOCAL COPY... from the File menu.

The Copy dialog box appears (Figure 9-11). The name of the selected file appears in the Copy text box.

Figure 9-11 Click the prompt button to select from the last ten copy destinations or type a destination in the To text box.



- 4 Type the destination pathname in the To text box.
- 5 Click OK.

Comparing Directories

The Compare Directories feature looks at both host and remote directories and informs you if they are the same. If the directories differ, the files that are different or missing are highlighted in both directories. The compare directories function only informs you of the differences; no action is taken.

It is a good idea to use the compare directories function before executing a synchronization or cloning command to verify the files that will be transferred.

NOTE: The compare function does not include comparing files in subdirectories at the same time.

To compare directories:

- 1 Start Norton pcANYWHERE File Manager at the host or remote computer. For more information see “Using Norton pcANYWHERE File Manager” earlier in this chapter.
- 2 Select host and remote directories you want to compare from the list.
- 3 Choose COMPARE DIRECTORIES from the File menu.

Norton pcANYWHERE compares the two directories and reports the results of the compare. If the directories are different, the affected files are highlighted. Double-click on the arrow between the computer names to switch between host and remote list boxes and view highlighted files.

Synchronizing and Cloning Directories

The processes of synchronizing and cloning directories are similar and both produce the same end result: host and remote directories will be identical to each other. The way in which these two features act upon directories is very different, however, and you should read this section carefully before using either feature.

Synchronization changes both host and remote directories by copying files in both directions to make the two directories identical to each other. Files that exist on the host but not on the remote are copied to the remote, and files that exist on the remote but not the host are copied to the host. When duplicate filenames are encountered, the date and time stamp of the file are compared and the file with the most current date and time is copied.

In addition to synchronizing directories, you can synchronize selected files. For example, you may want to synchronize only the *.DOC files. Synchronization on selected files ensures that both host and remote directories contain identical files.

Cloning transfers and deletes files to make both directories exactly like the source directory, that is, the directory you are in when you choose the CLONE menu command. Files that are in the source directory but not in the destination directory are transferred. Files that exist in the destination directory that are not in the source directory are *deleted* from the destination directory.



WARNING! Cloning could result in data loss. Files in the destination directory that are not in the source directory will be deleted from the disk. If you are unsure of the files that will be deleted, perform a directory compare first. Comparing directories creates a display of the file differences (see “Comparing Directories” in the preceding section).

To synchronize directories:

- 1 Start Norton pcANYWHERE File Manager at the remote or host computer. For more information see “Using Norton pcANYWHERE File Manager” earlier in this chapter.
- 2 Select the host and remote directories you wish to synchronize.
- 3 Click the Sync button.

Or,

Choose SYNCHRONIZE... from the File menu (Figure 9-12).

The Synchronize Directory dialog box appears (Figure 9-13).

Figure 9-12 Synchronization copies files in both directions resulting in identical directories.

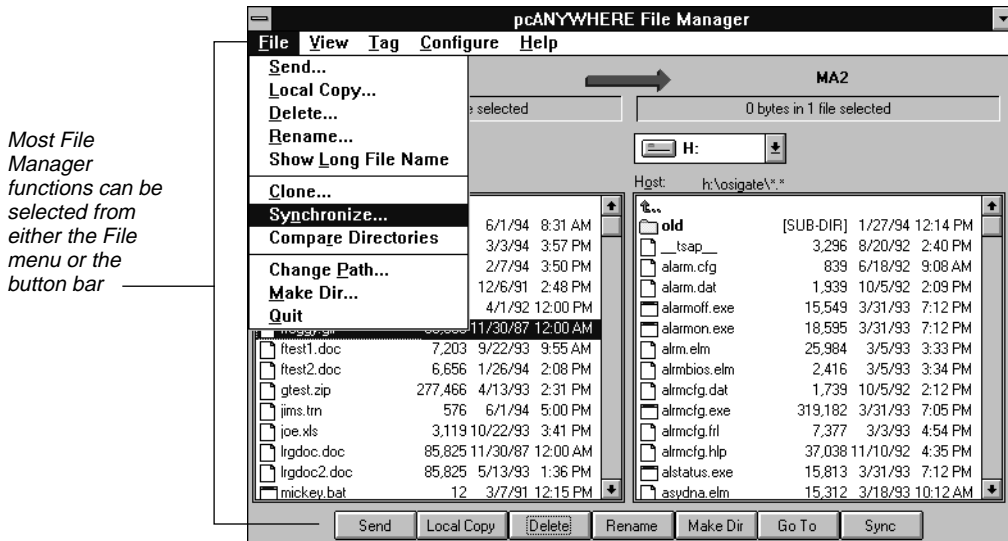
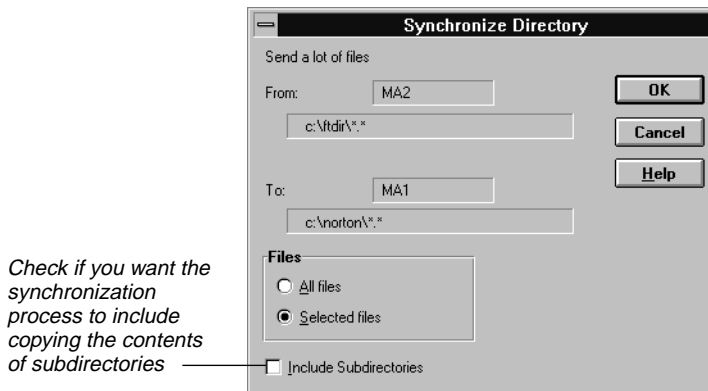


Figure 9-13 To synchronize directories, files are copied from and to the host and remote PC.



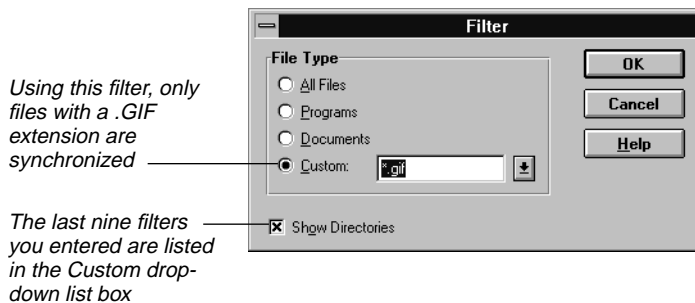
- 4 Verify that the both the host and remote directories are correct in the Synchronize Directory dialog box.
- 5 Click OK to begin synchronization.

To synchronize selected files in a directory:

- 1 Start Norton pcANYWHERE File Manager at the remote or host computer. For more information see “Using Norton pcANYWHERE File Manager” earlier in this chapter.
- 2 Select the remote and host directories that contain the files you wish to synchronize. See “Selecting Files and Directories” for details.
- 3 Choose FILTER... from the View menu.

The Filter dialog box appears (Figure 9-14).

Figure 9-14 Choose Custom to use wildcards to identify what files to synchronize.



- 4 Click the button for the file type you want to synchronize or type in a specific filter in the Custom text box.
- 5 Click OK.
The directory lists only the files specified in the filter.
- 6 Set a filter for the other list box following steps 3 and 4 above.

NOTE: Double-click the arrow between the computer names to easily switch between list boxes. The arrow indicates the direction of the file transfer.

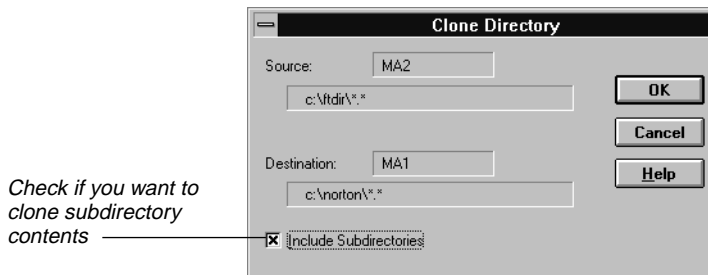
Synchronization affects the files listed in each list box at the time you execute the command. You must create a filter for both host and remote directories to restrict the synchronization process to those specific files.

To clone a directory:

- 1 Start Norton pcANYWHERE File Manager at the host or remote computer. For more information see “Using Norton pcANYWHERE File Manager” earlier in this chapter.

- 2 Select the directory that you want to duplicate (the *source*), then select the directory to be adjusted so that it becomes an exact match of the source directory (the *destination*). See “Selecting Files and Directories” for details.
- 3 Choose CLONE... from the File menu.
The Clone Directory dialog box appears (Figure 9-15).

Figure 9-15 Files in the destination directory that are not in the source directory are deleted.



- 4 Verify that the source and destination directories are correct.
- 5 Click OK to begin the cloning process.

Setting File Manager Options

Norton pcANYWHERE File Manager options include file sorting, file detail, and file transfer preferences.

Selecting File Sorting Options

By default, the files in the host and remote file list boxes are sorted alphabetically by name. You can change the sort criteria using the View menu. You can specify file sorting by name, extension, date, or size. For example, sorting by extension places .DOC files near the top of the list. Sorting by date places your most recently modified files at the top of the list.

You can select the FILTER... option from the View menu to sort files by types. For example, you can choose to view only program files (see Figure 9-14).

NOTE: Before selecting the Documents filter, you may need to edit the DOCUMENTS= line in your Windows WIN.INI file and enter the extensions that Windows should use to recognize files as documents.

To change file sorting for the active file list box:

- 1 Start the Norton pcANYWHERE File Manager on the remote or host computer. For more information see “Using Norton pcANYWHERE File Manager” earlier in this chapter.
- 2 Choose the desired sorting method from the View menu.

Selecting File Details Options

You control the amount of detail displayed for each file listed in the host and remote file list boxes. All listings must contain the file name, but you can choose whether or not to display file date, time, and size.

To change file details for the active file list box:

- 1 Start the Norton pcANYWHERE File Manager on the remote or host computer. For more information see “Using Norton pcANYWHERE File Manager” earlier in this chapter.
- 2 Choose from SHOW DATE, SHOW TIME, and SHOW SIZE on the View menu.

Selecting File Transfer Options

You can select file transfer options such as file overwrite preferences, file compression, and crash recovery settings.

File overwrite preferences allow you to specify whether or not you want to confirm before a file is overwritten during the file transfer process. Normally you should require verification before overwriting files. If you intend to overwrite a large number of files, however, verifying each one could be a nuisance. In this case you may want to choose to overwrite automatically, or to overwrite older files only.

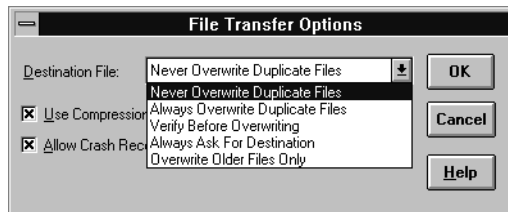
You can use file compression to improve file transfer speed. Files compressed by pcANYWHERE are automatically uncompressed to their original states before being written to the target drive. If files have already been compressed by a compression scheme such as PKZIP, there will be no noticeable improvement in the speed of the file transfer.

When crash recovery is enabled, if a file transfer is interrupted before completion you can reconnect and continue transferring the file from the point at which file transfer was interrupted. If crash recovery is not enabled, an interrupted file transfer starts again at the beginning of the file. You should consider using crash recovery when you transfer very large files.

To set file transfer options:

- 1 Start the Norton pcANYWHERE File Manager on the remote or host computer. For more information see “Using Norton pcANYWHERE File Manager” earlier in this chapter.
- 2 Choose FILE TRANSFER OPTIONS... from the Configure menu.
The File Transfer Options dialog box appears (Figure 9-16).

Figure 9-16 Click the Destination File prompt button to select a file overwrite preference.



- 3 Click the Destination File prompt button and select a file overwrite preference from the drop-down list.
- 4 Check the Use Compression check box to compress files during transfer.
- 5 Check the Allow Crash Recovery check box to enable crash recovery.
- 6 Click OK to save the settings and return to the pcANYWHERE File Manager window. The selections remain in effect for all sessions until you change them.

This chapter explains the utilities that come with Norton pcANYWHERE for Windows. You access these utilities by choosing options from the Utilities menu:

- **PLAYBACK SESSIONS/SCREENS.** This utility plays back recorded remote control and online sessions or specific screens you have saved from these sessions.
- **ACTIVITY LOG PROCESSING.** This utility manages the session data by creating log files that record the time, date, and duration of sessions, as well as other information. You can create a report, delete old log information, or move information to a history file for archiving.
- **SCRIPTS.** This utility allows you to create a new script, edit or compile an existing one, and run it. For information, see the *Creating Norton pcANYWHERE Scripts* manual, which accompanies this user's guide.

Capturing Remote Control and Online Session Information

It is often helpful to have a recording of a session. For example, as the host user demonstrates a complex program or procedure, you can record the host screen instead of taking notes. You then can play back the recording to review the exact steps demonstrated.

Recording Sessions

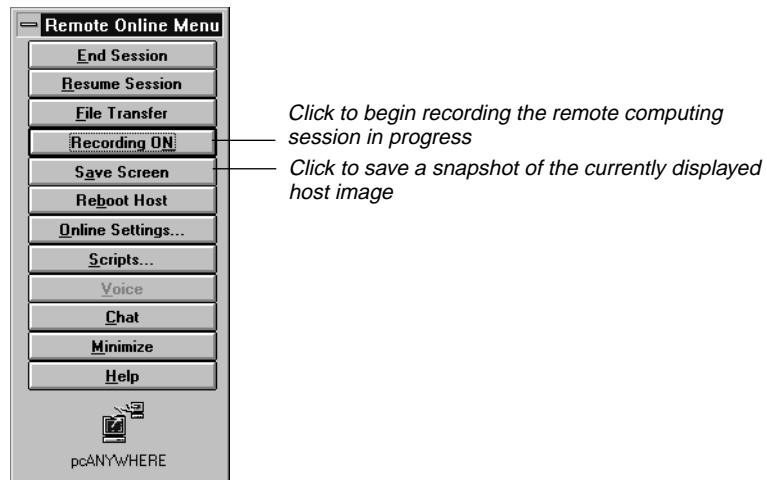
You can record a session manually or automatically in one or more recording (.RCD) files. Recording a session manually is similar to operating a VCR or audio tape recorder. You turn recording on and off as needed. Each start and stop define the beginning and ending of a recorded session. Sessions are numbered in the recording file beginning with 1. To automatically record sessions with specific host PCs and online services, you specify that you want to record the session and the name of the file for the recording as part of the session configuration.

To record a remote control session manually:

- 1 Begin a remote control session (see Chapter 6, "Starting a Remote Control Session").
- 2 Open the pcANYWHERE Session window's Control-menu box and choose ONLINE MENU....

The Remote Online Menu appears (Figure 10-1).

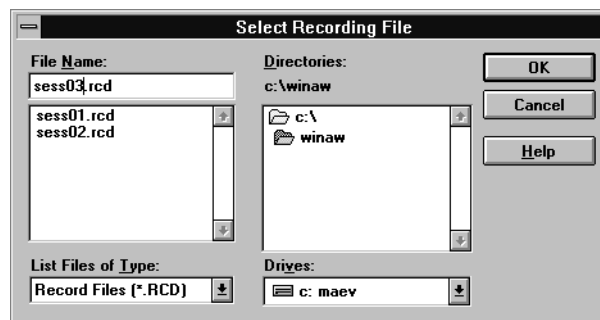
Figure 10-1 The Remote Online Menu lets you enable recording during a remote control session.



3 Choose RECORDING ON.

The Select Recording File dialog box appears (Figure 10-2).

Figure 10-2 The Select Recording File dialog box allows you to designate a filename for the recorded session.



4 Enter a filename for the new recording file.

Or,

Select a filename from the list box to append this recorded session to the existing recording (.RCD) file.

5 Click OK.

NOTE: The RECORDING ON/OFF button operates as a toggle. When you click RECORDING ON to start recording, the button changes to read RECORDING OFF. Click RECORDING OFF to stop recording, and the button changes to RECORDING ON.

To stop recording a remote control session:

- 1 Open the pcANYWHERE Session window's Control-menu box and choose ONLINE MENU....
- 2 Choose RECORDING OFF.

To record a remote control session automatically:

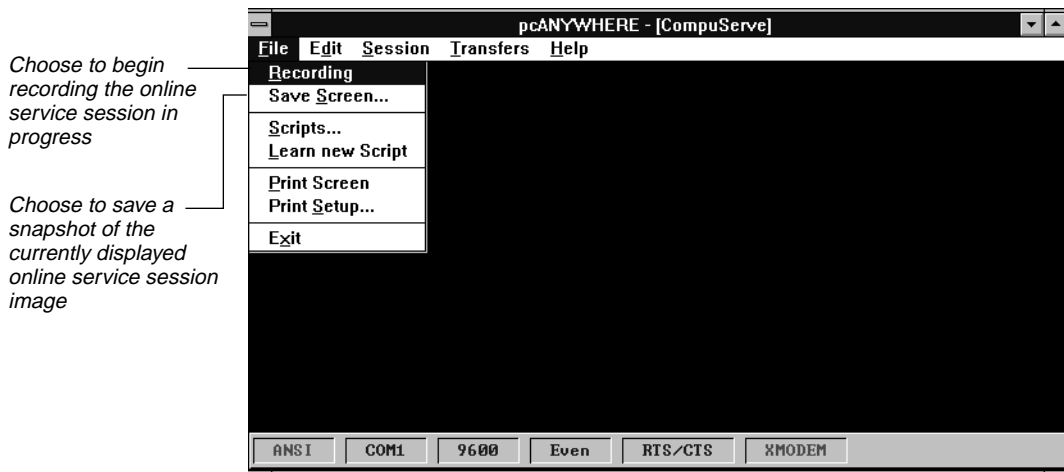
You can specify that all sessions with a particular host be recorded automatically. To do this, you must first modify the host entry in the Host PC Directory list box.

- 1 Click the Call A Host PC load button.
The Host PC Directory main window appears.
- 2 Select a host from the Host PC Directory list box and click Edit....
Or,
Click the New... button.
The Edit Host PC Entry dialog box appears.
- 3 Click the Advanced... button.
The Advanced Host PC Options dialog box appears.
- 4 Check the Record Session in File check box.
- 5 Enter a filename in the text box.
Or,
Click the Browse... button to locate an existing recording file. Norton pcANYWHERE appends the current session to the selected recording file.
- 6 Click OK to return to the Edit Host PC Entry dialog box.
When you begin a session with this host, pcANYWHERE automatically begins recording and saves the session to the specified file. You do not have to turn recording on.
- 7 Repeat steps 2 through 6 to specify automatic session recording for other host PCs.

To record an online session manually:

- 1 Begin a session with an online service (see Chapter 7, “Online Services”).
- 2 Choose RECORDING from the Terminal window's File menu (Figure 10-3).

Figure 10-3 The Terminal Window's File menu lets you enable recording during an online session.



The Select Recording File dialog box appears (see Figure 10-2).

- 3 Enter a filename for the new recording file.
Or,
Select a filename from the list box to append this recorded session to the existing recording (.RCD) file.
- 4 Click OK.
Recording of the session begins.

To record an online session automatically:

- 1 Click the Call Online Service load button.
- 2 Select an online service entry from the Online Service Directory list box and click Edit...
Or,
Click the New... button.
The Edit Online Service Entry dialog box appears.

- 3 Click the Advanced... button.
- 4 Check the Record Session in File check box.
- 5 Enter a filename in the text box.

Or,

Click the Browse... button to locate an existing recording file. Norton pcANYWHERE appends the current session to the selected recording file.

When you begin a session with this online service, pcANYWHERE automatically begins recording and saves the session to the specified file. You do not have to turn recording on.

- 6 Click OK to save the selection and return to the Edit Online Service Entry dialog box.
- 7 Repeat steps 3 through 6 to specify automatic recording for other online services.
- 8 Click OK to save settings and return to the Call Online Service main window.

Playing Back Recorded Sessions

When you play back a recorded session, you need to specify which file and which session within that file you want to replay. The sessions in a file are numbered in the order of their occurrence. pcANYWHERE automatically assigns an .RCD extension to record files.

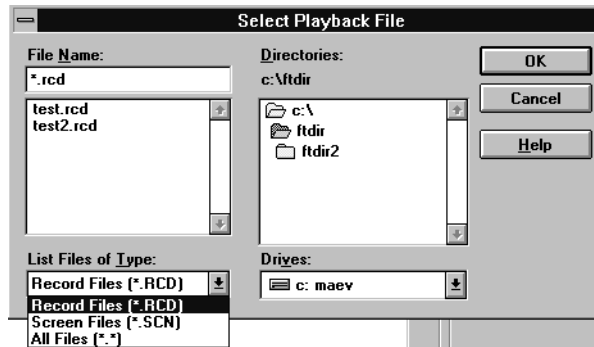
While you replay a session, you can do any of the following:

- Copy a session or a partial session to a new file.
- Save a recorded session as a raw binary file so you can process the text data in an application that requires binary files.
- Save a displayed screen from a recorded session as a screen shot.

To play back recorded sessions:

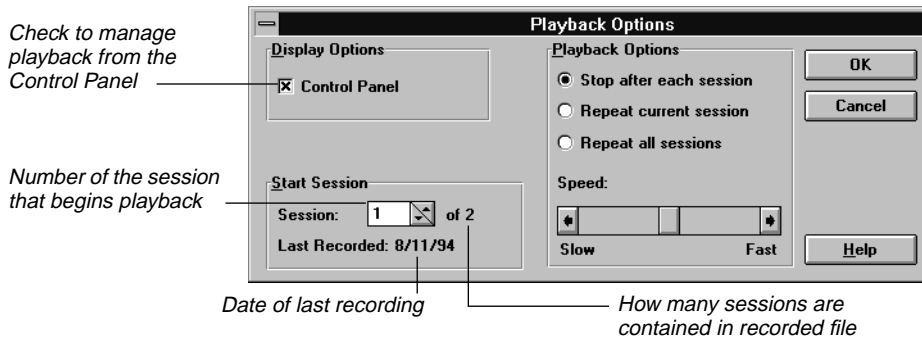
- 1 Choose **PLAYBACK SESSIONS/SCREENS...** from the Utilities menu.
The Select Playback File dialog box appears (Figure 10-4).

Figure 10-4 Select a record file (.RCD) or screen file (.SCN) for playback.



- 2 Select .RCD from the List Files of Type drop-down list box.
- 3 Select a recording file from the File Name list box and click OK. The Playback Options dialog box appears (Figure 10-5).

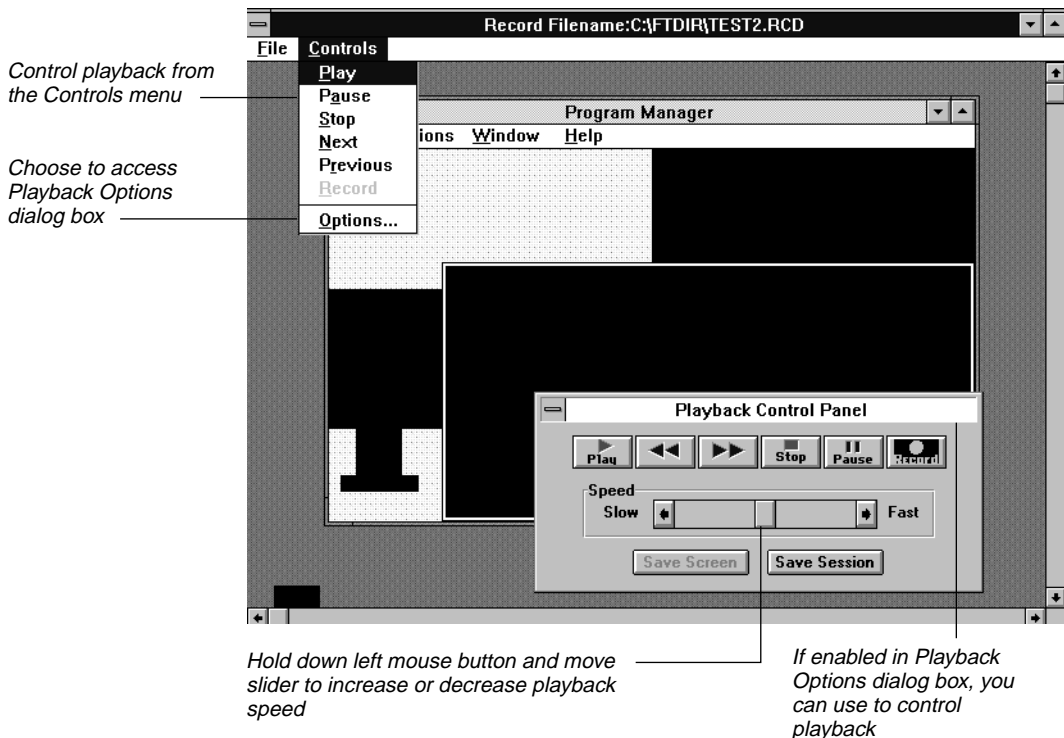
Figure 10-5 You can access the Playback Options dialog box during playback from the Controls menu.



- 4 Select the desired options in the Playback Options dialog box.
 - Control Panel check box—Causes the Playback Control Panel dialog box to appear. If unchecked, the Playback Control Panel does not appear; you select the options from the Control menu.
 - Stop After Each Session option button—Causes the playback to stop after each recorded session. Choose NEXT from the Controls menu or click the >> button in the Control Panel dialog box to continue with the next session.

- Repeat Current Session option button—Causes the session indicated in the Start Session group box to play back continuously.
 - Repeat All Sessions option button—Causes all the sessions in the recorded file to continuously play back.
 - Speed—Causes the playback speed to decrease if the slider is moved to the left and increase if the slider is moved to the right. You can use the speed control slider during a playback.
- 5 Click OK to start the playback. The first session in the selected file plays (Figure 10-6).

Figure 10-6 Control file playback from the Controls menu or from the Playback Control Panel dialog box.



To skip to the next session in the file choose NEXT from the menu bar Controls menu or the >> button on the Control Panel dialog box.

To view the previously displayed session, choose PREVIOUS from the menu bar Controls menu or the << button on the Control Panel dialog box.

To pause the playback choose PAUSE from the Controls menu or click the Pause button on the Control Panel dialog box.

To resume playback, choose PLAY from the Controls menu or click the Play button on the Control Panel dialog box.

To stop the playback choose STOP from the Controls menu or click the Stop button on the Control Panel dialog box. The Playback confirmation box appears.

- 6 Click Cancel to exit the playback session and return to the pcANYWHERE main window.

TIP: To display the Playback Control Panel dialog box, check the Control Panel check box in the Display Options dialog box before you play back the file. You can access the Playback Control Panel dialog box during playback by choosing OPTIONS... from the Controls menu.

Copying a Recorded Session to Another File

You can save all or part of a session to a separate record file or save a session to a raw binary file for use in another application.

To save a recorded session to a new file:

- 1 Choose PLAYBACK SESSIONS/SCREENS... from the Utilities menu.
The Select Playback File dialog box appears.
- 2 Select *.RCD from the List Files of Type drop-down list box.
- 3 Select a file from the File Name list box and click OK.
The Playback Options dialog box appears (see Figure 10-5).
- 4 Select the session to start with in the Start Session group box.
- 5 Click OK to begin playback.

You can move to the beginning of each session in the file by choosing NEXT or PREVIOUS from the Controls menu or clicking the << or >> buttons in the Control Panel.

- 6 Choose RECORD... from the Controls menu or click the Record button on the Control Panel to display the Select Record File dialog box.

- 7 Enter a new filename.
Or,
Select an existing filename to append the current session to the file.
- 8 Click OK.

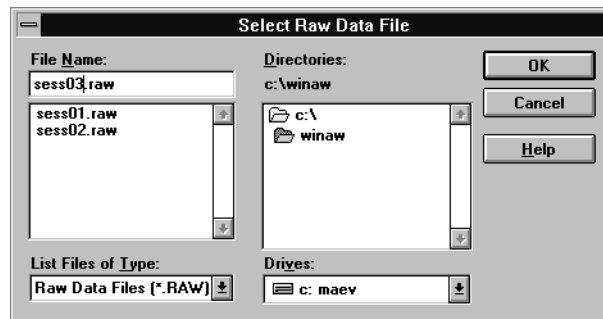
To save a recorded session to a raw binary file:

- 1 Follow steps 1-5 in the previous procedure to play back a session.
- 2 When playback has finished, choose **SAVE SESSION AS RAW BINARY FILE...** from the File menu or click the Save Session button on the Control Panel.

The Select Raw Data File dialog box appears (Figure 10-7).

- 3 Select a drive and directory for the binary file.
- 4 Type a filename in the File Name text box.
- 5 Click OK to save the session and return to the Playback Control Panel dialog box.

Figure 10-7 Saving the text as a binary file allows you to incorporate the data in applications requiring binary files.



Saving Screen Shots

Capturing the contents of the screen during a session is like taking a snapshot with a camera. Norton pcANYWHERE for Windows stores screen shots in a file with an .SCN extension. They appear in the order of occurrence, starting with 1.

To save session screens:

- 1 Begin a remote computing or online session.
- 2 If you are recording a remote computing session, choose ONLINE MENU... from the Control-menu and choose SAVE SCREEN from the Remote Online Menu (see Figure 10-1).

Or,

If you are recording an online session, choose SAVE SCREEN... from the File menu in the Terminal window (see Figure 10-2).

The Select Screen Filename dialog box appears.

- 3 Enter a new filename to create a new file for the screens.

Or,

Select an existing file to append the screens from the current session to the file.

- 4 Click OK.

Repeat steps 2 through 4 for each screen you wish to save. The screens are saved in the selected file in the order they are captured, starting with 1.

Saving Screens from Record Files

You can save one or more screens that appear in a recorded file. The procedure for doing this is similar to the one used to save screens during a session. You can save any number of screens from one or more recorded sessions as the session is played back.

To save screens from a record file:

- 1 Choose PLAYBACK SESSIONS/SCREENS... from the Utilities menu.
The Select Playback File dialog box appears.
- 2 Select .RCD from the List Files of Type drop-down list box.
- 3 Select a file from the File Name list box and click OK.
The Playback Options dialog box appears (see Figure 10-5).
- 4 Select the session to start with in the Start Session group box.
- 5 Click OK to begin playback.
- 6 Locate the desired session by choosing NEXT or PREVIOUS from the Controls menu or clicking the << or >> buttons in the Control Panel dialog box.

- 7 When the desired screen appears, choose PAUSE from the Controls menu or click the Pause button in the Control Panel dialog box.
- 8 Choose SAVE SCREEN... from the File menu.
Or,
Click the Save Screen button on the Control Panel.
The Select Screen Filename dialog box appears.
- 9 Enter a filename.
Or,
Select an existing filename to append the screen to a file.
- 10 Click OK.

NOTE: You cannot save graphical display data as ASCII text. If pcANYWHERE cannot translate a screen into ASCII text, the SAVE SCREEN AS ASCII menu item is dimmed.

Displaying Screen Shots

When you review screen shots, you need to specify which file and which screen shot within that file you want to see. The screen shots appear in the order in which they are captured.

While you are viewing a screen shot, you can:

- Copy it to a new .SCN file.
- Save a screen shot that contains only text to an ASCII file with the extension .TXT. This allows you to print the screen shot or import it into another application as text.

To review screen shots:

- 1 Choose PLAYBACK SESSIONS/SCREENS... from the Utilities menu to display the Select Playback File dialog box.
- 2 Select .SCN from the List Files of Type drop-down list box.
- 3 Select a screen file from the File Name list box and click OK.

The playback window appears and the first screen of the selected file is displayed.

- 4 Choose NEXT from the Controls menu to display the next screen in the file or click the >> button in the Playback Control Panel dialog box.
Or,
Choose PREVIOUS from the Controls menu to return to the previous screen or click the << button in the Playback Control Panel dialog box.
- 5 Click the Stop button in the Playback Control Panel to cancel the playback and return to the Norton pcANYWHERE main window.

Saving Screens as Plain Text

If you want to print out a screen or import it into another application, be sure to save the screen as a text file.

To save a screen as an ASCII text file:

- 1 Display the desired screen. (see “Displaying Screen Shots” in the previous section.)
- 2 Choose SAVE SCREEN AS ASCII from the File menu to display the Select Text File dialog box.
- 3 Enter a filename.
Or,
Select an existing filename to append the screen to the file.
- 4 Click OK.

NOTE: You cannot save graphical display data as ASCII text. If pcANYWHERE cannot translate a screen into ASCII text, the SAVE SCREEN AS ASCII menu item is dimmed.

Logging Remote Control and Online Sessions

You can log information about remote control and online sessions for curiosity, historical, or security purposes. For example, you may want to know just how often you call a particular host PC or online service or keep track of your total time online.

When a remote PC connects to either a host PC or an online service using a session configuration, an option in that configuration determines whether or not the session is logged on the remote PC. The remote log file is named AW.RL6, or AW*userid*.RL6 if the user is running a workstation version of pcANYWHERE (see Chapter 2, “Installation and General Setup”).

Similarly, the caller privileges set on the host PC determines whether or not the host logs the session. The host log file is *AW.HL6* or *AWuserid.HL6*.

When new log information is collected, it is appended to the existing log files. Consequently, log files can become very large. Norton pcANYWHERE includes an archive feature that moves older data (specified by date) into an archive file. The preserved information can be referenced at a later date. You can also delete log information without archiving it. The remote history log filename is *AW.RH6* or *AWuserid.RH6*, which stores data archived from the remote log file. The host history log filename is *AW.HH6* or *AWuserid.HH6*, which stores data archived from the host log file.

The log files are located in the directory where Norton pcANYWHERE for Windows is installed.

To log sessions on the remote PC:

- 1 Click the Call A Host PC load button.
The Host PC Directory main window appears.
- 2 Select a host and click Edit....
The Edit Host PC Entry dialog box appears.
- 3 Click the Advanced... button.
The Advanced Host PC Options dialog box appears.
- 4 Check the Save Session Statistics In Activity Log File check box.
- 5 Click OK.
- 6 Repeat the previous steps for each host you want to log.

NOTE: Remote logging can also be enabled for sessions with online services. Click the Call Online Service button. Then edit the Online Services Directory entry for each online service you want to log.

To log sessions on the host:

- 1 Click the Be A Host PC load button.
The Be A Host main window appears.
- 2 Select the Callers Have Individual Privileges option button.
- 3 Click the Settings... button.
The Caller List dialog box appears.

- Select a caller from the Caller List.

NOTE: If the Default Privileges option button is selected, the Edit Caller Entry dialog box appears instead of the caller list.

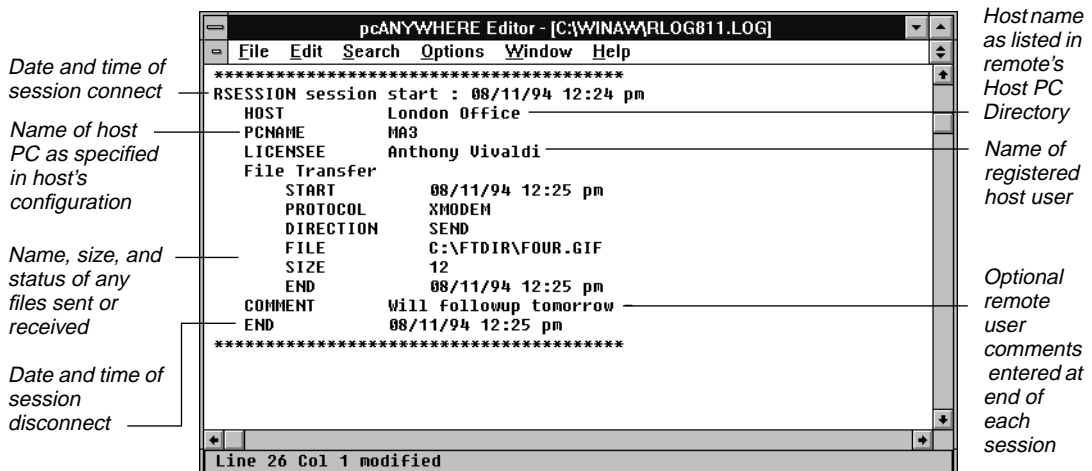
- Click Edit... to display the Edit Caller Entry dialog box.
- Click the Advanced... button.
The Advanced Caller Options dialog box appears.
- Check the Save Session Statistics in Activity Log check box in the Other Session Parameters group box.
- Click OK to save the settings and return to the Edit Caller Entry dialog box.
- Click OK to return to the pcANYWHERE main window.
The session statistics are recorded in the host's log each time this caller connects to the host.

Creating an Activity Log Report

From the information stored in log files, you can create a chronological listing of connections called an *activity log report*. You can display this report on screen or write it to a text file to print later.

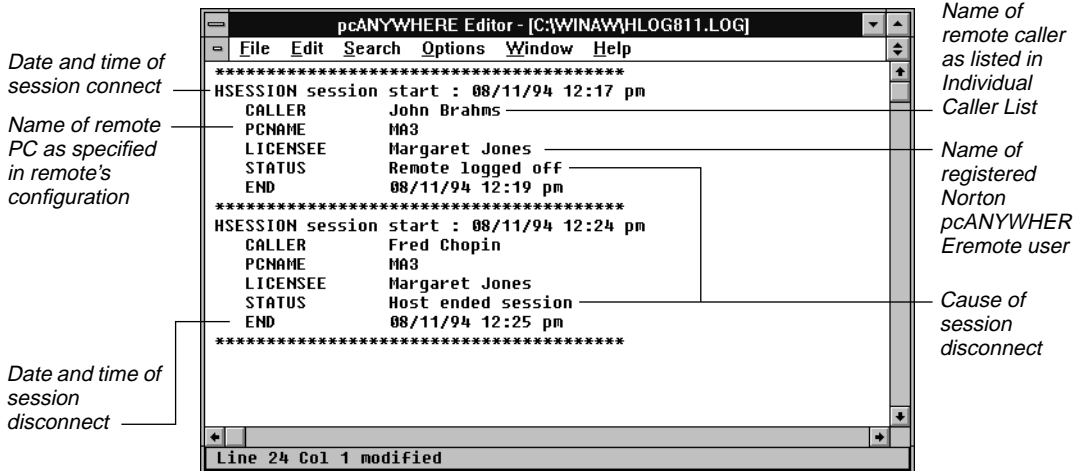
Remote logging of host connections includes data for each logged session (Figure 10-8).

Figure 10-8 The Remote's report of host connections lists detailed information of session activities.



Host logging of remote connections includes data for each logged session (Figure 10-9).

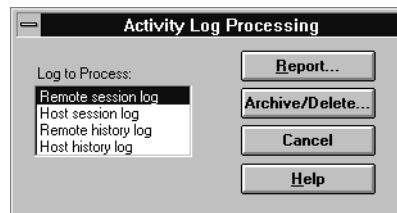
Figure 10-9 The host's report of remote connections identifies the remote callers.



To create and view a remote report of host connections:

- 1 Choose ACTIVITY LOG PROCESSING... from the Utilities menu.
The Activity Log Processing dialog box appears (Figure 10-10).

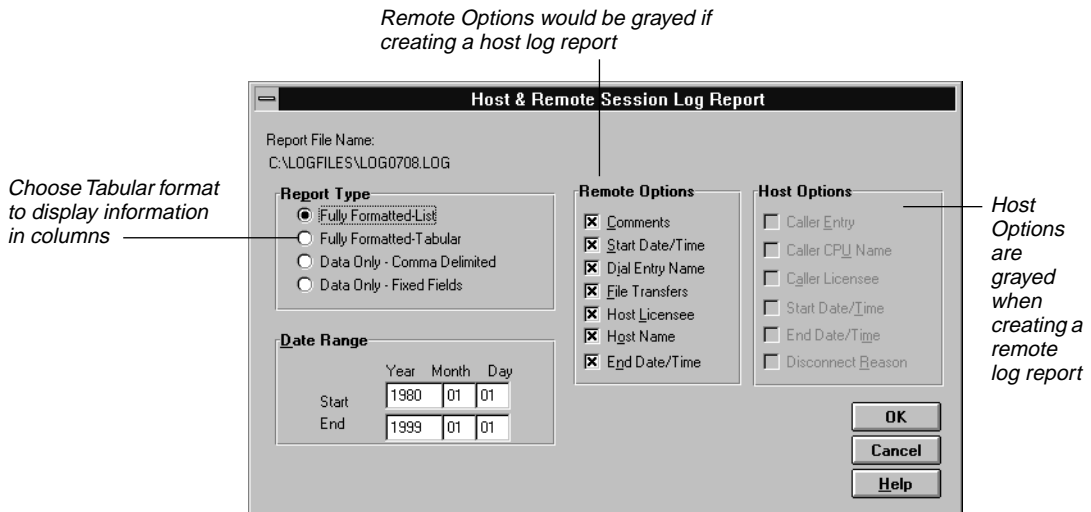
Figure 10-10 Log processing options include creating reports and archiving log data.



- 2 Select Remote Session Log from the Log to Process list box and click the Report... button.
The Select Destination File for Output dialog box appears.
- 3 Enter a filename in the File Name text box.
- 4 Click OK.

The Host & Remote Session Log Report dialog box appears (Figure 10-11).

Figure 10-11 Fully formatted reports include field titles with the data.



- 5 Check the check boxes to indicate which data to include in the report.
- 6 Enter start and end dates in the Date Range group box and click OK.
At the completion of the report generation, Norton pcANYWHERE asks you if you want to view the report.
- 7 To view the report, select Yes. The file is loaded into a text editor and can be viewed and printed.

To end session log report processing:

- 1 Choose EXIT from the File menu of the text editor.
- 2 Click the Cancel button in the Host & Remote Session Log Report dialog box.

To create a host report of remote connections:

- 1 Choose ACTIVITY LOG PROCESSING... from the Utilities menu to display the Activity Log Processing dialog box.
- 2 Select Host session log from the Log to Process list box and click the Report... button.

The Select Destination File for Output dialog box appears.

- 3 Enter a filename in the File Name text box.
- 4 Click OK.
The Host & Remote Session Log Report dialog box appears (see Figure 10-11).
- 5 Check the check boxes to indicate the data you want to include in the report.
- 6 Enter start and end dates for the sessions you want to include in the Date Range group box.
- 7 Click OK.
The report is generated. The report file is an ASCII text file that can be viewed or printed. At the completion of the report generation, Norton pcANYWHERE asks you if you want to view the report.
- 8 To view the report, select Yes. The file is loaded into a text editor.

To end session log report processing:

- 1 Choose EXIT from the File menu of the text editor.
- 2 Click Cancel in the Host and Remote Session Log Report dialog box.

Deleting and Archiving Logged Information

When new log information is saved in an existing log file, it is appended to the file, causing the file to increase in size. When a log file becomes too large, you may want to delete or archive some of the older data in it.

To delete or archive log file data:

- 1 Choose ACTIVITY LOG PROCESSING... from the Utilities menu to display the Activity Log Processing dialog box.
- 2 Select Host session log or Remote session log from the Log to Process list box.
- 3 Click Archive/Delete to display the Archive/Delete Host/Remote Log dialog box (Figure 10-12).

Figure 10-12 To delete information without archiving check Delete and uncheck Copy.



- 4 Enter start and end dates for the data you want to archive or delete in the Date Range group box.
- 5 Check the Copy Log Entries to Archive File check box to copy the data to a compressed archive file.
- 6 Check the Delete Log Entries from source check box to delete the data from the log file.
- 7 Click OK.

Creating Activity Reports Using Archived Data

Like activity log file data, archive file data can be used in a report. The procedure is very similar to the procedure for generating a report from a log file.

To create an activity report from archived data:

- 1 Choose ACTIVITY LOG PROCESSING... from the Utilities menu to display the Activity Log Processing dialog box.
- 2 Select the Host History Log or Remote History Log from the Activity Log Processing dialog box (see Figure 10-10) and click the Report... button.
- 3 Create the report as described in the procedures for session logs.

Technical Information



This appendix covers technical information about serial port connections, pcANYWHERE command-line options, and Windows communication issues.

- The PC, which sends data via its CPU and a serial port
- The modem, which allows the PC to make a connection via telephone lines
- The role of the data rate, flow control, and cables in the transmission of data
- The use of special telephone lines (leased lines and multiplexers)
- Error detection and correction
- pcANYWHERE command-line options
- Windows communication issues

The Role of the PC

Your PC relies on an electronic component known as the CPU, or *central processing unit*, to control all the various processes involved in the computing tasks that you ask the PC to do. This includes sending data to a serial port, also called a communications (or COM) port, that passes it on to a modem.

Serial Port Addressing

The CPU uses a system of addresses to control the physical components that make up your computer and its attached devices. Like postal addresses that you use to send written correspondence, these addresses allow the CPU to send instructions to the various components under its control. An address points to a *virtual* location rather than a physical location within the computer.

Each serial port in your system is assigned a unique address. The standard addresses for each of the four serial ports supported by DOS-based PCs are shown in Table A-1. When an adapter card containing a serial port is installed, its port is configured to one of these addresses. (For more information see your computer hardware manual or the adapter card's manual.) Some cards allow you to specify custom addresses. Norton

pcANYWHERE hardware configurations can support both standard and custom port addresses.

Table A-1 Each of the four COM ports has a standard I/O (input/output) address and IRQ (hardware interrupt) line.

COM Port	Address	Interrupt (IRQ)
1	3F8-3FF hex	4
2	2F8-2FF hex	3
3	3E8-3EF hex	4
4	2E8-2EF hex	3
COM Port	Address	Interrupt (IRQ)

NOTE: DOS versions before 3.3 do not support COM3 and COM4.

An external modem is attached to one of the standard PC serial ports. An internal modem has its own serial port. You may use a custom address and IRQ to define an additional communications port for your internal modem board (or another serial board). When you do this, the modem has a custom port.

Hardware Interrupts

The CPU controls many processes within the computer. While it is busy performing one task, a program or hardware component may need to get the CPU's attention for a more urgent task. The program or device sends a special signal that interrupts the task at hand. For example, when you press a key on your computer's keyboard, it sends a hardware interrupt request (IRQ) to the CPU. Unless the CPU is engaged in a critical task, it puts whatever it is doing aside to process your keystroke.

Each hardware component that needs to send interrupt requests is assigned a direct line to the CPU for that purpose. Each serial port is assigned a standard interrupt request line (Table A-1). Unfortunately because the original designers of the IBM PC only envisioned a need for two COM ports, there is a shortage of IRQ lines. COM1 and COM3 share one IRQ line, and COM2 and COM4 share another. In this way, all four COM ports can be enabled using the original two IRQ lines reserved for serial communications. This sharing of IRQ lines works fairly well most of the time.

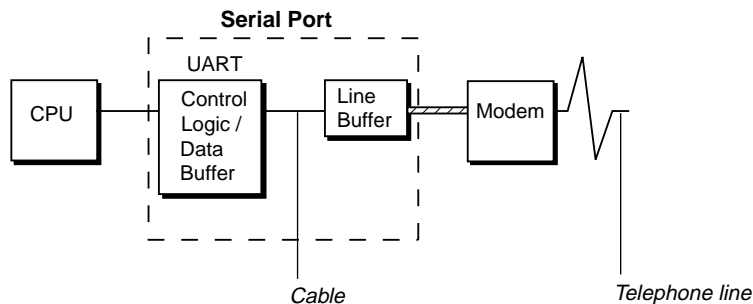
NOTE: Two ports sharing one IRQ line cannot be active at the same time. If both ports send an interrupt request to the CPU at the same time, the resulting confusion can force you to reboot your computer. For example, if your mouse is on COM1 and your modem is on COM3, moving your mouse can interfere with your modem. pcANYWHERE does not support IRQ sharing.

UARTs

The UART (universal asynchronous receiver transmitter) controls the transfer of data through a serial port. It contains both the receiving and transmitting circuits needed for serial communication. The most common UARTs found in PCs are the 8250, 16450, and 16550A.

Figure A-1 represents the CPU, the serial port, a cable, and an external modem. The UART is part of the serial port. If you have an internal modem, the serial port is part of the modem.

Figure A-1 A CPU, serial port, cable, external modem, and telephone line.



The 8250 UART was the standard UART in the original IBM XT, but some IBM-compatible ATs contain 8250 UARTs. The 16450 UART is standard on most 286 (AT), 386, and 486 PCs. Both UARTs generate an interrupt for each character that is sent or received. At data rates above 19,200 bps, this can slow down the computer as it handles the high volume of serial port interrupts. The UARTs also have a one-character buffer. At high data rates, in a multitasking operating system such as Windows, the computer does not have time to get the character before the next character overwrites it.

The 16550A UART can help handle these two problems. It has a 16-character data buffer and it generates an interrupt when the buffer is nearly full. This

reduces the number of interrupts the computer must handle, and allows more time for the computer to get the characters before they are overwritten. Norton pcANYWHERE automatically detects and enables the buffering capabilities of this UART.

In a multitasking OS such as Windows, it is possible to lose characters at high data rates with a 16550A UART. To handle the higher data rates of v.32bis and v.34 modems, manufacturers are releasing serial cards and internal modems that have buffers that can store 1,000 characters or more. Frequently, these devices emulate a 16550A; if this is the case, Norton pcANYWHERE automatically detects and enables the buffering capabilities.

The Role of the Modem

A PC sends data as electrical current that is understood as a series of ones and zeros. This type of communication is called *digital communication* because the individual charges are represented as one-digit numbers. The number one represents an “on” charge or *bit* (binary digit), and a zero represents an “off” bit. A set of eight bits makes a *byte*. Each byte represents a character (such as an integer from 0 to 9 or a letter of the alphabet).

The public telephone network was designed and constructed for voice communications, which is very different. As you speak into the telephone the full range of modulation in frequency produced by your voice is carried over the telephone lines to the party on the other end of the connection. This is called *analog communication*.

When data is transmitted between PCs over telephone lines, data is sent from one PC's serial port to a *modem*, which converts the data into a signal that can be carried over telephone lines. This is called *modulation*. At the receiving end, the process is reversed. The modem converts the signal into computer data and sends it to the PC through a serial port. This is called *demodulation*. The term *modem* is a contraction of the words *modulate* and *demodulate*.

Speed

Each modem has a range of line speeds at which it can transfer data over telephone lines. During a remote control or online session, the two modems involved communicate at the same speed. Most modems are “smart” enough to figure out the highest speed mutually available. Speeds such as 9600 and 14,400 are more commonly used in modem communications.

The speed of a modem is measured in *bps*: bits per second. This term is commonly, but incorrectly, used interchangeably with *baud*. A baud rate is a measure of how many times per second the modem's modulated analog signal changes states. Most 1200-bps modems operate at 300 baud and transmit four bits per baud to achieve a transfer rate of 1200 bps. As you can see a 1200-bps modem is not a 1200-baud modem. (In fact there is no such thing as a 1200-baud modem.) Most 2400-bps modems also send four bits per baud, but operate at 600 baud to achieve a data transfer rate of 2400 bps.

Data Compression

Modems that use data compression can move data faster than their normal transmission speed by compressing the data before sending it. This reduces the number of bytes needed to transmit the information. The receiving modem decompresses the data. By adding data compression to their modems, manufacturers can significantly boost the data throughput. Up to four times as much data can be sent, depending on the compression method used.

For data compression to work, both modems must use the same compression protocol (such as MNP5 or V.42bis). How well it works depends on the type of data. For example, a text file (.TXT) can be compressed more easily than an executable file (.EXE) or a file that has already been compressed, such as a .ZIP file. For more information on data compression, see your modem's manual.

Modem Commands

The primary job of the modem is to process the data it transmits and receives across telephone lines. When it is performing this function it is in *data mode*. But modems must also respond to software-generated modem commands. When the modem is processing these commands, it is in *command mode*. Modem commands perform many activities from dialing a telephone number to selecting a modem protocol. Norton pcANYWHERE issues an *initialization string* setting various modem parameters to their optimum values. The software also issues a command that dials a telephone number to establish contact with another modem.

Modem commands can also be issued directly. Most modems provide a *Hayes-compatible* command mode. The Hayes AT Command Set was developed by Hayes Microcomputer Products, Inc. for its Smartmodem 2400 product line. Additional commands and enhancements often are added by individual manufacturers. Both types of commands may be appended to the

standard initialization string that pcANYWHERE uses for your modem type (see Chapter 3, “Hardware Configurations”). For more information on AT and other modem commands, see your modem’s manual.

Modem Switches

Some modems use physical switches instead of modem commands to control certain functions. If your modem uses external switches you must set them to be compatible with Norton pcANYWHERE. See Table A-2 for the correct switch positions for most switched modems. See your modem’s manual for the location of each of these switches. Don’t worry if your modem doesn’t have switches for all the listed functions.

Table A-2 Some modems use physical switches to control certain functions.

Function	Switch Setting
Support DTR	ON
Digit Codes	ON or OFF
Send Results	ON
Echo Commands	ON
No Auto Answer	OFF
Support DCD	ON
Type of Jack	ON for single line OFF for multi-line
Allow Commands	ON
No hang on +++	OFF
Defaults from NRAM	ON

If you select Manual modem, you should fill in the other fields on the form yourself, according to instructions in your modem’s manual.

In this case, Norton pcANYWHERE does not use the telephone number entered in the session configuration. Instead, you must enter the telephone number, along with any modem initialization commands, as the setting for the Additional Modem Initialization String option in the hardware configuration. You should not use Modem response in the Connection Started By option. Check your manual for the correct setting; most modems use Carrier Detect (DCD). Set the data rate according to instructions in your modem’s manual.

Using the PC and the Modem Together

During a remote control or online session, the PC's CPU sends data to the serial port which, in turn, relays the data to one of the following:

- To an external modem, which is outside the PC, by way of a cable (Figure A-1)
- Directly to an internal modem, which is inside the PC
- Over a null modem cable to another computer

Data Rate

The data rate is the rate at which the CPU sends data to the serial port (and, therefore, to the modem). A null modem cable tricks two computers into thinking that they are connected via modems by crossing two or more of the serial lines. A null modem cable can transfer data at rates of 19,200 bps or greater, depending on the speed of the PCs and the capabilities of the serial ports. High-performance modems using data-compression techniques push the data transfer rate even higher. For a modem using data compression, the data rate may be four times the maximum speed of the modem.

The data rate is generally much higher than the line speed of the modem because the modem compresses the incoming data. However, because different blocks of data have different amounts of compression, the modem needs to periodically stop the flow of data from the PC while it catches up. *Flow control* temporarily halts data transmission while the modem sends the rest of the data block.

Flow Control

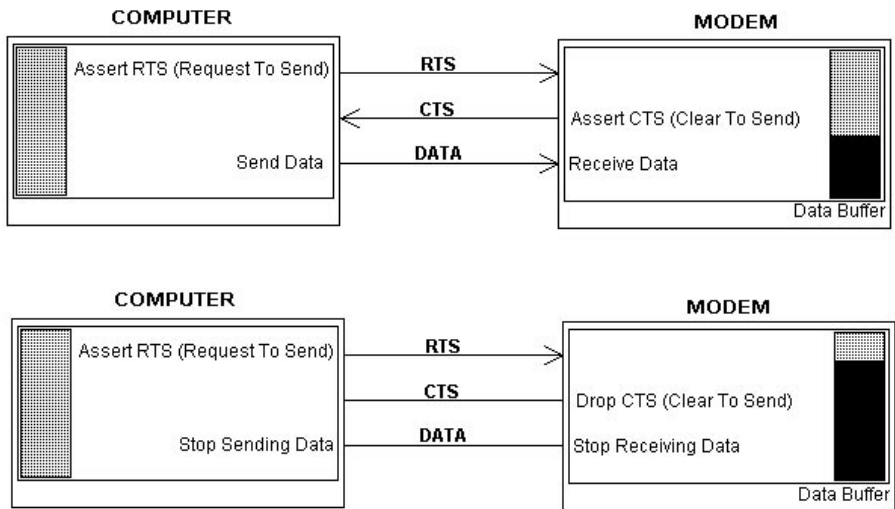
To avoid losing any data, *flow control* starts and stops data transmission. The modem and CPU signal each other by sending signals over the RTS and CTS lines of the RS-232 serial interface or special characters embedded in the data stream. For example, the modem may want to halt data transmission because the data is not compressing well, and the CPU may want to halt data transmission while it writes to disk.

Hardware flow control uses the RTS and CTS lines in the serial connection (Figure A-2) to start and stop data flow. For external modems, it is important that the cable pass these signals from the serial port to the modem.

Software flow control (XON/XOFF), used only in some online sessions, inserts special characters into the data flow itself to stop and restart transmission.

In either case, the receiving device transmits a signal to the sending device to stop the flow of data. When the buffer clears, the receiving device sends a signal to restart the flow.

Figure A-2 Hardware flow control stops data flow to avoid overflowing the data buffer.

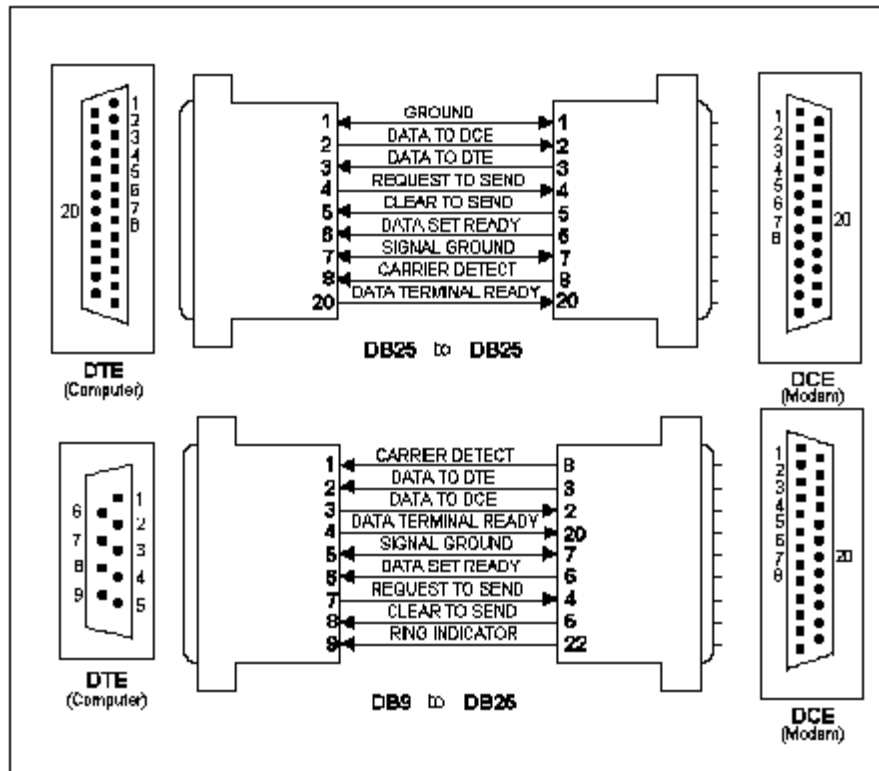


NOTE: Modems that use data compression must use hardware flow control.

Standard Serial Cables (RS-232-C)

When selecting a cable, the first thing to look for is RS-232-C compatibility. Because the standard covers a lot more than just modem connections, a "compatible" cable may not always implement all the RS-232-C signal lines. Cables for use with pcANYWHERE should include the nine signal lines shown in Figure A-3.

Figure A-3 Serial connectors have either 9 pins (DB9) or 25 pins (DB25).



Be sure that the cable you select has the correct type of connectors on either end. Computer equipment, called DTE (Data Terminal Equipment) by the standard, generally requires a cable with a female connector. This is connected to the serial port. Modem equipment, called DCE (Data Communications Equipment), usually requires a cable with a male connector. (Check your modem to be sure.) The cable you select will probably have a female connector at one end and a male connector at the other. The exception to this rule is the null modem cable (sometimes called a modem replacer) covered next in this appendix.

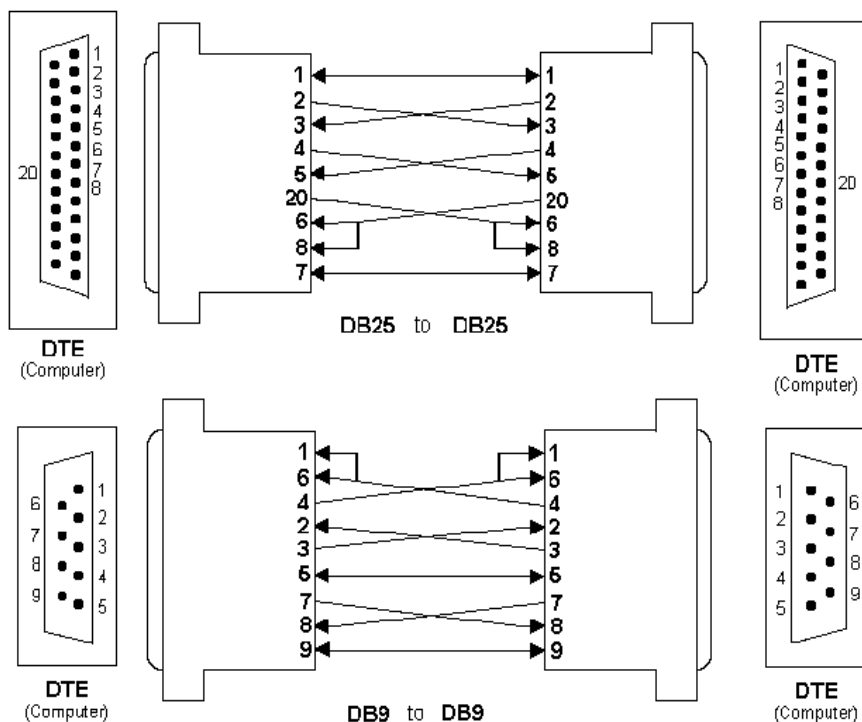
In addition, check to see whether your equipment uses a 9-pin connector or a 25-pin connector. Either is fine for use with pcANYWHERE, but you must match the ports on your computer and modem. Cables that match 9-pin and 25-pin connectors are commonly available.

CAUTION: Often you may find yourself with a 25-pin cable, but your computer has only a 9-pin port. Adapters are available for 25-to-9 pin and 9-to-25 pin and pass the correct signals. Make sure the adapter is designed for a modem. Mouse adapters may not pass all the correct signals.

Null Modem Cables

Direct connections use a special type of serial cable called a *null modem cable*. A null modem cable is sometimes called a *modem replacer* because it replaces the two modems that would normally be the link between computers. Because both sides of the cable connect directly to DTE (Data Terminal Equipment) ports, the null modem cable has female connectors on each end. The data send and receive lines are crossed, so that the data output signal line of one computer is connected to the data input signal line of the other. Some of the other signal lines are also crossed to enable data flow control. Null modem cables are readily available, but if you need to build your cable refer to Figure A-4 for pin assignments.

Figure A-4 Null modem pin configurations cross certain data and control lines.



Special Telephone Lines

This section explains how to use leased lines, special telephone lines that continually connect two sites, and multiplexers, hardware that allows multiple connections over a single telephone line.

Leased Lines

A leased line is a special service provided by the telephone company which allows for a continuous telephone line connection between two points. If normal telephones were connected to each end, a person at each of those ends could pick up the telephone and conduct a conversation with the other without dialing. Leased lines are similar to normal telephone lines in that modems are used to establish the connection. The difference is that leased lines do not have a dial tone, nor do they provide a “ring” signal to the answering modem. The most common usage of leased lines is between multiplexers. For more information on multiplexers, see “Multiplexers,” later in this appendix.

NOTE: It is important that the modems used with leased lines be leased-line compatible. Some modems on the market are not. If you are uncertain about your modem, refer to your modem’s manual or contact your modem manufacturer.

There are two methods to establish a connection over a leased line: one used with modems having an automatic leased-line mode and one used with modems that do not have an automatic leased-line mode.

Method #1: Modems with Automatic Leased Line Mode

If both modems are able to perform an automatic leased line connection (check the &L parameter in the modem’s documentation), then placing the modems in this mode causes them to go offhook as soon as they are turned on. Once offhook, they connect to each other independent of software control. Norton pcANYWHERE should be configured for a direct connection. You should review the modems’ documentation before attempting a leased line connection. Table A-3 describes the direct connect parameters.

Table A-3 Method #1 Hardware Configurations

	Host PC	Remote PC
Device:	(the port attached to the modem)	(the port attached to the modem)
Modem:	None	None
Data Rate:	(Same value as remote PC)	(Same value as host PC)
Parity:	None	None
Flow Control:	RTS/CTS	RTS/CTS
Connection Started By:	Receive 2 <CR>s	Always Connected
Connection Ended By:	Always Connected or DCD	Always Connected or DCD

Method #2: Modems without Automatic Leased Line Mode

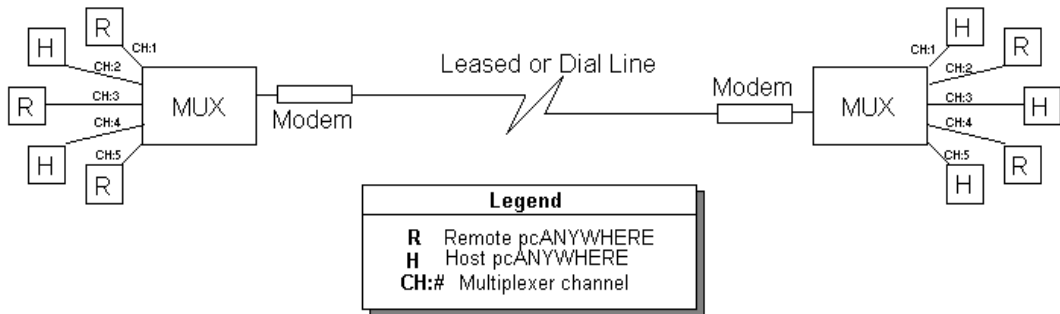
If the modems do not have the option of performing an automatic connection, then the modems remain onhook until pcANYWHERE is ready to make the connection. Configure pcANYWHERE as you normally would for use with your modem, but enable the Leased Line option in the hardware configuration. Once set, you are ready to begin a connection. Have the host PC wait for a call from the remote user. Since a “ring” signal cannot be generated, pcANYWHERE prompts you to press Enter on *both* sides to begin the connection. If a person cannot be present on each side to begin the connection, then you must use Method 1 (described above).

Testing Leased Lines

To make sure that your leased line is operating properly, replace the modems with normal telephones. Have a person on each end pick up the telephone and attempt a conversation. If both people can communicate, the modem connection should work correctly.

Multiplexers

A Multiplexer (MUX) allows multiple connections over a single telephone line. The telephone line can be a leased line or a dial-up line. Each device is connected to a channel on the MUX, which combines all the signals from each channel into a single composite signal. This signal is sent through a modem over the telephone line. A matching MUX on the receiving end de-multiplexes the signal and distributes each channel (Figure A-5).

Figure A-5 Multiplexers on a telephone line.

The modems, which can be internal to the MUX, operate in synchronous mode. Each channel behaves as if directly connected to the other device at the matched MUX, as shown above.

The MUX configuration must be operational to use Norton pcANYWHERE. Specifically, data must be flowing through the channel(s) to be used.

To determine if data can flow across the channel correctly, each PC user should perform these steps to conduct a remote-to-remote test.

To perform a remote-to-remote test:

- 1 Click Quick Connect in the Call A pcANYWHERE Host main window.
- 2 Click No Modem.
- 3 Set the data rate, if necessary.
- 4 Click CALL.
- 5 Type some characters.

If each user can see characters that are being typed at the other PC, the configurations are working.

The options in Table A-4 depend on the Multiplexer used.

Table A-4 Norton pcANYWHERE Configurations

	Remote PC	Host PC
Modem:	None	None
*Data rate:	(set to speed of MUX)	(set to speed of MUX)
*Parity:	None	None
*Flow control:	RTS/CTS	RTS/CTS
Conn. started by:	Carrier Detect (DCD)	Receive 2 CRs
Conn. ended by:	Carrier Detect (DCD)	Carrier Detect (DCD)

Error Detection and Correction

When line noise and other uncontrollable variables enter the data stream, transmission errors occur. The less-than-perfect conditions of real-world data transfer require special measures to keep the data flowing correctly.

Error detection and correction can be done by the modem, Norton pcANYWHERE, or both. Modern high-speed modems have their own built-in error detection and correction protocols, such as MNP and V.42, which are sufficient for most sessions. Norton pcANYWHERE supports a variety of parity checking schemes because some online services, such as CompuServe, require them. Error correction can be disabled if a compatibility issue occurs.

Parity checking is the simplest form of error detection. Interference on the line can sometimes alter the bits, causing an incorrect character to be transmitted. Parity-checking calculates the total number of ones in each byte (character) and appends a bit (called the parity bit) based on that value. *Even* parity checking adds a zero if the number of ones is even. If the number of ones is odd it adds a one. In this way the bytes are adjusted so that every byte should be received with an even number of ones. If an odd number is counted at the receiving end, it means an error has occurred. If the number is even, the appended parity bit is discarded and data transmission continues. CompuServe, for example, uses even parity. *Odd* parity checking works similarly, adjusting each byte to an odd number of ones. With *space* and *mark* parity, the parity bit, when sent, is always set to either 0 or 1, respectively. If a character is received with a parity bit set to a different value than expected, an error may have occurred during transmission. Space parity, also referred to as *bit trimming*, can be used to transmit 7-bit characters to a device that is expecting 8-bit characters. Mark parity can be referred to as *bit forcing*.

Table A-5 shows the number of data bits and stop bits for each type of parity checking used by Norton pcANYWHERE.

Table A-5 Parity Settings

pcANYWHERE Setting	Data Bits	Parity	Stop Bits
None	8	N	1
Even	7	E	1
Odd	7	O	1
Mark	7	M	1
Space	7	S	1

Serial Hardware Configurations

The port for the modem, the name of the modem (or a reasonable substitute), data rate, parity, and flow control are the first five options that you set when you create a hardware configuration for a modem. The connected computers must both use the same parity. For example, a remote control session always uses “None” as the parity setting. During a session, two modems communicate at the same rate, but your settings for data rate on each PC do not have to be the same. Most modems can determine the highest data rate available to both of them.

When your modem is not supported, see the following. Possible actions to take are listed in order of preference.

- Refer to your modem’s manual or ask your modem’s manufacturer which modem in the list has a similar command set and select that modem from the list. For example, many 2400-bps modems are compatible with the Hayes Smartmodem 2400 setting.
- Choose the default modem (Hayes compatible) and experiment with some of its settings.
- Choose Manual modem and type a string of commands after the Additional Modem Initialization String.
- Define a custom modem as explained in Chapter 3, “Hardware Configurations.”

If you have selected Manual modem as the Device/Port setting in a hardware configuration, you should enter an initialization string recommended by your modem manufacturer as the setting for the Additional Modem Initialization String option. If you have selected Custom modem, you need to check your modem’s manual to determine its setup. See “Using Modem Commands,” and “Setting Modem Switches,” later in this appendix.

When you select the name of a modem, Norton pcANYWHERE automatically sets the remaining modem options to default settings. For example, a modem that does compression must use hardware flow control, so Norton pcANYWHERE automatically sets Flow Control to RTS/CTS.

If you are using a direct connection, the maximum speed of data transfer is determined by the speed of your computer and the capabilities of your UART and serial port. Since both the host and remote configurations must use the same speed, both configurations must use the speed of the slowest system. You'll probably want to adjust the setting for data rate.

Flow control and parity must remain at their default settings for remote control sessions (RTS/CTS and none, respectively), but you may adjust them to meet an online service session's requirements. If you have difficulty connecting with online services, you may need to alter one or more of the other settings.

If you regularly access an online service for which you make setting changes, you may want to have an additional hardware configuration for when you call that service.

Miscellaneous Modem Hardware Configuration Options

There are other hardware configuration options for modems, which perform the following functions:

- Indicate the types of signal your system uses to detect a connection to or disconnection from another computer.

Connection Started By and Connection Ended By are explained in the Glossary.

- Provide dialing instructions.

Ring No. To Answer On, Dial Type, Redial Attempts, Seconds To Wait After Dial, and Seconds Between Redials are, for the most part, self-explanatory. You can find them in the Glossary as well.

- Allow you to control hardware settings for serial communications.

DTR State and RTS State refer to *Data Terminal Ready* (sent by a computer to the modem, indicating that the computer is available to accept incoming transmissions) and *Request To Send* (an RS-232-C signal used in hardware flow control to pace information sent from one device to another).

Norton pcANYWHERE automatically sets these options for your modem. Change them only when special equipment is in use. See the Glossary for information about their settings.

- Set the length of the break signal used in terminal emulations. A break signal usually interrupts a program running on a mainframe or minicomputer. (This is different from the Ctrl+C or Ctrl+Break used by PCs.)

For more information about what settings to choose for hardware configuration options related to your modem, refer to your modem's manual. Check the Glossary in this guide for definitions of other options not explained in this section.

Norton pcANYWHERE for Windows Command Lines

Command lines allow you to automatically run pcANYWHERE in a particular mode of operation. You could, for example, have pcANYWHERE automatically start in the remote mode and dial a phone number.

Command-line options are typed in Program Manager's FILE RUN... or FILE PROPERTIES... command line text boxes.

Included with Norton pcANYWHERE for Windows, version 2.0, is a host TSR program named AW_HOST.EXE. This is a TSR version of the host program that can be run from the DOS prompt using the pcANYWHERE command-line options.

The following examples are some situations in which you would use command-line options for the host TSR:

- To create batch files tailored for individual host users
- To start the host TSR
- To load or remove the gateway TSR

Command-Line Arguments

Command-line arguments consist of:

- A dash or hyphen (-)
- A command-line option (described below)
- An equal sign (=)
- A value (described below)

NOTE: pcANYWHERE for DOS, version 5.0, uses a slash (/) and a colon (:) as arguments instead of the hyphen (-) and equal sign (=). pcANYWHERE for Windows, version 2.0 can use either set of arguments. These pairs of arguments are not interchangeable. In a command line, you can use either / and : or - and =; you cannot, for example, use - with :.

Use a space to separate arguments and complete the command line with a carriage return (↵).

```
WINAW -o=h -m=w↵
```

Or,

```
WINAW /o:h /m:w↵
```

This example command line loads the pcANYWHERE host in Wait for a Call mode.

Command-Line Options

Each command-line option is indicated by a hyphen followed by a letter (for example, -I).

- -I The six-character ID used to identify network users

```
I=xxxxxx
```

- -O The type of operation

```
=r remote operation
```

```
=h host operation
```

- -M The mode of operation

The modes available for host operation (WINAW) are:

```
=w Wait for incoming call
```

```
=d Dial a phone number
```

The modes available for host TSR operation (AW-HOST) are:

```
=w Wait for incoming call
```

```
=d Dial a phone number
```

```
=a Allow incoming calls (automatically answers an incoming call)
```

```
=r Wait in resident mode (use hot-key to activate the host TSR when needed)
```


The modes available for remote operation are:

- =d Call a host
- =s Run a script
- -N Name of host, phone number to call, or name of script to execute.
- -C Hardware configuration to use as host

The syntax for the WINAW command line is as follows:

```
[-I=<user id>] [-O=r] [-M=d|s] [-N=host name|script]
```

```
[-I=<user id>] [-O=h] [-M=w|d] [-C=<configuration>] [-N=<phone #>]
```

The syntax for the host TSR command line is as follows:

```
AW_HOST [-M= w|d|a|r] [-C=<configuration>] [-N=<phone #>]
```

Command Line Examples

Type the following command-line options in the Command Line text box in the FILE RUN... or FILE PROPERTIES... dialog boxes. Precede the command-line options with WINAW.EXE, including the full path, as follows:

```
C:\WINAW\winaw.exe
```

- | | |
|-----------------------------|--|
| -O=h -M=w | Start a host operation in wait for a call mode. (The PC cannot be used while pcANYWHERE is waiting for a call in this mode.) |
| -O=h -M=a | Start a host operation to allow incoming calls. (The host is waiting in background and the PC can be used while pcANYWHERE is waiting for a call in this mode.) |
| -O=r -M=d -N="Host via IPX" | Start a remote operation and connect to the host named "Host via IPX." |
| -O=r -M=s -N=callbbs | Start a remote operation and run a script file named "callbbs." (If the script you want to run is not in your pcANYWHERE directory, include the full path to the script file.) |

Type the following host TSR command-line options at the DOS prompt:

AW_HOST -M=a -C=modem	Loads the host TSR in allow incoming calls mode using a hardware configuration named "modem."
AW_HOST -M=w	Loads the host TSR in wait for a call mode.
AW_HOST -M=d -N=345-6789	Loads the host TSR in dial mode and dials the number 345-6789.
AW_HOST -M=r	Loads the host TSR in resident mode. Use the host hotkey to activate host.

Windows Communication with OLE and Visual Basic

Object Linking and Embedding (OLE 2) Automation Support

Norton pcANYWHERE for Windows, version 2.0 acts as an OLE-Server, allowing OLE-Controller applications to access the following:

- **CmdLine**—This method requires a single parameter, which is a string that represents the command line to be executed. All valid pcANYWHERE command-line arguments can be used. When this method is used, pcANYWHERE starts and the specified command line executes (see "Norton pcANYWHERE for Windows Command Lines" in the previous section.)
- **CallHost**—Starts pcANYWHERE and executes a Call A Host operation. Two parameters are required:
 - operation: 0=dial, 1=wait for a call (byte)
 - directory-entry: a zero-terminated string containing the online service directory entry to use
- **CallOnlSvc**—Starts pcANYWHERE and executes a Call an Online Service operation. Two parameters are required:
 - operation: 0=dial, 1=wait for a call (byte)
 - directory-entry: a zero-terminated string containing the online service directory entry to use
- **BeAHost**—Starts pcANYWHERE and executes a Be A Host operation. Two parameters are required:
 - operation: 0=dial, 1=wait for a call (byte)
 - name: a zero-terminated string containing a phone number for a dial operation to use
- **Quit**—If pcANYWHERE is running, it terminates.

To configure pcANYWHERE for OLE Automation:

- Using a text editor, edit the LocalServer= statement in the WINAW.REG to include the full path and directory in which pcANYWHERE is installed.

This file is used by the REGEDIT program that comes with Windows to publish the existence of pcANYWHERE as an OLE-Server.

To run the REGEDIT program:

- 1 Choose RUN... from the File menu on the Program Manager's main window.
- 2 Type in the text box:

```
REGEDIT c:\winpath\WINAW.REG
```

Replace *winpath* with the directory in which pcANYWHERE is installed.

Using Visual Basic as an OLE Controller

Visual Basic provides the functionality that allows you to create a program that acts as an OLE controller. The following Visual Basic examples demonstrate each of the pcANYWHERE OLE Automation Methods.

CmdLine

This example starts pcANYWHERE, then executes a Call A Host operation using the dial directory named "A pcANYWHERE Host."

```
Dim winaw as OBJECT
Dim iStatus as INTEGER
Set winaw=CreateObject ("pcANYWHERE.Application")
iStatus=winaw.CmdLine("-o=r -m=d -n=A pcANYWHERE Host")
```

CallHost

This example starts pcANYWHERE, then executes a Call A Host operation using the dial directory named "A pcANYWHERE Host."

```
Dim winaw as OBJECT
Dim iStatus as INTEGER
Set winaw=CreateObject ("pcANYWHERE Application")
iStatus=winaw.CallHost(0,"A pcANYWHERE Host")
```

CallOnISvc

This example starts pcANYWHERE, then executes a Call An Online Service operation using the "CompuServe" Online Service Directory entry.

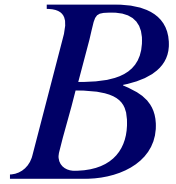
```
Dim winaw as OBJECT
Dim iStatus as INTEGER
Set winaw=CreateObject ("pcANYWHERE Application")
iStatus=winaw.CallHost(0, "CompuServe")
```

BeAHost

This example starts pcANYWHERE, then executes a Be A Host operation. pcANYWHERE waits for a call.

```
Dim winaw as OBJECT
Dim iStatus as INTEGER
Set winaw=CreateObject ("pcANYWHERE Application")
iStatus=winaw.BeAHost(1)
```

Terminal Emulation



This appendix contains reference information about the terminal emulations used during online sessions. It provides:

- PC keyboard mappings for terminal emulation. This is for users who need to use a PC keyboard to emulate a terminal.
- Translation table code reference. This is for advanced users who need to create custom terminal configurations.

Terminal Emulation Keys

Norton pcANYWHERE emulates a wide variety of popular terminals. Using a terminal emulation, your PC keyboard can imitate a selected terminal. Because terminal keyboard configurations often differ from the standard PC keyboard, it is necessary to map some of the terminal keys to designated PC keys.

Most of the keys you use are unchanged. Only keys that are unique to a specific type of terminal are remapped. To determine the location of the remapped terminal keys simply locate your terminal type in the charts that follow and note the PC keys that are used to emulate them.

NOTE: Some terminals operate in two distinct modes: character and block. Norton pcANYWHERE supports character mode only.

ADDS Viewpoint

PC KEY	ADDS KEY
F1	F1
F2	F2
F3	F3
Home	Home Cursor
Up	Up
Left	Left
Right	Right
Down	Down
Shift+F1	Shift+F1
Shift+F2	Shift+F2
Shift+F3	Shift+F3
Gray-Home	Home Cursor
Gray-Up	Up
Gray-Left	Left
Gray-Right	Right
Gray-Down	Down

ADM 3A

PC KEY	ADM3A KEY
Home	Home Cursor
Up	Up
Left	Left
Right	Right
Down	Down

ADM 3A *(continued)*

Gray-Home	Home Cursor
Gray-Up	Up
Gray-Left	Left
Gray-Right	Right
Gray-Down	Down

ANSI

PC KEY	ANSI
F1	PF1
F2	PF2
F3	PF3
F4	PF4
Up	Up
Left	Left
Right	Right
Down	Down
Gray-Up	Up
Gray-Left	Left
Gray-Right	Right
Gray-Down	Down

DG 100/200

PC KEY	DG KEY
Backspace	New Line
Alt+Q	Ctrl+F13
Alt+W	Ctrl+F14
Alt+E	Ctrl+F15
Alt+A	Ctrl+Shift+F13
Alt+S	Ctrl+Shift+F14
Alt+D	Ctrl+Shift+F15
F1	F1
F2	F2
F3	F3
F4	F4
F5	F5
F6	F6
F7	F7
F8	F8
F9	F9
F10	F10
Home	Home Cursor
Up	Up
Left	Left
Right	Right
Down	Down
Del	Char Del
Shift+F1	Shift+F1

DG 100/200 *(continued)*

Shift+F2	Shift+F2
Shift+F3	Shift+F3
Shift+F4	Shift+F4
Shift+F5	Shift+F5
Shift+F6	Shift+F6
Shift+F7	Shift+F7
Shift+F8	Shift+F8
Shift+F9	Shift+F9
Shift+F10	Shift+F10
Ctrl+F1	Ctrl+F1
Ctrl+F2	Ctrl+F2
Ctrl+F3	Ctrl+F3
Ctrl+F4	Ctrl+F4
Ctrl+F5	Ctrl+F5
Ctrl+F6	Ctrl+F6
Ctrl+F7	Ctrl+F7
Ctrl+F8	Ctrl+F8
Ctrl+F9	Ctrl+F9
Ctrl+F10	Ctrl+F10
Alt+F1	Ctrl+Shift+F1
Alt+F2	Ctrl+Shift+F2
Alt+F3	Ctrl+Shift+F3
Alt+F4	Ctrl+Shift+F4
Alt+F5	Ctrl+Shift+F5
Alt+F6	Ctrl+Shift+F6

DG 100/200 *(continued)*

Alt+F7	Ctrl+Shift+F7
Alt+F8	Ctrl+Shift+F8
Alt+F9	Ctrl+Shift+F9
Alt+F10	Ctrl+Shift+F10
Alt+3	F13
Alt+4	F14
Alt+5	F15
Alt+8	Shift+F13
Alt+9	Shift+F14
Alt+0	Shift+F15
F11	F11
F12	F12
Shift+F11	Shift+F11
Shift+F12	Shift+F12
Ctrl+F11	Ctrl+F11
Ctrl+F12	Ctrl+F12
Alt+F11	Ctrl+Shift+F11
Alt+F12	Ctrl+Shift+F12
Ctrl+Backspace	127
Gray-Home	Home Cursor
Gray-Up	Up
Gray-Left	Left
Gray-Right	Right
Gray-Down	Down
Gray-Del	Char Del

Hazeltine 1500

PC KEY

Home

Up

Left

Right

Down

Gray-Home

Gray-Up

Gray-Left

Gray-Right

Gray-Down

HAZ KEY

Home Cursor

Up

Left

Right

Down

Home Cursor

Up

Left

Right

Down

IBM 3101

PC KEY

F1

F2

F3

F4

F5

F6

F7

F8

Home

Up

Left

IBM 3101 KEY

F1

F2

F3

F4

F5

F6

F7

F8

Home Cursor

Up

Left

IBM 3101 *(continued)*

Right	Right
Down	Down
Del	Del
Ctrl+End	Clr EOP
Ctrl+PgDn	Clear
Backspace	Backspace
Ctrl+Backspace	Del or Backspace
Gray-Home	Home Cursor
Gray-Up	Up
Gray-Left	Left
Gray-Right	Right
Gray-Down	Down
Gray-Del	Del
Gray-Ctrl+End	Clr EOP
Gray-Ctrl+PgDn	Clear

Televideo 912/920

PC KEY	TVI912/920 KEY
Alt+F n	Funct+n
F1	F1
F2	F2
F3	F3
F4	F4
F5	F5
F6	F6

Teletype 912/920 *(continued)*

F7	F7
F8	F8
F9	F9
F10	F10
Home	Home Cursor
Up	Up
Left	Left
Right	Right
End	Line Del
Down	Down
Ins	Char Ins
Del	Char Del
Shift+F1	Shift+F1
Shift+F2	Shift+F2
Shift+F3	Shift+F3
Shift+F4	Shift+F4
Shift+F5	Shift+F5
Shift+F6	Shift+F6
Shift+F7	Shift+F7
Shift+F8	Shift+F8
Shift+F9	Shift+F9
Shift+F10	Shift+F10
Ctrl+End	Page Erase
Ctrl+PgDn	Clear Screen
Ctrl+Home	Line Ins

Teletype 912/920 *(continued)*

Alt+1	F11
Alt+2	Shift+F11
Gray-Home	Home Cursor
Gray-Up	Up
Gray-Left	Left
Gray-Right	Right
Gray-End	Line Del
Gray-Down	Down
Gray-Ins	Char Ins
Gray-Del	Char Del
Gray-Ctrl+End	Page Erase
Gray-Ctrl+PgDn	Clear Screen
Gray-Ctrl+Home	Line Ins

Teletype 925

PC KEY	TVI925 KEY
Alt+F n	Funct+n
F1	F1
F2	F2
F3	F3
F4	F4
F5	F5
F6	F6
F7	F7
F8	F8

Teletype 925 *(continued)*

F9	F9
F10	F10
Home	Home Cursor
Up	Up
Left	Left
Right	Right
End	Line Del
Down	Down
Ins	Char Ins
Del	Char Del
Shift+F1	Shift+F1
Shift+F2	Shift+F2
Shift+F3	Shift+F3
Shift+F4	Shift+F4
Shift+F5	Shift+F5
Shift+F6	Shift+F6
Shift+F7	Shift+F7
Shift+F8	Shift+F8
Shift+F9	Shift+F9
Shift+F10	Shift+F10
Ctrl+End	Page Erase
Ctrl+PgDn	Clear Screen
Ctrl+Home	Line Ins
Alt+1	F11
Alt+2	Shift+F11

Teletype 925 *(continued)*

Backspace	Backspace
Ctrl+Backspace	Del or Backspace
Gray-Home	Home Cursor
Gray-Up	Up
Gray-Left	Left
Gray-Right	Right
Gray-End	Line Del
Gray-Down	Down
Gray-Ins	Char Ins
Gray-Del	Char Del
Gray-Ctrl+End	Page Erase
Gray-Ctrl+PgDn	Clear Screen
Gray-Ctrl+Home	Line Ins

VT 100/102/220

PC KEY	VT100/220 KEY
F1	PF1
F2	PF2
F3	PF3
F4	PF4
F6	F6
F7	F7
F8	F8
F9	F9
F10	F10

VT 100/102/220 *(continued)*

Home	Find
Up	Up
Left	Left
Right	Right
End	Select
Down	Down
Ins	Insert Here
Del	Remove
Shift+F1	F11
Shift+F2	F12
Shift+F3	F13
Shift+F4	F14
Shift+F5	F15 (Help)
Shift+F6	F16 (Do)
Shift+F7	F17
Shift+F8	F18
Shift+F9	F19
Shift+F10	F20
Ctrl+PgDn	Next Screen
Alt+1	PF1
Alt+2	PF2
Alt+3	PF3
Alt+4	PF4
Ctrl+PgUp	Previous Screen
F11	F11

VT 100/102/220 *(continued)*

F12	F12
Del	Backspace or Del
CR	CR or CR LF
Pad *	Numeric Pad ,
Pad -	Numeric Pad -
Pad .	Numeric Pad .
Pad 0	Numeric Pad 0
Pad 1	Numeric Pad 1
Pad 2	Numeric Pad 2
Pad 3	Numeric Pad 3
Pad 4	Numeric Pad 4
Pad 5	Numeric Pad 5
Pad 6	Numeric Pad 6
Pad 7	Numeric Pad 7
Pad 8	Numeric Pad 8
Pad 9	Numeric Pad 9
Ctrl+Backspace	Del or Backspace
Gray-Home	Find
Gray-Up	Up
Gray-Left	Left
Gray-Right	Right
Gray-End	Select
Gray-Down	Down
Pad <-'	Pad <-'

VT 52

PC KEY	VT52KEY
F1	PF1
F2	PF2
F3	PF3
F4	PF4
Up	Up
Down	Down
Right	Right
Left	Left
Shift+F1	F11
Shift+F2	F12
Shift+F3	F13
Alt+1	PF1
Alt+2	PF2
Alt+3	PF3
Alt+4	PF4
Backspace	Backspace
Enter	Enter
Pad <-'	Pad <-'
Ctrl+Backspace	Del or Backspace
Pad *	Pad ,
Pad -	Pad -
Pad .	Pad .
Pad 0	Pad 0
Pad 1	Pad 1

VT 52 *(continued)*

Pad 2	Pad 2
Pad 3	Pad 3
Pad 4	Pad 4
Pad 5	Pad 5
Pad 6	Pad 6
Pad 7	Pad 7
Pad 8	Pad 8
Pad 9	Pad 9
Gray-Up	Up
Gray-Down	Down
Gray-Right	Right
Gray-Left	Left

Wyse 50

PC KEY	WYSE50 KEY
Tab	Horizontal Tab
Backspace	Backspace
Ctrl+Backspace	Char Del
Backtab	Reverse Tab
Alt+F n	Funct+n
F1	F1
F2	F2
F3	F3
F4	F4
F5	F5

Wyse 50 *(continued)*

F6	F6
F7	F7
F8	F8
F9	F9
F10	F10
Home	Home Cursor
Up	Up
Left	Left
Right	Right
End	Line Erase
Down	Down
Insert	Insert Char
Delete	Delete Char
F11	F11
F12	F12
Shift+F3	F13
Shift+F4	F14
Shift+F5	F15M
F16(Shift+F6)	F16
Ctrl+F1	Sh Line Erase
Ctrl+F2	Sh Pg Erase
Ctrl+F3	Sh Line Ins
Ctrl+F4	Sh Line Del
Ctrl+F5	Sh Char Ins
Ctrl+F6	Sh Char Del

Wyse 50 *(continued)*

Ctrl+End	Page Erase
Ctrl+PgDn	Clear Screen
Ctrl+Home	Insert Line
Ctrl+PgUp	Delete Line
F11	F11
F12	F12
Backspace	Backspace
Ctrl+Backspace	127
Gray-Home	Home Cursor
Gray-Up	Up
Gray-Left	Left
Gray-Right	Right
Gray-End	Line Erase
Gray-Down	Down
Gray-Insert	Insert Char
Gray-Delete	Delete Char
Gray-Ctrl+End	Page Erase
Gray-Ctrl+PgDn	Clear Screen
Gray-Ctrl+Home	Insert Line
Gray-Ctrl+PgUp	Delete Line

X3270

PC KEY	3270 Key
Backtab	Field Backtab
F1	PF1
F2	PF2
F3	PF3
F4	PF4
F5	PF5
F6	PF6
F7	PF7
F8	PF8
F9	PF9
F10	PF10
Home	Home
Up	Up
Left	Left
Right	Right
End	Erase Input
Down	Down
Insert	Toggle Insert
Delete	Delete
Shift+F1	PF11
Shift+F2	PF12
Shift+F3	PF13
Shift+F4	PF14
Shift+F5	PF15

X3270 *(continued)*

Shift+F6	PF16
Shift+F7	PF17
Shift+F8	PF18
Shift+F9	PF19
Shift+F10	PF20
Ctrl+F1	PF21
Ctrl+F2	PF22
Ctrl+F3	PF23
Ctrl+F4	PF24
Ctrl+F9	Column Tab
Ctrl+F10	Column Backtab
Ctrl+End	Erase EOF
Ctrl+PgDn	Undo indent
Ctrl+Home	Clear
Alt+1	PA1
Alt+2	PA2
Alt+3	PA3
Ctrl+PgUp	Indent
F11	PF11
F12	PF12
Shift+F11	PF21
Shift+F12	PF22
Tab	Field Tab
Pad <-'	Clear
Pad *	PF23

X3270 *(continued)*

Pad +	Clear
Pad -	PF12
Gray-Home	Home
Gray-Up	Up
Gray-Left	Left
Gray-Right	Right
Gray-End	Erase input
Gray-Down	Down
Gray-Del	Del
Gray-Ctrl+End	Erase EOF
Gray-Ctrl+PgDn	Undo indent
Gray-Ctrl+Home	Clear
Gray-Ctrl+PgUp	Indent

Translation Table Codes

Occasionally a mainframe, minicomputer, or other multi-user system may require you to customize the selected terminal emulation for maximum compatibility. Using a translation table, you modify the binary codes that are sent and received during the session. These binary codes are represented in the translation table as hexadecimal (HEX) codes. For more information see Chapter 7, "Online Services." You may need to refer to the following information on the ASCII and OEM character sets as you create a translation table.

The ASCII Character Set

The ASCII standard is the most commonly used language for data communication. ASCII is an acronym for American Standard Code for Information Interchange. Despite the national reference, this code has become an international standard. The binary codes for the ASCII characters range in value from 0 to 127.

Values 0 to 31 are assigned as control codes, such as backspace and carriage return, and are generally nonprinting characters. See Table B-1. These nonprinting characters were designed to control various communications, display, and printer functions. In some fonts, these characters represent graphical symbols (see Table B-2).

Table B-1 ASCII Control Character Set

Character	Dec	Hex	Character	Dec	Hex
^@ NUL	0	00	^P DLE	16	10
^A SOH	1	01	^Q DC1	17	11
^B STX	2	02	^R DC2	18	12
^C ETX	3	03	^S DC3	19	13
^D EOT	4	04	^T CD4	20	14
^E ENQ	5	05	^U NAK	21	15
^F ACK	6	06	^V SYN	22	16
^G BEL	7	07	^W ETB	23	17
^H Backspace	8	08	^X CAN	24	18
^I HI	9	09	^Y EM	25	19
^J LF	10	0A	^Z SUB	26	1A
^K VT	11	0B	^[ESC	27	1B
^L FF	12	0C	^\ FS	28	1C
^M CR	13	0D	^] GS	29	1D
^N SO	14	0E	^^ RS	30	1E
^O SI	15	0F	^_ US	31	1F

The values from 32 to 127 represent the numbers 0 to 9, common punctuation marks, and the upper- and lowercase letters of the alphabet you find on your PC keyboard. These characters are invoked by pressing one of the standard keys. These characters are shown in Table B-2.

The values from 128 to 255 are not part of the standard and are assigned different sets of characters by computer manufacturers and software

developers. Most DOS programs use a set of eight-bit characters developed by IBM and Microsoft for creating graphic representations while in text mode and for other special functions (see Table B-2). They are sometimes referred to as the extended ASCII character set. Microsoft refers to them as the OEM character set.

Table B-2 OEM Character Set

0		32		64	@	96	`	128	Ç	160	á	192	Ł	224	α
1	⊕	33	!	65	A	97	a	129	ü	161	í	193	ł	225	β
2	⊗	34	"	66	B	98	b	130	é	162	ó	194	Ł	226	Γ
3	♥	35	#	67	C	99	c	131	â	163	ú	195	ł	227	Π
4	♦	36	\$	68	D	100	d	132	ä	164	ñ	196	—	228	Σ
5	♣	37	%	69	E	101	e	133	à	165	Ñ	197	†	229	σ
6	♠	38	&	70	F	102	f	134	å	166	º	198	‡	230	μ
7	•	39	'	71	G	103	g	135	ç	167	¸	199	‡	231	τ
8	◻	40	(72	H	104	h	136	ê	168	¸	200	Ł	232	θ
9	◻	41)	73	I	105	i	137	ë	169	¸	201	Ł	233	Θ
10	◻	42	*	74	J	106	j	138	è	170	¸	202	Ł	234	Ω
11	◻	43	+	75	K	107	k	139	ï	171	½	203	Ł	235	δ
12	♀	44	,	76	L	108	l	140	î	172	¾	204	Ł	236	ω
13	♯	45	-	77	M	109	m	141	ì	173	¸	205	=	237	ø
14	♯	46	.	78	N	110	n	142	ñ	174	«	206	Ł	238	€
15	✱	47	/	79	O	111	o	143	ř	175	»	207	Ł	239	Ń
16	▶	48	0	80	P	112	p	144	é	176	▩	208	Ł	240	≡
17	◀	49	1	81	Q	113	q	145	æ	177	▩	209	Ł	241	±
18	‡	50	2	82	R	114	r	146	ŕ	178	▩	210	Ł	242	≥
19	‡	51	3	83	S	115	s	147	ô	179		211	Ł	243	≤
20	♯	52	4	84	T	116	t	148	ö	180	†	212	Ł	244	ƒ
21	♯	53	5	85	U	117	u	149	ò	181	‡	213	F	245	J
22	—	54	6	86	V	118	v	150	û	182	‡	214	Ł	246	÷
23	±	55	7	87	W	119	w	151	ù	183	Ł	215	‡	247	≈
24	↑	56	8	88	X	120	x	152	ÿ	184	‡	216	‡	248	o
25	↓	57	9	89	Y	121	y	153	õ	185	‡	217	Ł	249	·
26	→	58	:	90	Z	122	z	154	Ü	186	‡	218	Ł	250	·
27	←	59	;	91	[123	{	155	ç	187	‡	219	▩	251	√
28	└	60	<	92	\	124		156	£	188	‡	220	▩	252	n
29	┘	61	=	93]	125	}	157	¥	189	Ł	221	▩	253	z
30	▲	62	>	94	^	126	~	158	℞	190	‡	222	▩	254	■
31	▼	63	?	95	_	127	Δ	159	f	191	‡	223	▩	255	

Converting Decimal Numbers to Hex

To convert a number from decimal to hex, divide the decimal number by 16. The integer of the quotient becomes the first digit of the hex number, and the remainder becomes the second digit. Use Table B-3 to convert both the integer quotient and the remainder from a decimal number to a two-digit hex number.

For example, 128 divided by 16 is 8 remainder 0, so the hex equivalent for the decimal number 128 is 80. Similarly, 191 divided by 16 is 11 remainder 15, so the hex equivalent for the decimal number 191 is BF.

Table B-3 Decimal and Hex

Decimal	Hex
0	0
1	1
2	2
3	3
4	4
5	5
6	6
7	7
8	8
9	9
10	A
11	B
12	C
13	D
14	E
15	F

Troubleshooting



This appendix can help you troubleshoot your remote control sessions. It covers:

- Error messages and their explanations
- Common problems and their possible solutions

Interpreting Error Messages

Many of the pcANYWHERE error messages that may appear to alert you to a problem or condition are self-explanatory. Table C-1 lists alphabetically some of the messages. Each listed message is followed by one or more solutions or explanations. Italics are used to indicate words or values that may vary according to the names and settings in your copy of Norton pcANYWHERE for Windows.

NOTE: Please check the README.TXT file for any additions or corrections to the messages.

Table C-1 Common Error Messages

The caller file could not be found, logging off...

The host's caller privileges files—*AW.CI6* or *AWuserid.CI6*—could not be found, so the host PC cannot accept connects. These files must be located in the directory that was specified during installation.

The caller file is invalid, logging off...

The caller privileges file is most likely physically damaged. The filename is *AW.CI6* or *AWuserid.CI6*. The host user may have to reenter the caller information.

Cannot identify the parameter to change

Norton pcANYWHERE is unable to change the requested parameters. The requested parameters cannot be changed while the program is running. Exit Windows and reboot the PC.

Table C-1 Common Error Messages (*continued*)

Connection has been lost	For an unknown reason, a physical break in the connection occurred. This can be caused by a number of things: telephone line failure, hanging up the telephone, a call-waiting signal on the line, or some other interruption.
Could not adjust to the connect speed	The modems are not synchronizing their speeds. Set both modems to the data rate of the slower modem. See the explanation for “No response from the modem” for additional information.
Could not find hardware configuration file	See the explanation for “Unable to access data file.”
Could not find the requested host	The remote attempts to connect with the specified host. If the Host PC Computer Name has been entered incorrectly in the Edit Host PC Entry dialog box, or if the selected host is already in use, this message appears. Clear the Host PC Computer Name field, and try connecting again. When the Host PC Computer Name field is left blank, a list of available hosts appears.
Could not perform a partial attach to get status information	Your network driver version may not be recent enough to support pcANYWHERE connections. Novell NetWare users should use rev. 3.10 or higher.
Did not receive the expected response from the modem	Your modem did not understand the initialization string. See “My modem isn’t on pcANYWHERE’s list...” in the “Solving Problems” section at the end of this appendix.
Disk create error	pcANYWHERE was unable to create the file or directory. Your disk may be full, or you may be attempting to write to a network drive for which you do not have write access.
Disk or directory full	Your disk may be full, or you may be attempting to write to a network drive for which you do not have write access.

Table C-1 Common Error Messages (*continued*)

Disk read error	The source disk has some problem that prevents the file from being sent. Run Norton Disk Doctor or the DOS CHKDSK /F utility on the troubled disk.
Disk write error	The destination disk has some problem that is preventing the file from being sent. Run Norton Disk Doctor (or the DOS CHKDSK /F utility) on the troubled disk. Your disk may be full, or you may be attempting to write to a network drive for which you do not have write access.
DOS is busy. Exit menu, try again later.	See the explanation for “DOS is currently busy on the host PC,” next.
DOS is currently busy on the host PC	This error may occur when a remote user tries to connect to a waiting host. Certain DOS operations (such as writing to a disk) keep the host program from reading the disk.
End of file	An end-of-file character was received. pcANYWHERE may have received a character that it interpreted as an end-of-file character (^Z).
An error has occurred trying to determine which video driver to load.	Switch to a standard resolution such as 640x480, 1024x768, or 800x600, and 256 color. Double-click the Windows Setup icon in Program Manager’s Main program group. Choose CHANGE SYSTEM SETTINGS... from the Options menu and adjust the Display settings as desired.
Error on command line	The command line specified was incorrect. Please review the command line options in Appendix A.
Error opening file	The specified file cannot be opened for copying. You may have misspelled the filename. If the file is on a network drive, the file may be in use on another station.

Table C-1 Common Error Messages (*continued*)

Error processing the modem script	Some portion of a Norton pcANYWHERE modem script that you have created is causing an error. Try to isolate the error by splitting the script in half and processing each half. Then split the half that is causing the error and so on. Check the script for misspelled words or other errors. See the manual <i>Creating Norton pcANYWHERE Scripts</i> .
Error reading hardware configuration file	See the explanation for “Unable to access data file.”
File already exists	You have specified the name of an existing file. Use a different filename or path.
Inactivity timeout expired	The session has ended because the amount of time specified for an inactivity timeout has elapsed with no activity occurring during the connection.
Invalid connection parameters	One of the settings required for a connection is invalid. See the explanation for “No response from the modem,” later in this section or “pcANYWHERE thinks there is a connection...” in the “Solving Problems” section later in this appendix.
Invalid drive	The drive you specified is not available. You may have specified a network drive for which you do not have write access.
Invalid path specified	The path specified does not exist or cannot be created. You cannot create more than one subdirectory at a time, or you may have specified a network drive for which you do not have write access.

Table C-1 Common Error Messages (*continued*)

Log in unsuccessful	<p>If you are the host user, a remote PC tried unsuccessfully to connect with your host PC. The most likely problem was an incorrect password.</p> <p>If you are the remote user, you have entered an incorrect password. Another password attempt is not allowed by the host.</p> <p>The password set for this host in the Host PC Entry dialog box may be incorrect. Check with the host user or network administrator to determine the correct password.</p>
No carrier	<p>This message appears in the Modem Initializing... dialog box and indicates that the modem did not receive a data tone from the host's modem.</p>
No connection	<p>Norton pcANYWHERE could not make the connection. Perhaps the modem is malfunctioning or the PCs are not cabled properly. See Appendix A, "Technical Information," for information on modems and cabling.</p>
No response from the modem	<p>Your modem does not respond to Norton pcANYWHERE. The reason may be one of the following:</p> <ul style="list-style-type: none"> ■ The serial port you have designated in the hardware configuration is not working. ■ The modem is not turned on. ■ The modem is not cabled properly. ■ The serial port you specified in the hardware configuration is not the one your modem is connected to. ■ The serial board or internal modem is not correctly configured for Norton pcANYWHERE's use. <p>Appendix A, "Technical Information," contains information on modems and cabling. For other problems, see your modem or system manual, or contact your system administrator.</p>

Table C-1 Common Error Messages (*continued*)

No 2nd connection (via gateway.)	See the explanation for “No connection,” earlier in this section.
Not enough file handlers	See the explanation for “Too many opened files.”
Only the previous user’s password will be accepted	You cannot access this host PC until you enter the previous user’s password, or the host’s master password. The previous session ended abnormally and the host configuration does not allow any password on reconnect. See Chapter 5, “Configuring Norton pcANYWHERE,” for details.
Operator abort	A character may have been received that pcANYWHERE interpreted as an escape. When the escape key is pressed, the file transfer is aborted.
Other side canceled	See “Operator abort,” above.
An out of memory error has occurred. Please close some applications and try this operation again.	A function you have requested, such as a file transfer, cannot be executed because there is not enough available memory. Make sure you are not running software that is taking up random-access memory (RAM) needed by Norton pcANYWHERE.
pcANYWHERE does not support the video driver that is currently loaded.	See the explanation for “An error has occurred trying to determine which video driver to load.”
Port not available	The port selected in the hardware configuration is not correct. See Chapter 3, “Hardware Configurations,” for more information.
The remote access driver <i>filename</i> could not be loaded	Check the pcANYWHERE directory for the driver in question. If the file is not there, reinstall pcANYWHERE.
The requested communications device is already in use	This indicates that another communications program is using the COM port of the modem, or the COM port is signaling that the modem is offhook.

Table C-1 Common Error Messages (*continued*)

Time allowed on-line expired	The session ended because the host user has specified a limit on the amount of time you can spend in a session.
Time Out	One side of the remote control session was not responding, so the file transfer could not be performed. There is a problem on the other PC.
Too many opened files	The current operation attempted to open a file at a time when DOS or your network shell does not permit any more files to be opened. Try increasing the number of files in the FILES= line of your CONFIG.SYS file, or ask your network administrator to check your network shell setup to ensure that you can open more files.
Too many retries	pcANYWHERE kept trying to send blocks of data but they were not received. A data packet may be bad.
Unable to access data file	Check whether the file is already in use or does not exist. Also check your network access rights to the file.
Unable to attach to the other system	<p>If you are using a modem or direct cable connection, see the explanation for the error message: "No response from the modem."</p> <p>If you are using a network connection, your network driver version may not be recent enough. Check with your network administrator.</p>
Unable to create configuration files	Norton pcANYWHERE needs read/write access to the drive where it creates configuration files. If you are installing on a network drive, be sure you are logged in as network supervisor or other login with the necessary read/write access.
Unable to establish connection	This message can occur for a variety of reasons, but is usually caused by a physical problem. The telephone line or cable may be disconnected.

Table C-1 Common Error Messages (*continued*)

Unable to open the requested channel	See the explanation for “No connection.”
Unable to read installation data	Try reinstalling first. If any files are missing from your installation of Norton pcANYWHERE, the installation program will tell you.
Unable to release allocated memory	You attempted to remove pcANYWHERE from memory, but other programs used by this host PC may have utilized memory in a way that prevents Norton pcANYWHERE from being removed. Remove other more recently loaded programs from memory then try again.
Unable to release system resources	You attempted to remove Norton pcANYWHERE from memory, but other TSRs have been loaded into memory (RAM) after pcANYWHERE. Remove the most recently loaded programs then try again.
Your PC or terminal is not compatible with the host PC...	Terminal emulation must match on both sides of the connection. A standard communications program or terminal cannot connect with a Norton pcANYWHERE for Windows host. If you are using a Norton pcANYWHERE remote, something is causing the host to believe a different communications program is calling. Check the configuration on the remote.

Solving Problems

This section lists some common remote computing problems and possible solution for them.

Incorrect cabling and modem switch settings also are common problems. If you are using a serial configuration, be sure to review Appendix A, "Technical Information."

Serial Communications

Incorrect modem settings and conflicts with hardware interrupt requests (IRQs) cause a number of serial communications problems. COM1 and COM3 share the same interrupts, and COM2 and COM4 share the same interrupts. So, you cannot have, for example, a computer with a mouse on COM3 and a modem on COM1, as this arrangement would cause a device conflict.

Q I can't seem to transfer files with my IBM-compatible computer.

A Some IBM compatibles, especially Leading Edge Models D and M, may not be able to transfer files unless you use a cable that supports auxiliary RS-232 signals, carried on pins 4, 5, 6, 8, and 20.

Q I get a "No response from modem" message.

A There may be a piece of hardware, such as a network card or tape backup card, that conflicts with the IRQ number used by Norton pcANYWHERE for your serial port. You can solve this problem by checking your modem's manual to find out which IRQ number and port address it uses. You may be able to set up a Custom Port. See Chapter 3, "Hardware Configurations." If this doesn't work, check the manuals for your other hardware, and make sure the modem isn't conflicting with something. You may have to make some changes to the ports used by your system components. Check with your network administrator or dealer. Also refer to the previous section, "Interpreting Error Messages," for details.

Q I am accessing a host using a modem. My modem dials the host, but I can't make a connection.

A If you use a modem to reach a host (or if the host calls you) and nothing happens after dialing, you should check the Seconds To Wait After Dial option in the answering PC's hardware configuration. The default setting of 60 seconds may have to be increased or decreased. Some telephone systems may require from 45 to 120 seconds after dialing to complete the connection.

Q When I call the host PC I get connected, but the connection quickly ends and I see three plus signs (+++) at the top of my screen.

A This usually indicates a hardware or software conflict of some kind. First check that the modem does not share the IRQ with another device on the PC. If you use an external modem, check that you use an RS-232 cable. See Appendix A, "Technical Information," for cable information.

Q The modems "screech" at each other, but never make a connection.

A Usually this is a hardware problem. First check for an IRQ conflict. If there is no IRQ conflict, the problem is caused by the modem. Contact your modem's manufacturer for assistance.

Q What versions of IPX and NETx do I need to work with pcANYWHERE for Windows on a Network?

A pcANYWHERE requires NetWare IPX, version 3.10 or greater, or NETx, version 3.26 or greater.

Q When I connect to the host PC, the menu bar is garbled.

A Choose REMOTE OPERATION... from the Configure menu and uncheck the Use Local Fonts check box. Checking this option improves the display speed by using fonts available on the remote. If the menu is garbled, you need to uncheck this option so the host can send its font information to the remote.

Q When I connect to the host PC all the icons are black.

A Check that you have the latest video drivers for the host computer's video card and that you are running a supported video mode. The maximum supported by pcANYWHERE is 1024x768 with 256 colors.

Q My modem isn't on pcANYWHERE's list, and it won't initialize.

A If your modem is supposed to be Hayes-compatible, use the Hayes modem setting that most closely matches the data rate of your modem. If that doesn't work, try the Hayes Compatible modem setting. Check your modem's manual and use the Additional Modem Initialization String option in the hardware configuration to add any commands needed. You can also try using a Custom Modem setup. See "Customizing the Command Set for your Modem" in Chapter 3, "Hardware Configurations," for additional information.

If Norton pcANYWHERE issues the message "The modem is not responding" or another message indicating that it can't start your modem, in the Additional Modem Initialization String you can include commands for carrier-detect (DCD) to follow a normal carrier, DTR on, and a Ring Number to Answer On.

- Q My modem isn't on pcANYWHERE's list and I get strange characters when I try to start a session.**
- A See the item above.
- Q pcANYWHERE thinks there is a connection when there is none.**
- A The factory setting on your modem for carrier detect (DCD) may be On (or true). Change it to Off (false), so that the carrier detect signal goes on only when there is a call. (The modem command to toggle the carrier detect signal is AT&C1.) Alternatively, your cable may be incorrectly wired, forcing pin 8 on the PC's side to be connected to a signal that is always active.
- Q Sometimes there is a break in the connection when I try to access the DOS applications on the host PC.**
- A Check the software on the host PC. If the application expects to find the mouse or a printer on the same port that the host uses for the remote control session, you may have to reinstall the application or change its settings.
- Q The host PC sometimes drops the connection during a session.**
- A Make sure the telephone line used by the host modem does not have call waiting. When another call comes in on that line, you may lose your connection.
- Q When the host user calls the remote PC, there's no response.**
- A If there is a problem when the host user calls the remote PC, it may be caused by a setting on the remote's modem. Make sure that the carrier detect signal (DCD) is set to follow a normal carrier.
- Q pcANYWHERE seems to freeze up when I use it to access Novell NetWare services.**
- A Make sure you run the NetWare shell program *before* you run Norton pcANYWHERE for Windows.

Keyboard

Many software applications require control of the keyboard to function properly, so you must use the special keyboard handler, a device that allows the remote user to operate the host PC effectively while executing host applications that handle keyboard input in a non-standard fashion. Other TSRs can also affect the keystrokes on the host PC.

Q My remote screen looks fine, but the keyboard doesn't seem to work correctly.

A You may need to try Norton pcANYWHERE's special keyboard handler. Choose ONLINE SETTINGS... from the Remote Online Menu, and select Level 1 from the Special Keyboard Handler drop-down list box. If Level 1 fails continue to try the other levels. (The host must have the Allow Special Keyboard Handler option enabled in the Advanced Caller Options dialog box.)

DOS Graphics

Both the host TSR and remote PCs have display options for DOS sessions that can improve the display of graphics on the remote screen.

Q My remote screen repaints frequently on my monochrome monitor when I run host programs that are in color.

A Try running the programs in black-and-white mode, if possible. Norton pcANYWHERE is sending a lot of attribute information that your screen doesn't need. Also you can uncheck the Translate Monochrome Attributes option in the Configure Remote Operation dialog box.

Q Both the remote and host PCs have graphics adapters that are compatible with pcANYWHERE, but graphic images do not appear on the remote screen.

A The host user may need to make a change in the host TSR configuration. Try checking the Advanced Graphics Mode Detection check box found in the DOS TSR Setup dialog box.

Remote Printing

Q When I issue a print command during a session, nothing happens.

A Discard is the default destination for print output in pcANYWHERE. Make sure that you have the print destination configured correctly. You can check this during a session by choosing ONLINE SETTINGS... from the Remote Online Menu and selecting the desired destination from the Print Output Destination drop-down list box. This option is in effect for the *current session only*. To select a print destination for *all* remote control sessions, end the current session and choose REMOTE OPERATION... from the Configure menu and change the Print Output Destination option. See “Configuring Remote Operations in Chapter 5, “Configuring Norton pcANYWHERE,” for details.

If PCs are on a network, make sure that a network print queue utility is not active on the Host.

Q I am using a serial connection with the host PC. When I try to print to my remote printer, some of the characters don't print.

A If your printer runs at a slower speed than the data rate used for Norton pcANYWHERE, you may have to communicate at a slower rate or use a print buffer to solve this problem.

Q My print commands print only at the host location.

A When selecting the remote as a print destination, the host must have a printer driver that matches the driver installed for your local printer. The host application you are printing from must be configured to use the same print driver as the remote. If you do not select the correct printer driver, your printed output may print incorrectly. If you print to both the host and remote, both host and remote printer drivers must be identical.

In addition, the Windows Printer configuration on the host PC may require some changes.

To change the host's printer configuration while connected:

- 1 Double-click the Control Panel icon in the Program Manager's Main group box.
- 2 Double-click the Printers icon to open the Printers dialog box.
- 3 Select a printer, click the Set As Default Printer button, and uncheck the Print Manager check box.
- 4 Click Connect.... Make sure the printer's port is connected to LPT1. Uncheck the Fast Printing Direct to Port check box.
- 5 Click OK.
- 6 Click Close to return to the Control Panel dialog box.
- 7 Close the Control Panel dialog box.

Glossary

ACS (asynchronous communications server)

A communications server that manages a pool of modems. It directs outgoing messages to the next available modem and directs incoming messages to the appropriate workstation. *See* asynchronous transmission.

Additional Modem Initialization String

An option in serial hardware configurations. Norton pcANYWHERE automatically issues the modem initialization string for the selected modem (unless you have selected Manual or Custom). However, you can use special commands supported by your modem by including those commands in the setting for this option. For example, you can enter a command that automatically turns off the speaker of your modem. For a Hayes-compatible modem, such a command would be: `ATM0`.

If you have selected the Manual modem option, the setting for this option initializes your modem. Follow the instructions in your modem's manual, and make sure that the other hardware configuration settings are correct for your modem.

Adjust Speed to Modem

An option in serial hardware configurations. When it is set to Yes, the serial port speed is always adjusted to the connect speed reported by the modem. If it is set to No, the speed is not adjusted.

Always Connected

A setting for the Connection Started By and Connection Ended By options in serial hardware configurations. Use this setting if your equipment does not support connection detection signals. *See* connection detection.

ANSI (American National Standards Institute)

An organization of industry and business groups that develops voluntary U.S. standards for trade and communications. In Norton pcANYWHERE, this refers to a terminal emulation that enables the use of ANSI commands (escape sequences) to control the screen and keyboard. These escape sequences have been standardized by ANSI.

asynchronous transmission

A way of transmitting data at irregular time intervals in which information is sent one character at a time. Each character contains a start bit, followed by a number of data bits, and ends with a stop bit. This is the common method of communicating using a modem. *Contrast* synchronous transmission.

- attribute** A characteristic of something. A video attribute is a visual feature used to set off certain parts of a screen, such as highlighting or blinking. Not all monitors and display adapters support all attributes, so you may want Norton pcANYWHERE to translate certain attributes when the host screen is displayed on the remote PC. File attributes include the date, time, and size of the file.
- Banyan** A network protocol you can choose as part of a hardware configuration. It is one of the possible settings for the Device/Port option and refers to the network driver for Banyan VINES.
- baud rate** The number of times per second a signal changes in a communications channel. The term baud is often erroneously used to describe the speed at which the modem can transfer data. The correct measure for data rate is bits per second (bps).
A baud can vary in the number of bits it can represent. For example, a 300-baud modem that transmits one bit per baud (300 x 1) is also a 300-bps modem. However, what is often called a 1200-baud modem is really a 300-baud modem that transmits four bits per baud (300 x 4) or 1200-bps. *See* bps and data rate.
- BBS (Bulletin Board Service)** A computer system that serves as an information and messaging center for a group of users who can dial in and connect using modems and communications software. Generally, users of a bulletin board share a particular interest.
- bidirectional gateway** A gateway that accepts data via either of two communications devices and transmits that data via the other. A device can be the incoming device for one transmission and the outgoing device for another. *Contrast* unidirectional gateway.
- bit** A computer sends electrical current that is understood as a series of ones and zeros. The number one represents an “on” charge or *bit* (binary digit), while a zero represents an “off” bit.
- blank** With regards to a computer screen, to clear or not show an image on the screen. You can configure a Norton pcANYWHERE host to blank the host screen once a connection has been made or to allow the remote user to blank it. This allows the remote user to work unobserved.
- blink** With regards to a computer screen, the flashing on and off of a displayed character or the cursor. You can configure Norton pcANYWHERE to disable blinking characters if you do not want to support the blinking text attribute, or if it causes unstable display performance.

bps	Abbreviation for bits per second, a measure of the speed at which a device such as a modem can transfer data. Also known as data rate. <i>Compare</i> baud rate.
break length	<i>See</i> break signal.
break signal	In terminal emulation, a break signal interrupts a program running on a mainframe or minicomputer. This is different from the Ctrl+C or Ctrl+Break used by PCs. You specify the length of the break signal as part of a serial hardware configuration.
byte	A set of eight bits. Each byte represents a character (such as an integer from 0 to 9 or a letter of the alphabet). <i>See</i> <i>bit</i> .
cable	A group of wires enclosed in a protective tube, usually an organized set of wires that correspond to specific pins on 9- or 25-pin connectors located at each end. A cable is used to connect peripheral devices to each other or to another computer. <i>See</i> also null modem cable.
callback	A return call to the remote PC made by the host PC after verifying the remote password—if there is one. Callbacks are controlled by the host PC. If the telephone number is not part of the caller information, the remote user is prompted for a number. To specify a number of seconds as a delay before the host PC makes the call back, use the Delay Before Callback Attempt option, which is a host general preference.
caller information	All the information and access privileges for a specific remote user or a group of remote users. The information can include a password, drive access, and so forth.
carriage return (CR)	A control character (^M) that tells a computer to return to the beginning of the current line. A separate character, the linefeed (LF)# character (^J), advances the cursor to the next line. Because carriage return is often combined with linefeed, the combination is often referred to as carriage-return/linefeed, CR/LF, or hard carriage return.
carrier	The signal generated by a modem that is used to transmit data. The scratchy sound you hear when you initially connect with another modem is the carrier signal.
carrier detect	The connection detection method used by most modems. Carrier Detect is a signal indicating that two modems have detected one another. This is also a setting for the Connection Started By and Connection Ended By options that appear in serial hardware configurations. It is used as the setting for both options in direct

	serial connections (with a null modem cable) and for Connection Ended By for modem connections. <i>See</i> connection detection.
carrier loss	A break in the connection between two computers.
case-sensitivity	The discrimination between lowercase and uppercase characters.
channel	In communications, a medium for transferring information, also known as a line or a circuit. Depending on its type, a communications channel can carry information in analog or digital form. A communications channel can be a physical link, such as the cable connecting two stations in a network, or it can consist of some electromagnetic transmission on one or more frequencies within a bandwidth in the electromagnetic spectrum.
chat mode	A way for the host and remote user to communicate online during a remote control session. A dialogue window appears on each screen. Both users' messages appear on both screens.
class	A way to group gateway hardware configurations that have similar characteristics. When you create the gateway, you assign it to a class. A class is specified in a network hardware configuration when you want to use a gateway in that class.
Clear To Send (CTS)	A setting for the Connection Started By and Connection Ended By options in serial hardware configurations. Use it if the manual for the special hardware you are using indicates that this is the method used to signal an incoming call. <i>See</i> CTS and RTS/CTS.
COM port	Also known as a serial port. DOS references these ports by the names COM1, COM2, COM3, and COM4.
command-line option	An option added to a command that is entered at the DOS prompt. Also called a switch or argument. For example, in <code>AW_HOST -m=w</code> is a command-line option that loads the pcANYWHERE HOST TSR in wait for a call mode.
communications	The transfer of data between computers by means of a device such as a modem or a cable.
communications link	A connection between computers (and/or peripherals) that enables data transfer. A communications link can be a network, modem, or cable.
communications port	A location for sending and receiving serial data transmissions. <i>See</i> port.

- communications protocol** A set of rules designed to allow computers to exchange data with one another with as little error as possible. Some protocols, such as RS-232-C, refer to hardware standards; others, such as XMODEM, refer to file-transfer protocols. *See* flow control, protocol.
- communications system** The combination of hardware, software, and data-transfer links that makes communications possible.
- compression** *See* data compression.
- computer name** The name you assign to your PC for Norton pcANYWHERE sessions.
- configuration** *See* hardware configuration, session configuration, caller privileges, and gateway configuration.
- connection** The point at which devices establish a communications link.
- connection detection** A method by which your system determines that a physical connection has been made or ended, whether you are connecting using a modem or by a direct connection. (Norton pcANYWHERE uses two hardware configuration fields: Connection Started By and Connection Ended By.)
- Almost all modems send a signal called a carrier detect via cable using a pin in the serial interface with the same name.
- In very rare cases, and depending upon your equipment, you may use other signals, such as Clear To Send (CTS), Ring Indicator (RI), or Data Set Ready (DSR).
- Connection Ended By** An option in serial hardware configurations that indicates the type of signal your system uses to detect a disconnection from another computer when you end a session. In most cases, Norton pcANYWHERE sets this for you automatically. *See* Connection Started By.
- Connection Started By** An option in serial hardware configurations that indicates the type of signal your system uses to detect a connection to another computer when you begin a session. In most cases, Norton pcANYWHERE sets this for you automatically.
- Direct connections typically use Carrier Detect (DCD) as the setting for both the Connection Started By and Connection Ended By options. If you are using a modem other than Manual, the Connection Started By option should be filled in with Modem Response; even for Manual modems, the Connection Ended By option almost always should be set to Carrier Detect (DCD). *See* Connection Ended By.

- CR** *See* carriage return.
- crash recovery** A way to salvage data partially transmitted at the time a connection ends abnormally. One of the options that can be set in the Norton pcANYWHERE for Windows File Manager or the ZMODEM file transfer protocol.
- CTS** Clear To Send. A signal sent from a modem to the computer to which it is connected, indicating that it is ready for transmission. CTS is sent over line five in standard RS-232-C connections. *See* connection detection, RTS/CTS, and Clear to Send.
- Custom Modem** A modem option available in the Edit Hardware Configuration dialog box. When your modem or a reasonable alternative cannot be found in the list of supported modems, you can select Custom Modem and enter all the commands needed by your modem to make a connection.
- data bits** In asynchronous transmission, this is the group of binary digits (bits) used to represent a single character of data. The number of data bits (usually 7 or 8 for modems) used in a transmission must be agreed upon by the sending and receiving computers. Each group of data bits in a transmission is preceded by a start bit and followed by an optional parity bit as well as one or more stop bits.
- Norton pcANYWHERE uses 7 when parity is set to anything other than NONE. *See* asynchronous transmission, parity, start bit, stop bit.
- data compression** A method by which data is compacted for more efficient transmission. It is compressed before transmission and decompressed afterwards.
- data rate** The speed at which information is moved between the computer and the modem; measured in bits per second, or bps.
- Data Rate** An option found in serial hardware configurations. It specifies the bps at which data is transmitted over a modem or null modem cable.
- Data Set Ready (DSR)** A setting for the Connection Started By and Connection Ended By options in serial hardware configurations. Use it if the manual for the special hardware you are using indicates that this is the method used to signal an incoming call. *See* DSR and connection detection.

data transfer	The movement of information from one location to another. The speed of transfer is called the data rate, or data transfer rate, and is usually measured in bits per second (bps).
data transmission	The electronic transfer of information from a sending device to a receiving device.
destination	The directory to which a file is being transferred.
Device/Port	An option in all hardware configurations. It allows you to select a type of device or device driver for communications, or the port used by such a device.
dial	In Norton pcANYWHERE, to initiate a connection via LAN, modem, or direct connection, whether or not actual "dialing" is involved.
Dial Type	An option in serial hardware configurations. Most telephone systems support tone dialing, which is faster than the old-fashioned pulse dialing. However, some phone systems still support pulse dialing only. If your telephone is set to tone, this setting should also be Tone. The settings are Tone and Pulse, with Tone as the default.
direct connection	A form of data communication in which one computer or terminal is directly connected to another, usually via a null modem cable. <i>See</i> null modem cable.
display	<p>The screen or monitor.</p> <p>The following display options affect the display speed and graphic representation of the host screen on the remote PC during DOS applications: Maximize Display Speed, Synchronize Display with Host, Full Graphics Support, Advanced Graphics Mode Detection, Translate Monochrome Attributes, and Allow Blinking Characters.</p>
download	In communications, the process of transferring a copy of a file from a host computer to the local computer by means of a modem or network. In Norton pcANYWHERE, using a modem-based communications link, the process generally involves the local computer instructing the distant or host computer to begin the transfer and the local computer saving the incoming file on disk. <i>Compare</i> upload.
download directory	The directory in which files received during file transfer are stored.

drive mapping	Allowing remote drives to be accessed as if they were additional drives on the host PC (during remote control sessions). From the remote PC, select Drive Mapping in the Edit Host PC dialog box to define what drive letters will be used on the host PC to access the remote's drives.
drive security	The designation of fixed, floppy, and network drives on the host PC as accessible or inaccessible to the remote user. When accessible, the drives may be designated as read-only or read/write.
DSR	Data Set Ready. A signal sent from a modem to the computer to which it is attached, indicating that it is ready to operate. <i>See</i> Data Set Ready and connection detection.
DTR	Data Terminal Ready. A signal used in serial communications that a computer sends to the modem, indicating that the computer is available to accept incoming transmissions. <i>See</i> DTR State.
DTR State	An option in serial hardware configurations that allows you to control hardware settings for serial communications. Automatically set by Norton pcANYWHERE for your modem. Change it only when special equipment is in use. The settings are Always On, Always Off, and On While Connected. <i>See</i> DTR.
error-checking method	A method of error correction. For example, for the ZMODEM file-transfer protocol, you can specify 16-bit CRC or 32-bit CRC error-checking.
error correction	Noisy lines or faulty connections can sometimes cause errors that translate into erroneous characters on the screen and in transferred files. With error correction, data is retransmitted until it has been received correctly. Norton pcANYWHERE performs software-based error correction.
external modem	These <i>modems</i> are independent from the computer and have sockets to connect a phone line, a computer, and a power supply. They usually connect directly to the phone line, via a phone jack. This is called a modular connection.
file transfer	The process of using communications to move or transmit a file from one computer to another. In communications, a protocol must be agreed upon by sending and receiving computers before file transfer can take place. <i>See</i> file-transfer protocol.

file-transfer protocol

The method of file transfer understood and used by both the remote and the host computer. For online sessions, you select a file-transfer protocol acceptable to the online service as part of the session configuration. You can change your selection during a session. If you select ASCII or ZMODEM as the protocol, you can set preferences for them prior to or during the session.

For remote control sessions, the protocol is built into the Norton pcANYWHERE File Manager program.

flow control

A signal that acknowledges that communication or the transfer of information can take place. When a modem or computer receives data at a faster rate than it can be processed, data is stored in a special area of memory called a data buffer. Flow control prevents data loss by temporarily halting data transmission when the buffer approaches its capacity. Also an option in serial hardware configurations. *See* handshake.

Handshakes, as flow control is also called, can be controlled by either hardware or software. A hardware handshake, as between a computer and a modem, is an exchange of signals, over specific wires, in which each device signals its readiness to send or receive data (*see* RTS/CTS). A software handshake, usually exchanged during modem-to-modem types of communication, consists of actual information transmitted between the sending and receiving devices. A software handshake establishes agreement between devices on the protocols that both will use in communicating. *See* communications protocol, XON/XOFF. If your modem supports hardware flow control and the online session requires software control, try choosing Both as the flow control setting.

gateway

A pcANYWHERE gateway is a PC on a LAN with a modem. The PC runs a small TSR in the background, which allows users on the network to dial-out and/or off-LAN users to dial-in to the LAN via the modem. *See* bidirectional gateway and unidirectional gateway.

gateway configuration

The setup for a gateway that provides its name, class, incoming configuration, and outgoing configuration. *See* gateway, incoming configuration, and outgoing configuration.

Gateway Name

An option in network hardware configurations indicating the name of the gateway to be used for the connection.

- handshake** A signal indicating that the devices involved are ready to communicate. Handshakes can be controlled by either hardware or software. A hardware handshake occurs when the two devices send signals over specific wires, indicating they are ready to send/receive data. A software handshake occurs when actual information is sent between the two devices. *See* flow control.
- hardware configuration** A set of hardware options, such as modem type, port/device, and data rate, that indicates exactly what hardware is used to make the connection between two computers for either a remote control or an online session.
- host PC** The computer to which the remote user is connected.
- host password** The password a remote user uses to access a specific host PC. The password is often listed as part of caller privileges.
- The host user can stipulate one password for any remote user or individual passwords for particular remote users. The host user can limit the number of times the user can attempt to enter the password, the amount of time during which the user can enter the password, or designate the password as case-sensitive.
- As a precaution when a connection is ended abnormally or by an inactivity timeout, the host PC can stipulate that only the password used for the lost connection or the host's master password can be used to reconnect to the host. If it is not necessary to protect the previous remote user in this way, the host PC can allow any valid password to connect to the host PC (as is usual when using caller information configurations). *See* password, master password.
- hotkey** The keystroke sequence that brings up a Norton pcANYWHERE for Windows menu during a session with the DOS Host TSR. The host hotkey is initially Alt+RightShift.
- inactivity timeout** The time period (in minutes) after which a remote control session is ended for inactivity. Inactivity is defined as the absence of keystrokes, mouse movements, and data transmission between PCs. Establishing an inactivity timeout period keeps the telephone line free in case the remote user forgets to end the session when finished using the host PC. Specify the number of minutes in the Disconnect if Inactive for text box in the Host Security Options dialog box. The host can control which remote callers are subject to the inactivity timeout by enabling or disabling the Caller Subject to Inactivity Timeout option in the Advanced Caller Options dialog box.

As a precaution when a connection is ended by an inactivity timeout, the host PC can stipulate that only the password used for the lost connection or the host's master password can be used to reconnect to the host. The Allow Any Password on Reconnect to Session option in the Host Security Options dialog box, determines what passwords are valid in this case.

A gateway preference can also specify an inactivity timeout. It applies only to idle sessions that use a gateway. Inactivity, in this case, is defined as an absence of transmitted data.

incoming configuration

One of the two hardware configurations specified for a gateway. For unidirectional gateways, it describes the hardware connection that initially links a computer to the gateway. *See* hardware configuration, outgoing configuration, unidirectional gateway, and bidirectional gateway.

initialize

To prepare for use. In communications, to set modem and software parameters at the start of a session.

Int14

See Interrupt 14.

internal modem

An internal modem is a circuit board installed in a computer. It generally has two connectors, or jacks, which are visible at the back of the computer. One connects directly into the phone line; the other can be connected to a telephone handset. *See* also external modem.

Interrupt 14

A special interrupt method of communicating with a communications port via BIOS calls. This method slows down communications, but is used only with special interrupt device driver software.

Select this option as your Device/Port option in a hardware configuration if you are using a third-party communications driver and its instructions stipulate Interrupt 14 BIOS calls. If you select this option, you are also prompted to choose 1 of the 16 communications ports (COM1, COM2, COM3, and so on).

interrupt request (IRQ)

Request for a hardware interrupt. Each IRQ has a number corresponding to one of the fixed set of interrupts for the PC. PC's with the AT architecture have interrupts from 0 to 15.

keyboard

The input-only device used to type keystrokes.

The host user can decide whether the host PC receives keystrokes from the host PC, the remote PC, or both. When the remote keyboard is disabled, the remote user is merely an

onlooker, which may be useful in a tutorial session. When the host keyboard is disabled, the remote user cannot be interrupted. *See also* keyboard handler.

keyboard handler (DOS HOST TSR)

A device that allows the remote user to operate the host PC effectively while executing host applications that handle keyboard input in a non-standard fashion.

The host user uses the Allow Special Keyboard Handler option (in Advanced Caller Options) to specify whether or not a keyboard handler is used by the remote user and the Special Keyboard Handler Type option (a DOS Host TSR Setup option) to specify which handler is used. The two keyboard handlers available are called Type 1 and Type 2. The Type 1 keyboard handler has three variations known as Level 1, Level 2, and Level 3. The Type 1 handler monitors the BIOS keyboard routines. For most applications, Type 1 is appropriate and is, therefore, the default setting for the Special Keyboard Handler Type option. The Type 2 handler writes keyboard codes to the keyboard. It is faster than Type 1, but it does not work on all host PCs. For example, it works well with computers that have a PS/2 BIOS. The remote PC cannot use a keyboard handler on the host PC if the host does not allow it.

When the Type 1 handler is used, the remote user can choose the level or choose not to use the handler by setting the Special Keyboard Handler option, a remote control session preference. This can be changed during a session. If you, as the remote user, experience keystroking difficulties, try Level 1, then Level 2, then Level 3. For example, Level 1 is best for Microsoft editors. If you find it difficult to select menu items using keystrokes or cannot select text with the arrow keys in the editor, use Level 1. A number of terminal emulations require Level 1 or Level 2.

LAN

Local Area Network; a group of computers and other devices dispersed over a relatively limited area and connected by a communications link that enables any device to interact with any other device on the network. *See* network.

launch

To start a program or application.

leased line

A telephone channel leased from a common carrier for private use. A leased line is faster and quieter, but generally more expensive than a switched telephone line. *Compare* switched line. Leased Line is an option in serial hardware configurations. Set it to Yes if you are using a leased line. It is set to No by default.

- linefeed (LF)** A control character (^J) that tells a computer to advance one line below the current line. Because linefeed is often combined with carriage return, the combination is often referred to as carriage-return/linefeed or CR/LF.
- local** An item or operation that is close at hand. For example, when a remote user downloads a file to the remote PC, the file is downloaded locally.
- log** The action of recording or the record of the activities and events that take place on a computer system. The records are stored in a data file.
- Information about a session can be logged in the remote or host PCs' log files. The host PC can log information about connections with specific remote users and specify that all failed connections be logged. The remote PC can log information about sessions with specific host PCs and online services.
- login procedures** The process of identifying oneself to a computer after connecting to it over a communications line. During the login procedure, the computer usually requests the user's name and a password. On a computer used by many people, the login procedure provides a means of identifying authorized users, keeping track of their usage time, and maintaining security by controlling their access to sensitive files or actions.
- Norton pcANYWHERE can be configured to require a password and a login name for remote control sessions. These options are found in the Host Security Options dialog box.
- logoff** Also called logout. The process of ending a session with a computer accessed over a communications line.
- LPT1, LPT2, LPT3** Names reserved by the MS-DOS operating system for up to three parallel printer ports. See *parallel port*.
- macro** A set of characters and/or control codes assigned to a macro key. When the macro key is typed, the assigned keystrokes are executed (played back). For example, a single macro keystroke can send a password to an online service.
- macro key** Keystroke (from Alt+0 to Alt+9) assigned to a string of keystrokes. See macro.
- map** To give a drive on the remote PC a drive letter on the host PC. You can then use the remote drive as though it were a drive on the host PC. For example, you can access a document on the remote PC while running a program remotely on the host.

- master password** The password that must be entered before changes can be made to configurations and other setup information stored by Norton pcANYWHERE. *See* also password and host password.
- modem** Short for *modulator/demodulator*, a communications device that enables a computer to transmit information over a standard telephone line. A modem translates (modulates) digital data to an analog signal for transmission over telephone lines, then translates back to digital (demodulates) at the other end. Modems can transmit at different speeds or data-transfer rates. *See* baud rate, bps.
- Modem Response** A setting for the Connection Started By option in serial hardware configurations. Do not use this setting when you have selected Manual modem. *See* connection detection.
- mouse** A handheld device used to control a cursor on the screen. For remote control sessions, the remote user can adjust certain features about the mouse and the mouse cursor for DOS applications. These adjustments go into effect only if the host user allows them to by enabling the Allow Remote Mouse option, which is a host features preference.
- NACS** Novell NetWare Asynchronous Communications Services. NACS allows any network station to share dial-up phone lines or directly connected lines to a host or other asynchronous device. In addition, remote users can access the network and transmit data over synchronous protocols.
- NASI** NetWare Asynchronous Services Interface. Network station software used with Novell's NetWare Asynchronous Communications Services (NACS).
- NASI/NCSI** The device driver for a network asynchronous communications server (ACS) such as an ACS2 or a NACS. Select this as the setting for the Device/Port option in a hardware configuration if your network is set up for this type of ACS connections. *See* ACS.
- NetBIOS** A standard network protocol introduced by IBM and implemented by a device driver. Most network operating systems (including NetWare) have support for NetBIOS. Select this as the setting for the Device/Port option in a hardware configuration if you are on network other than NetWare IPX that uses a NetBIOS device driver.

- NetWare IPX** A Novell network protocol implemented by a device driver. Select this as the setting for the Device/Port option in a hardware configuration if you are on a NetWare network and want to communicate with other PCs on the network or use a gateway for off-LAN connections.
- network** A group of computers and associated devices that are connected by communications facilities (both hardware and software) for the purpose of sharing information and peripheral devices such as printers and modems. *See* LAN.
- node** A PC connected to a LAN through a network adapter card and appropriate software. Also called a workstation.
- null modem cable** A cable that enables two computers to communicate without the use of modems. A null modem cable accomplishes this by crossing the sending and receiving wires so that the wire used for transmitting by one device is used for receiving by the other and vice versa.
- offhook** A telephone or modem that is in use.
- onhook** A telephone or modem that is not in use.
- online service** A computer communications system or service that allows users to dial in for information, messages, and files. CompuServe is an example of a commercial online service. *See* BBS.
- outgoing configuration** One of the two hardware configurations specified for a gateway. For unidirectional gateways, it describes the hardware connection used by the gateway to transmit the data it has received via the incoming configuration. *See* hardware configuration, incoming configuration, unidirectional gateway, and bidirectional gateway.
- parallel port** Generally used for printer connections. Most computers have at least one parallel port (referred to as LPT1) for this purpose.
- parity** An error-checking procedure in which the number of 1's must always be the same—either even or odd—for each group of bits transmitted without error.
- In typical modem-to-modem communications, parity is one of the parameters that must be agreed upon by sending and receiving parties before transmission can take place. Parity is also an option in serial hardware configurations.

- parity bit** An extra bit called a parity bit, which represents a character, is added to the data bits by the sending computer. Parity bits are used in modem-to-modem communications. The setting of the parity bit depends on the type of parity used. The receiving device counts the number of 1s in each arriving group of data and parity bits; if the number is odd when it should be even, the device can assume that one of the bits was transmitted incorrectly and that an error occurred. *See* parity.
- password** A password is a unique string of characters that a user types as an identification code. The system compares the code against a stored list of authorized passwords and users. If the code is legitimate, the system allows access, at whatever security level has been approved for the owner of the password. *See* host password and master password.
- port** A hardware location for passing data in and out of a computing device. Computers have ports for connecting peripheral devices, such as the COM (or RS-232-C) ports used to connect modems and printers. *See* communications port.
- prefix** A code required before a telephone number. For example, the number 9 is often required to call out from many office PBX systems.
- protocol** A set of rules designed to allow computers to exchange data with one another with as few errors as possible. *See* communications protocol.
- PRN** The logical device name for the printer.
- pulse dialing** Rotary-style dialing (clicks can be heard when dialing) as opposed to touch-tone dialing.
- Receive 2 CRs** A setting for the Connection Started By option in serial hardware configurations. Use this setting for the host PC if no other connection detection system can be used and you want some type of signal. When the user types two carriage returns (CRs), a connection is assumed. The remote PC must use a hardware configuration that specifies Always Connected as the setting for both the Connection Started By and Connection Ended By options. *See* connection detection.
- record** To capture a chronological series of actions and events that occurred during a remote control or online session and store this information in a file called a record file.

Redial Attempts	An option for serial hardware configurations that indicates how many times to attempt to make a connection to another computer after the first attempt fails (usually because the line is busy). Type in any number from 0 (the default) to 9999.
remote PC	A computer that controls another PC, called a host PC.
remote communications	Interaction with a host by a remote computer through a telephone connection or another communications line.
remote control	The act of controlling one PC, called a host PC, from another, called a remote PC.
remote drive mapping	<i>See</i> drive mapping.
Ring Indicator (RI)	A setting for the Connection Started By and Connection Ended By options in serial hardware configurations. Use it if the manual for special hardware you are using indicates that this is the method used to signal an incoming call. Some PBX systems require Ring Indicator (RI) as the setting for the Connection Started By option and Carrier Detect (DCD) for the Connection Ended By options. <i>See</i> connection detection.
Ring No. to Answer On	An option for serial hardware configurations that indicates the number of rings after which your modem answers the phone when you receive a call. Normally, the setting is 1, but you can specify more rings if you wish to allow time for a person to answer before the modem does.
RS-232-C standard	An industry standard for serial communication connections. Specific lines and signal characteristics are used to control the transmission of serial data between devices.
RTS	Request to send. An RS-232-C signal used in hardware flow control to pace information sent from one device to another. RTS is also used in most modems that equal or exceed 9600 baud, as well as direct connections. <i>See</i> RTS/CTS, CTS, and RTS State.
RTS/CTS	A setting for flow control in a hardware configuration. It specifies hardware flow control rather than software flow control. This is recommended, but some online service sessions may require software flow control (XON/XOFF). <i>See</i> RTS, CTS, XON/XOFF, and flow control.
RTS State	An option in a serial hardware configuration that allows you to control hardware settings for serial communications. Automatically set by Norton pcANYWHERE for your modem. Change it only when special equipment is in use. The settings are Always On, Always Off, and On While Connected. <i>See</i> RTS.

scan	The process by which Norton pcANYWHERE checks the host screen to see if anything has changed since the last scan. In rare cases you may need to change the time delays between scans.
script	A type of program that consists of a set of instructions to an application. A script usually consists of instructions expressed using the application's rules and syntax, combined with simple control structures. See <i>Creating Norton pcANYWHERE Scripts</i> , which accompanies this user's guide.
Seconds Between Redials	An option for serial hardware configurations that indicates the number of seconds that Norton pcANYWHERE should wait before attempting a redial. Type in any number up to 9999. The default is 10.
Seconds To Wait After Dial	An option for serial hardware configurations that indicates the maximum number of seconds that Norton pcANYWHERE will wait for a successful connection after dialing a number. You can tailor this time period to the speed of the telephone system you are working with. The default is 60.
serial communication	The transmission of information between computers or between computers and peripheral devices one bit at a time over a single line (or data path one-bit wide). Serial communications can be synchronous or asynchronous. Both the sender and receiver must use the same data rate, parity, and control information. Most modems can determine automatically the best rate available to both of them.
serial interface	A data-transmission scheme that sends data and control bits in a one-bit wide data path sequentially over a single transmission line. See RS-232-C.
serial port	A location for sending and receiving serial data transmissions. Also known as a communications port or COM port.
serial transmission	The transmission of discrete signals one after the other. In communications and data transfer, serial transmission involves sending information over a single wire one bit at a time; this is the method used in microcomputer modem-to-modem communications over telephone lines.
session	In communications, the time during which two computers maintain a connection and, usually, are engaged in transferring information.

session configuration	Information used to automate the connection process for a remote control or an online session. For example, a session configuration may include the telephone number to be dialed, the terminal emulation to be used for an online service, or the host password for a host PC.
signal	A general term for any electrical quantity that can be used to transmit or represent information.
signal state	A high or low voltage state. +3 volts or higher equals a binary 0, -3 volts or less equals a binary 1.
spool file	A file that stores data to be printed until the printer is ready to process it. Computer software called a print spooler controls the file and prints the data.
start bit	In asynchronous transmission, the bit that signals the beginning of a character. Start and stop bits are required in asynchronous transmissions because the irregular time gaps between transmitted characters makes it impossible for a receiving device to determine when the next character should arrive. These start and stop bits add considerable overhead to transmissions, increasing the transmission time as much as 20 percent over the synchronous equivalent.
stop bit	In asynchronous transmission, the bit that signals the end of a character. Start and stop bits are required in asynchronous transmissions because the irregular time gaps between transmitted characters makes it impossible for a receiving device to determine when the next character should arrive. Norton pcANYWHERE always uses 1 stop bit.
suffix	A code appended to the end of a telephone number, such as a calling card number for billing purposes.
switched line	A standard dial-up telephone connection; the type of line established when a call is routed through a switching station. <i>Compare</i> leased line.
synchronous transmission	A form of data transmission in which information is sent in blocks of bits separated by equal time intervals. The sending and receiving devices must first be set to interact with one another at precise intervals, then data is sent in a steady stream. <i>Contrast</i> asynchronous transmission.

TCP/IP (Transmission Control Protocol/Internet Protocol)	<p>A set of network protocols developed to allow PCs on networks to communicate with other PCs, as well as a variety of non-PC systems such as minicomputers and mainframes.</p> <p>Norton pcANYWHERE for Windows only supports PC connections using the TCP/IP protocols.</p>
Telebit ACS	<p>The Telebit ACS device driver for a network asynchronous communications server(ACS). Select this as the setting for the Device/Port option in a hardware configuration if your network has Telebit ACS connections.</p>
terminal	<p>A device consisting of a monitor, video adapter, and keyboard. A terminal does little or no processing on its own; instead, it is connected to a computer with a communications link over a cable. Terminals are used mainly with multi-user systems, where they are used to monitor and receive but not store information (i.e., with a mainframe). <i>See</i> terminal emulation.</p>
terminal emulation	<p>The technique of imitating a terminal by using software that conforms to a standard such as the ANSI standard for terminal emulation. Norton pcANYWHERE can make your computer act as if it were a particular type of terminal in order to communicate with another computer, such as a mainframe.</p>
terminal mode	<p>The pcANYWHERE mode that mimics a terminal when connecting to an online service for an online session.</p>
timeout	<p>A predetermined period of time during which a given task must be completed. If the timeout value is reached before or during the execution of the task, the task is canceled. <i>See</i> inactivity timeout.</p>
tone dialing	<p>Sounds of particular frequencies can be heard when dialing, as opposed to pulse dialing, in which clicks can be heard.</p>
translation table	<p>A table that specifies a conversion of specific data bytes from one code to another.</p>
unidirectional gateway	<p>A gateway that receives data only via the communications device specified in the incoming configuration and transmits data only via the device specified in the outgoing configuration. <i>Contrast</i> bidirectional gateway.</p>
upload	<p>In communications, the process of transferring a copy of a file from a local computer to a distant computer by means of a modem or network. With a modem-based communications link, the requesting computer generally instructs the distant computer to prepare to receive the file on its disk and then waits for the transmission to begin. <i>Compare</i> download.</p>

- Use Gateway** An option in network hardware configurations. Set this to Yes if you want to use a gateway. *See* gateway.
- voice-first connection** A connection via modem for a remote control session, in which you talk first, then switch to data communications. The telephone line must be shared by both the modems and the telephones. Norton pcANYWHERE prompts you through this process.
- Windows swap file** In remote control sessions, a file (AW.SWP) used to improve the display of Windows, when Windows is run on the host PC. The swap file (on the remote PC) contains Windows' bitmap data. If the bitmap data is in the file when a Windows screen is redrawn, the data does not have to be resent, which results in better performance. The remote user specifies the size of the swap file.
- wrap** The ability of the program to continue displaying information on a new line or page when the end of that line or page is reached.
- XON/XOFF** The most common of asynchronous communications protocols established to govern software flow control. Under this protocol, the receiving device sends a specific character when it wants the transmitting device to stop sending characters. It sends a different character when it wants the transmission to resume. Depending on the online service you are accessing, you may need to choose XON/XOFF as the setting for flow control in a hardware configuration. *See* flow control and RTS/CTS.

Index

Symbols

@@@ ID, 39, 41

A

access

- restrict in caller information setup, 96
- restrict using gateway configuration, 77

ACS, 67

- See also* Telebit ACS
- definition, 20
- driver, 67
- hardware configuration, 67–72
- NASI-compliant, 67
- port selection, 69
- Telebit, 70

Action menu, 30

activity log, 200–206

ACTIVITY LOG PROCESSING command, 189, 203–206

Add TCP/IP host dialog box, 101

adding

- caller to list, 97
- host PC entry to list, 102
- online service to directory, 134–135
- TCP/IP host, 100, 101

Additional Modem Initialization String, 73, 221

addresses

- serial port, 208

ADM 3A terminal emulation, 230–231

administrative installation, 38–47

administrator ID, 39

- See also* @@@ ID; supervisor ID

advanced

- caller information options, 95, 96
- direct connect options, 59
- Interrupt 14 options, 64

advanced (*continued*)

- leased line options, 61
- modem options, 57
- online service session options, 135–137

Advanced Caller Options dialog box, 95, 96

Advanced Hardware Options dialog box

- direct connection, 59
- leased line, 61
- modem, 57

Advanced Online Service Options dialog box, 136

Allow AW= check box, 44

Alt+Right Shift, 147

Alt+Tab, 154

analog communication, definition, 210

ANSI terminal emulation, 135, 231

Archive/Delete Host/Remote Log, 206

archiving log information, 205–206

arguments

- command-line, 223

ASCII

- control characters, 250
- definition, 249
- file-transfer protocol, 166, 249

ASCII text file

- saving recorded sessions as, 196, 197
- saving screens as, 200

assumptions of this guide, 15

asynchronous communications server. *See* ACS

attempted connection

- logging, 89
- prompt before, 89

AUTOEXEC.BAT, 47

- adding WIN command to load Windows automatically, 157

changing configuration file path, 44, 49

LASTDRIVE= statement, 105

AUTOEXEC.BAT (*continued*)
 modification by install program, 36

automatic
 downloading, 167
 script recording, 136
 session recording, 191
 Windows loading, 157

automating
 connection to network hosts and gateways, 103
 online service session functions, 135

AW.RH6, 201
 AW.RL6, 200
 AW= environment variable, 39, 41, 49
 AW.CI6, 29
 AW_GATE, 79
 AW_HOST, 48, 223
 command line syntax, 225
 loading, 116
 AW.HW6, 29
 AW.OS6, 29
 AW.PC6, 29
 AWuserid.BIN, 40
 AWuserid.CI6, 40
 AWuserid.HW6, 40
 AWuserid.INI, 40
 AWuserid.OS6, 40
 AWuserid.PC6, 40
 AWuserid.RH6, 201
 AWuserid.RL6, 200

B

backspace key
 destructive, 127, 163
 non-destructive, 127, 163

Banyan VINES, 65
 support for, 18

baud rate, definition, 211

BBS, connecting to, 125

Be A Host PC load button, 30, 31, 108

Be A Host PC main window, 31

Begin File Transfer dialog box, 173

bidirectional gateway, 27, 76
 specifying, 78
 what it does, 75

binary file, saving session to, 196–197

bit, 210

bit forcing, 220

bit trimming, 220

blackboard, 52

blank host screen, 89, 152
 allowing, 95

blinking characters, 100, 152

bps, contrasted to baud rate, 211

Break key, 95

break signal, 127, 223

buffer, explanation, 213

bulletin board service. *See* BBS

button bar (File Manager window), 170

buttons. *See* entries for specific buttons

byte, 210

C

cables, 214
 9-to-25-pin adapters, 215
 25-to-9-pin adapters, 215
 modem, 215
 null modem, 216
 selection, 215
 technical information, 214–216

cache file, 99

Call A Host PC load button, 30, 31, 117

Call A Host PC main window, 31

Call button, 117, 137

Call Online Service load button, 30, 31, 137

Call Online Service main window, 31

CALL REMOTE command (Offline Menu), 115

callback
 enabling, 94, 97
 specify delay before, 86

caller
 adding, 97
 default, 97
 defining, 97–98

- caller information, 92–98
 - configuration files, 28
 - what it does, 21
- caller information file (AWuserid.C16), 40
- caller information file (AWuserid.C16)
 - file not found or invalid, 253
- Caller List dialog box, 97
- caller privileges, 21
 - default, 93–96
 - individual, 97–98
- calling
 - another computer, 117
 - host PC from remote PC, 117–120
 - host using OLE, 226
 - host using voice connection, 118
 - online service, 137–138
 - online service using OLE, 226
 - remote PC from host PC, 111
 - remote using voice connection, 111
 - using Quick Connect, 118–120
 - using Quick Start setup, 23–27
- CANCEL command (Offline Menu), 115
- canceling
 - gateway operation, 80
 - host PC, 115
- capturing sessions and screens, 189–200
- carriage return/line feed, 127, 163
- Carrier Detect, 212
- case-sensitive password, 89
- central processing unit. *See* CPU
- CHANGE DIRECTORY... command (File Manager File menu), 170
- changing
 - AUTOEXEC.BAT
 - to add pcANYWHERE to path, 49
 - to override personal files path, 44, 49
 - computer name, 82
 - configurations, 53
 - directory, 35
 - directory for personal configuration files, 49
 - directory in File Manager, 170
 - drive, 35
 - changing (*continued*)
 - drive in File Manager, 170
 - file details, 186
 - file transfer protocol, 164, 165–166
 - font, 162
 - hardware settings during online session, 161
 - host mode, 95, 146
 - host options, 152
 - personal files to shared files, 39
 - print destination, 149
 - printer, 266
 - printer while connected, 266
 - remote control session options during a session, 143–159
 - terminal emulation during session, 162
 - character blink attributes, 100, 152
 - character mode, 229
 - CHAT command (Host/Remote Online Menu), 145
 - chat window, 145–146
 - class
 - assigning gateway to, 78
 - gateway, 79
 - CLEAR TAGS command (File Manager Tag menu), 172
 - clear to send, 213, 214
 - clipboard
 - online service session, 161
 - remote control session, 175
 - support for, 27
 - using, 160
 - viewing contents, 176–177
 - CLONE... command (File Manager File menu), 185
 - Clone Directory dialog box, 185
 - cloning directories, 184–185
 - cold boot, 86, 156
 - color
 - remote control session, 100
 - Terminal window, 132
 - COM port, 207
 - addresses, 207, 208

- COM port (*continued*)
 - direct connect, 58
 - Interrupt 14, 63
 - interrupts, 208
 - leased line, 60
 - selecting, 55
 - setting, 54
 - specifying, 38
 - technical information, 207–223
- command line, 223–226
 - arguments, 223
 - entering, 223, 225
 - error, 255
 - load DOS TSR, 116
 - OLE access, 226
 - options, 224
 - syntax, 225
- command mode, modem, 211
- commands
 - DOS prompt, 223–226
 - modem, 211
- communication
 - analog, 210
 - digital, 210
- communications device
 - network, 66
 - sharing, 75
- communications port. *See* COM port
- COMPARE DIRECTORIES command (File Manager File menu), 181
- comparing directories, 181
- compression
 - file transfer, 186
 - setting, 222
- CompuServe, 19, 125
 - parity setting, 67
- computer, 18
 - See also* PC
- computer name, 38, 82
- configuration. *See* hardware configuration
- configuration files, 41
 - AWuserid.BIN, 40
 - AWuserid.C16, 40
- configuration files (*continued*)
 - AWuserid.HW6, 40
 - AWuserid.INI, 40
 - AWuserid.OS6, 40
 - AWuserid.PC6, 40
 - changing directory location, 49
 - conversion from earlier versions of
 - pcANYWHERE, 28
 - creating, 45
 - filenames, 29
 - management, 44
 - personal, 29, 39–41, 44
 - shared, 29, 39–41, 44
- Configure Gateway dialog box, 78
- Configure Hardware Setup dialog box
 - override settings, 161
- Configure menu, 54–74, 77, 81–92, 126
- Configure Remote Operation dialog box, 98–100
- Configure System Hardware dialog box, 54
- Configure Terminal Emulations dialog box, 126
 - override settings, 161
- configuring
 - caller information, 92–98
 - DOS Host TSR, 90–92
 - file transfer options, 187
 - gateways, 75–80
 - host options, 85–92
 - pcANYWHERE for host and remote operation, 81–106
 - pcANYWHERE for OLE automation, 227
 - pcANYWHERE for online service sessions, 125–137
 - pcANYWHERE for your computer's hardware, 53–74
 - terminal emulation settings, 126–128
 - translation tables, 130–131
- connection
 - allowing, 89
 - automating, 103
 - capturing date and time, 202
 - difficulties, 222

- connection (*continued*)
 - direct, 20, 57
 - gateway, 75
 - leased-line, 59
 - logging, 21, 89
 - lost, 253
 - methods of loading host, 108
 - methods of loading remote, 116
 - methods of starting an online session, 137
 - modem, 19
 - network, 20, 64
 - not established, 259
 - not made, 257
 - off-LAN, 64, 65, 75
 - online service, 133, 137
 - prompt host user when attempted, 89
 - Quick Start, 23–27
 - serial, 19
 - technical information, 207–223
 - types of, 19–20
 - voice, 118, 155
 - what information pcANYWHERE needs, 20
- connection detection, 222
- Control Panel. *See* Playback Control Panel
- dialog box
- Controls menu, 195
- conventions of this guide, 16
- conversation
 - using chat window, 145
 - voice, 143
- conversion of 1.0 files, 28
- copying
 - clipboard text and graphics during online service session, 161
 - clipboard text and graphics during remote control session, 175
 - files and directories using File Manager, 180–181
 - recorded session to a file, 196–197
- CPU
 - port addresses, 207–208
 - usage, gateway, 78
- CR/LF, 127, 163
- crash recovery, 186
 - enabling, 187
- creating
 - ACS hardware configuration, 68–70
 - caller entries, 97–98
 - custom modem hardware configuration, 73–74
 - direct connect hardware configuration, 57–59
 - directory, 178
 - gateway configuration, 77
 - Interrupt 14 hardware configuration, 62–64
 - leased line hardware configuration, 60–62
 - list of host PCs, 102–103
 - log report, 202–205
 - macro keys, 128
 - modem hardware configuration, 54–57
 - NASI/NCSI hardware configuration, 68–70
 - network node hardware configuration, 65–67
 - null modem hardware configuration, 57–59
 - online service list, 133–135
 - prefix/suffix list, 84
 - reports using archived data, 206
 - script file, 136
 - shared configuration files, 45
 - Telebit ACS hardware configuration, 71–72
- Ctrl+Break key, allowing, 95
- CTS, 213
- Cue Cards, 28, 30, 50, 51
- Custom Modem, 73, 221
 - settings, 73–74
- Custom Modem Settings dialog box, 74
- customizing
 - host installation, 48
 - modem commands, 73
 - system hardware settings, 54
 - terminal emulation, 126–128
 - Terminal window display, 132

D

Data Communications Equipment. *See* DCE

data compression, 211

protocol, 211

data encryption, 28, 89

data files

personal, 39–41, 44

shared, 39–41, 44

data mode, modem, 211

data rate, 213, 222

changing during online service session,
162

definition, 213

Interrupt 14, 63

modification, 55

setting, 58

Data Terminal Equipment. *See* DTE

Data Terminal Ready signal, 222

data transfer speed, 221

data transmission, 207–223

DB9 connectors, 215, 216

DB25 connectors, 215, 216

DCD, 212

DCE, 215

decimal numbers, conversion to hexadecimal,
252

default

caller, 97

caller privileges, 93–96

modem settings, 54, 55, 73

online menu hotkey, 147

Delete button, 179

DELETE... command (File Manager File menu),
179

Delete dialog box, 179

deleting

activity logs, 205–206

directories, 178–179

files, 178–179

description of hardware configuration, 58

deselecting files, 172

destination directory, 174

device sharing, 75

DG 100/200 terminal emulation, 232–234

dialing

host PC, 117

remote PC, 110

voice-first call, 111

dialing instructions, 84, 222

Dialing Prefix/Suffix dialog box, 84

dialog box. *See* entries for specific dialog
boxes

dialogue window. *See* chat window

digital communication, 210

definition, 210

direct connection, 20, 57

See also null modem cable

directory

changing, 35

changing for configuration files, 49

changing in File Manager, 170

cloning, 182–184, 184–185

compare directories feature, 181

copying locally, 180–181

creating, 178

deleting, 178–179

displaying, 171

management, 177–185

renaming, 179–180

selecting at installation, 34, 35, 43

selecting for online service file transfer,
167

synchronization, 182–184

WINAW, 34

DISABLE command (Offline Menu), 114

disabling

host PC, 114, 147

host's keyboard, 152

host's mouse, 152

host's screen, 152

remote's keyboard, 158

remote's mouse, 158

remote's screen, 158

disconnect

capturing date and time, 202

- disconnecting, 147
 - after file transfer, 174
- disk errors, 254
- display, 91
 - See also* screen
 - color, 100
 - full-screen, 153
 - graphics support, 100
 - host image, 100
 - monochrome, 100
 - synchronizing on host and remote, 100, 153
 - Terminal window, 128
- display speed
 - in DOS session, 91
- DISPLAY... command, 163
- displaying
 - captured screens, 199–200
 - clipboard contents, 176–177
 - directory contents, 171
 - file details, 186
 - Playback Control Panel dialog box, 196
- document conventions. *See* conventions of this guide
- Documents file filter, 185
- DOS graphics representation, 152
- DOS Host TSR, 48
 - command-line options, 223–226
 - command line syntax, 225
 - configuring, 90–92
 - display options, 100
 - loading, 115–116
 - network command line, 116
 - online menu hotkey, 147
 - session options, 152–153
 - smallest version, 92
- DOS sessions. *See* DOS Host TSR
- DOS TSR OPTIONS command, 90
- DOS TSR Setup dialog box, 91
- Dow Jones, 19, 125
- downloading files
 - allowing, 96
 - automation, 167
 - downloading files (*continued*)
 - file selection, 167
 - host to remote, 174
 - from online service, 164–168
 - drag-and-drop file transfer, 173, 174
 - drive
 - accessing using drive mapping, 104, 149
 - availability for mapping, 105
 - changing, 35
 - changing in File Manager, 170
 - restricting access, 96
 - selecting, 35, 167
 - File Manager, 170
 - drive mapping, 18, 27, 104–106, 149–151
 - allowing, 91
 - Drive Mappings for Host Applications dialog box, 105, 151
 - Drives list box, 35
 - DTE, 215
 - DTR state, 222
 - duplicating directories. *See* cloning directories; synchronizing
- E**
- Edit Caller Entry dialog box, 97
- Edit Hardware Configuration dialog box, 23, 55
- Edit Host PC Entry dialog box, 103
- Edit menu (Terminal window), 161
- Edit menu (Windows application), 161
- Edit Online Service Entry dialog box, 134
- editing
 - ACS hardware configuration, 68–70
 - AUTOEXEC.BAT file, 49
 - clipboard, 161
 - custom modem hardware configuration, 73–74
 - gateway settings, 79
 - Interrupt 14 hardware configuration, 62–64
 - leased line hardware configuration, 60–62
 - modem hardware configuration, 54–56
 - NASI/NCSI hardware configuration, 68–70

- editing (*continued*)
 - network node hardware configuration, 65–67
 - null modem hardware configuration, 59
 - online service directory, 134–135
 - PATH statement, 49
 - Telebit ACS hardware configuration, 71–72
 - Terminal window text, 161
 - translation tables, 131
 - editor, 202
 - electronic registration, 36
 - encryption, 28, 89
 - END SESSION command (Host/Remote Online Menu), 146, 147
 - ending
 - online service session, 164
 - remote control session, 146–147
 - end-of-file character, 255
 - environment variable, 49
 - error correction, 220
 - error detection, 220
 - error messages, 253–260
 - even parity, 220
 - exit
 - File Manager, 170
 - gateway, 80
 - host, 115
 - online service session, 164
 - remote control session, 146–147
 - EXIT command (File Manager File menu), 170
 - EXIT command (Terminal window File menu), 164
 - external modem, 208, 213
- F**
- file compression, 186
 - enabling, 187
 - file details, 186
 - file management using pcANYWHERE File Manager, 177–185
 - File Manager, 169–187
 - exiting, 170
 - file and directory management, 177–185
 - navigation and file selection techniques, 170–172
 - starting, 169
 - window, 170
 - File menu (File Manager), 183
 - File menu (Terminal Window), 192
 - File menu (Terminal window), 160, 164
 - file transfer
 - automatic downloading using ZMODEM, 167
 - between PC and online service, 164–168
 - between remote and host, 169–187
 - disconnect after completion, 174
 - drag-and-drop, 173, 174
 - file overwrite preferences, 186
 - host to remote, 174
 - interrupted, 186
 - modem speed, 211
 - new features, 27
 - PC-to-PC, 169–187
 - remote to host, 173–174
 - setting options, 187
 - speed, 175, 213
 - using Windows Clipboard, 175
 - FILE TRANSFER command (Host Online Menu), 174
 - FILE TRANSFER command (Remote Online Menu), 169, 174
 - FILE TRANSFER OPTIONS... command (File Manager Configure menu), 187
 - File Transfer Options dialog box, 187
 - file transfer protocol
 - changing, 164, 165–166
 - common types, 135
 - selecting, 135
 - File Transfer Protocol dialog box, 166
 - file transfer protocol
 - See also* protocols, 168
 - File Transfer Status dialog box, 174

- filenames
 - configuration files, 29
 - long, 28
 - files
 - copying locally, 180–181
 - deleting, 178–179
 - deselecting, 172
 - filtering, 185–186
 - managing, 177–185
 - overwriting during file transfer, 186
 - personal, 39, 44
 - renaming, 179–180
 - selecting for online service file transfer, 167
 - selecting in File Manager, 171
 - sending, 164–168, 169–187
 - shared, 39
 - sorting, 185–186
 - system, 36
 - FILTER... command (File Manager View menu), 184
 - Filter dialog box, 184
 - filtering files by type, 185
 - filters, using to select files in File Manager, 184
 - flow control, 222
 - changing during online service session, 162
 - definition, 213
 - explanation, 213
 - hardware, 213, 214
 - setting, 58, 222
 - software, 214
 - Font dialog box, 132
 - font size, 164
 - fonts
 - local, 100
 - remote control session, 100
 - Terminal window, 128, 132, 162
 - full-screen display, 100, 153
- G**
- gateway, 75–80
 - activating, 79–80
 - automatic connection, 103
 - bidirectional, 27, 75, 76
 - canceling, 80
 - class, 66, 78, 79
 - configuring, 75–80
 - definition, 20, 75
 - diagram, 76
 - grouping, 78
 - incoming configuration, 75, 76, 78
 - loading, 79–80
 - loading into high memory, 78
 - modifying settings, 79
 - name, 66
 - options, 78
 - outgoing configuration, 75, 76, 78
 - parity, 67
 - selecting, 121, 139
 - setting up, 66
 - starting, 79–80
 - unidirectional, 75, 76
 - using, 65
 - to call online service, 139–140
 - to conduct remote control session, 120–123
 - GATEWAY... command, 77
 - Gateway group box options, 66
 - GENERAL... command, 85
 - general configuration files, 40
 - graphics
 - copying, 161
 - detection in DOS application, 91
 - display problems, 264
 - representation in DOS application, 152
 - support, 100
 - transferring between host and remote, 175
 - transferring to online service, 161
 - grouping gateways, 78

H

- HARDWARE... command, 161–162
- hardware configuration, 53–74
 - ACS, 67–72
 - changing settings during online session, 161
 - Custom Modem, 73–74
 - description, 58
 - direct serial connection, 59
 - explanation, 20
 - file conversion from 1.0, 28
 - gateway, 75–79
 - Interrupt 14, 62–64
 - leased line, 59–62
 - modem, 53–64, 221–223
 - NASI/NCSI, 67–70
 - network, 64–73
 - node, 65–67
 - null modem, 57–59
 - online service, 222
 - problems creating or editing, 65
 - selecting for online service, 135
 - serial, 53–64
 - standalone PC, 53–59
 - Telebit ACS, 70–72
- hardware configuration file (AWuserid.HW6), 40
- hardware flow control, 213, 214
- hardware interrupt, 208
- hardware requirements, 17
- Hardware Settings dialog box, 162
- hardware setup. *See* hardware configuration
- Hayes AT Command Set, 211
- Hayes Compatible setting, 221
- Hayes Smartmodem 2400 setting, 221
- Hazeltine 1500 terminal emulation, 235
- Help menu, 51
- hexadecimal conversion table, 252
- Host & Remote Session Log Report dialog box, 204
- Host Accepts Another Call check box, 146
- Host [Disabled] icon, 114
- Host General Options dialog box, 86, 87
- host log file, 201
- host main window, 109
- host mode
 - allowing caller to change, 95
 - changing, 146
- Host Online Menu, 144, 158
 - hotkey, 92, 147
 - opening from DOS TSR, 147
 - options available to both host and remote user, 144–147
 - options available to host user, 158
- HOST OPERATION command, 85, 87, 90
- host options, 85–92
 - changing while connected, 152
- host PC
 - adding, 102
 - allowing caller to change host mode, 95
 - blanking screen, 89
 - calling, 117
 - canceling, 115
 - configuring, 85–92
 - contrasted to remote PC, 18
 - creating list of hosts to call, 102–103
 - disabling, 114, 147
 - explanation of, 18
 - initiating remote control session, 109–113
 - load automatically, 87
 - locking, 88
 - methods used to load, 108
 - minimize when waiting, 87
 - OLE operation, 226
 - Quick Start setup, 23–27
 - rebooting, 156
 - removing from memory, 115
 - starting, 107–116
 - waits for call, 108–109
- host report of remote connections, 203
- Host Security Options dialog box, 88–90
- hotkey
 - default, 147
 - specifying, 92

I

I/O (input/output) port address, 208
 IBM terminal emulation, 235–236
 ID
 administrator, 39
 user, 40
 importing
 recorded session data into other application, 200
 screen captures into other applications, 200
 inactivity timeout
 enforcing, 96
 length, 89
 incoming configuration, 76, 77
 incoming gateway, using, 120–122
 individual privileges, 97
 initialization string. *See* modem initialization string
 Install Program Files To dialog box, 35
 installation
 administrative, 38–47
 customizing, 48
 installing
 from DOS prompt, 42
 on a LAN, 38–47
 on network workstation, 47
 on a standalone PC, 33–37
 uninstalling, 48
 from Windows, 41–42
 Int 14. *See* Interrupt 14
 internal modem, 208, 213
 interrupt. *See* IRQ
 Interrupt 14
 advanced options, 64
 data rates supported, 63
 hardware configuration, 62–64
 interruption of file transfer, 186
 IRQ, 55
 explanation, 208

K

Kermit file transfer protocol, 135
 key. *See* hotkey; keyboard handlers; Windows system keys
 key combinations, 128
 key handler, 154
 keyboard
 control, 87
 disabling on host during session, 152
 disabling on remote during session, 158
 file selection in File Manager, 170–172
 locking, 158
 mapping for terminal emulation, 229
 problems, 264
 keyboard handlers
 allowing, 95
 levels, 153–154
 specifying, 99
 types, 153–154
 types of, 92

L

LAN, 20
 hardware configuration, 64–73
 installation, 38–47
 off-LAN connection, 64
 Quick Start PC connection, 25
 laptop, 18
 LASTDRIVE= statement, 105
 leased line
 advanced options, 61
 definition, 59
 hardware configuration, 60–62
 technical information, 217–218
 testing, 218
 use with modems, 217
 license files, 44
 licensing your copy of Norton pcANYWHERE for Windows, 34, 42
 line noise, 220
 line wrap, 127, 163
 load buttons. *See* entries for specific buttons

- loading
 - DOS Host TSR, 115–116
 - DOS Host TSR into high memory, 92
 - gateway, 79–80
 - gateway into high memory, 78
 - host PC, 108
 - host PC with Windows, 87
 - pcANYWHERE with Windows, 157
 - program modules, 30
 - remote PC, 116
 - local area network. *See* LAN
 - Local Copy button, 180
 - LOCAL COPY... command (File Manager File menu), 180
 - local fonts, 100
 - locking
 - host, 88
 - host's keyboard and mouse, 152
 - remote's keyboard and mouse, 158
 - log file, 21
 - creating report from, 202–205
 - enabling, 89, 136
 - host, 201
 - remote, 200
 - log reports, 202–205
 - archiving, 205–206
 - deleting, 205–206
 - logging
 - connection attempts, 21, 89
 - enabling, 136
 - enabling on host, 201–202
 - enabling on remote, 201
 - session data, 200–206
 - login attempts, maximum allowed, 90
 - login name
 - See also* log-on procedures, online service assigning, 97
 - conflicts, 89
 - defining, 93
 - entering, 117, 121, 123
 - requiring, 88
 - log-on procedures, online service, 138
 - See also* login name
 - long filename support, 28
- ## M
- macro keys, 128
 - creating, 129
 - enabling, 136, 163
 - functions, 129
 - types, 129
 - Macro Keys dialog box, 129
 - macros
 - See also* macro keys; Norton Assistant Norton Assistant, 51
 - predefined, 51
 - main window, 30
 - mainframe. *See* online service session
 - Make Dir button, 178
 - MAKE DIR... command (File Manager File menu), 177, 178
 - Make Directory dialog box, 178
 - managing
 - directories and files using pcANYWHERE File Manager, 170–187
 - personal and shared data files, 44
 - Manual modem, 56, 73, 221
 - Map button, 150
 - mapping drives, 104–106, 149–151
 - mark parity, 220
 - master password, 82, 83
 - MCI Mail, 19
 - memory
 - conserving, 91
 - requirements, 17
 - menu bar, 30
 - menu commands. *See* entries for specific menu commands
 - menus. *See* entries for specific menus
 - messages
 - error, 253–260
 - Microsoft Windows. *See* Windows
 - minimize host when waiting for call, 87
 - .MK6 file extension, 128

- modem, 210
 - advanced options, 57
 - cables, 215
 - Custom, 221
 - custom settings, 73–74, 221
 - data compression, 211, 222
 - default settings, 54, 55, 73
 - definition, 19
 - external, 208, 213
 - hardware configuration, 54–57
 - Hayes-compatible command mode, 211
 - how it works, 210
 - interaction with PC, 213–216
 - internal, 208, 213
 - leased line compatibility, 60, 217
 - Manual, 56, 73, 221
 - not supported, 73
 - recommended settings, 212
 - selecting, 55
 - sharing, 62
 - specifying, 38
 - speed, 210–211
 - switch settings, 212
 - troubleshooting, 261–263
 - modem cable selection, 215
 - modem commands, 211
 - modem connection, Quick Start setup, 23–27
 - modem does not respond, 257, 261
 - modem hardware configuration, 53–64, 221–223
 - connection detection, 222
 - creating, 54–57
 - custom, 73–74
 - dialing instructions, 222
 - hardware settings, 222
 - modem initialization string, 56, 73, 212, 221
 - what it does, 211
 - modem options
 - advanced, 57
 - customizing, 73
 - setting, 55
 - modem port, specifying, 38
 - modem settings
 - default, 54, 55, 73
 - recommended, 212
 - modem switches, setting, 212
 - monitor, 91
 - See also* display; screen
 - monochrome attribute translation, 100
 - mouse
 - control, 87
 - disabling on host during session, 152
 - disabling on remote during session, 158
 - drag-and-drop file transfer, 173, 174
 - use in DOS applications, 91
 - use in Windows applications, 15
 - multiplexers, 59, 217, 218, 218–220
 - remote-to-remote test, 219
 - MUX, 217, 218, 218–220
- ## N
- NACS, 67
 - naming your computer, 38, 82
 - NASI-compliant ACS, 67
 - NASI/NCSI, 65
 - hardware configuration, 67–70
 - support for, 18
 - NASI/NCSI Port Selection dialog box, 69
 - navigation and selection techniques
 - File Manager window, 170–172
 - Windows, 15
 - NetBIOS, 65
 - support for, 18
 - NetWare IPX, 65
 - shell, 263
 - support for, 18
 - version required, 262
 - network, 47
 - See also* LAN
 - automatic connection, 103
 - communications device, 66
 - device drivers, 65
 - restricting access using unidirectional gateway, 77

- network connection, 20
 - automatic, 103
 - device, specifying, 68
 - NetWare, 66
 - Quick Start, 25–27
 - Network Customization dialog box, 39
 - network driver
 - specifying, 38
 - network hardware configuration, 64–73
 - network installation, 38–47
 - default settings, 39
 - from DOS prompt, 42
 - from Windows, 41–42
 - network node
 - advanced options, 67
 - hardware configuration, 65–67
 - network protocol support, 18
 - new features in version 2.0, 27–28
 - no carrier, 257
 - no connection, 257
 - No Modem (Direct Connect) button, 58
 - node
 - definition of, 65
 - hardware configuration, 65–67
 - Norton Assistant, 28, 30, 50, 51, 52
 - Norton pcANYWHERE Editor, 202
 - Norton pcANYWHERE for DOS, 152
 - command-line arguments, 224
 - Norton pcANYWHERE for Windows
 - command lines, 223–226
 - compatibility with version 1.0, 28
 - configuring for your modem or network, 53–74
 - File Manager, 169–187
 - functions, 30
 - gateways, 75–80
 - hardware requirements, 17
 - installing on a network, 38–47
 - installing on a PC, 33–35
 - license information, 34
 - new features, 27–28
 - OLE support, 226
 - online service session, 125–142
 - Norton pcANYWHERE for Windows
 - (*continued*)
 - program group, 36
 - program modules, 30
 - remote control session, 107–123
 - remote control session management, 143–159
 - starting, 37–38, 50
 - uninstalling, 48
 - utilities, 189–206
 - what it does, 17
 - Novell Asynchronous Communications Server. *See* NACS; NASI/NCSI
 - Novell Asynchronous Services Interface. *See* NASI; NASI/NCSI
 - Novell NetWare. *See* NetWare IPX
 - null modem cable, 57, 213
 - See also* direct connection
 - data-transfer speed, 213
 - definition, 20
 - explanation, 216
 - pin configuration, 216, 219
 - what it does, 57
 - numbers, conversion of decimal to hex, 252
- O**
- Object Linking and Embedding. *See* OLE
 - OEM character set, 251
 - off-LAN connections, 65, 75
 - Offline Menu, 114
 - OLE
 - support for, 28, 226
 - online menu. *See* Host Online Menu; Remote Online Menu
 - online service, 19
 - calling, 137–138
 - difficulty connecting, 222
 - list of, 133–135
 - Online Service Directory, 134
 - online service session
 - advanced settings, 135–137
 - automating, 159
 - configuration files, 28

online service session (*continued*)
 configuring, 125–137
 contrasted to remote control session, 19
 ending, 164
 logging, 200–206
 OLE operation, 226
 playback, 22, 193–196
 printing, 160
 recording, 136, 192–193
 running scripts, 159
 starting, 137–138

online service session configuration file
 (AWuserid.OS6), 40

Online Settings dialog box (host), 158

Online Settings dialog box (remote), 148

ONLINE SETTINGS... command (Host Online
 Menu), 158

ONLINE SETTINGS... command (Remote Online
 Menu), 148–154

opening
 File Manager, 169
 Host Online Menu, 144, 158
 Remote Online Menu, 144
 during full-screen display, 153

outgoing configuration, 76, 77

outgoing gateway
 using, 122–123
 using to call online service, 139–140

overwriting files during file transfer, 186

P

parity, 222
 changing during online service session,
 162
 CompuServe, 67
 even, 220, 221
 mark, 220, 221
 none, 221
 odd, 220, 221
 selecting for gateway, 67
 setting, 58
 space, 220, 221

parity-checking error detection, 220

parity settings, 221

password
 allow any to reconnect, 88
 assigning, 97
 default, 94
 defining, 94
 entering, 109, 117, 121, 123
 individual caller, 97
 master, 82, 83
 requiring, 83
 setting case-sensitivity, 89
 supervisor ID, 46

path
 adding pcANYWHERE directory, 49
 personal configuration files, 39, 44
 shared configuration files, 39

PATH statement, editing, 49

PC, 18
See also host PC; remote PC
 comparison of host and remote, 18
 installing for single user, 33
 interaction with modem, 213–216
 naming, 38, 82
 remote-only operation, 48

PC-to-PC connection, 57

pcANYWHERE. *See* Norton pcANYWHERE for
 DOS; Norton pcANYWHERE for Windows

pcANYWHERE Translation Tables dialog box,
 131

pcANYWHERE Waiting... dialog box, 26, 110

personal configuration files, 29, 39–41, 44
 creation of, 40

personal ID code, 40

phone number. *See* telephone number

pin configuration
 null modem cable, 216
 serial connector, 214

PKZIP files, 186

Playback Control Panel dialog box
 displaying, 196
 enabling, 194
 options, 194–195

Playback Options dialog box, 194–195

PLAYBACK SESSIONS/SCREENS... command, 189, 193, 196, 198, 199

playing back recorded sessions, 193–196

pool, select by, 70, 72

port, 38

- See also* COM port; modem port; serial port
- addresses, 207, 208
- modem, 38
- not available, 258
- select by, 71, 72
- selecting for ACS, 69
- selecting for Telebit ACS, 72

prefix

- creating, 84
- definition, 83
- enabling, 97
- selecting, 134
- using, 134

PREFIX/SUFFIX... command, 84

Prefix/Suffix dialog box, 84

PRINT ONLINE command, 160

PRINT SCREEN command, 160

printer

- changing while connected, 266

printer output destination, 99, 149

printer setup, 149

printing, 148

- captured screens, 200
- online service session, 160
- Terminal window contents, 160
- troubleshooting, 265

privileges, 21

- configuration files, 44
- default, 93–96
- individual, 92, 97

program directory, specifying, 34

program group, creation of, 36, 47

protecting shared files, 39

PROTOCOL... command (Terminal window Transfers menu), 164, 165

protocols

- protocols. *See also* file transfer protocol

protocols (*continued*)

- changing, 164, 165–166
- data compression, 211
- support for, 18

Q

Quick Connect, 21

- calling host, 118–120
- calling online service, 141
- calling remote from host, 112–113
- saving dialog box settings, 113, 120

Quick Connect: Be A Host PC dialog box, 112

Quick Connect... button, 112

Quick Connect: Call A Host PC dialog box, 119

Quick Connect: Call Online Service dialog box, 141

Quick Start, 23–27

- modem connection, 23–24
- network connection, 25–27

quit

- See also* exit
- online service session, 164
- remote control session, 146–147

R

raw data file, saving recorded session to, 197

.RCD file, 190, 193, 194

reboot

- after remote control session, 86
- allowing, 95
- configuring, 86
- host from remote, 156

REBOOT HOST command (Remote Online Menu), 156

receiving files. *See* downloading files, file transfer

record file, 22, 190

- capturing screen shots from, 198–199
- playback, 193–196
- saving as ASCII file, 196
- selecting, 194

- recording
 - online service session, 136, 192–193
 - remote control session, 189–191
 - script, 136
- RECORDING command (Terminal window File Menu), 192
- RECORDING ON/OFF command (Remote Online Menu), 190, 191
- REGEDIT program, 227
- register, select by, 71, 72
- registering
 - by mail or fax, 37
 - electronically, 36
- remote caller inactivity timeout, 96
- remote control session
 - changing session options, 143–159
 - configuring, 81–106
 - contrasted to online service session, 19
 - ending from host, 146–147
 - ending from remote, 146
 - explanation, 18
 - file transfer operations, 169–187
 - initiating from host PC, 109–113
 - initiating from remote PC, 116–120
 - logging, 200–206
 - PC-to-PC, 23–27
 - playing back, 193–196
 - Quick Start, 23–27
 - recording, 189–191
 - resuming after suspension, 156
 - starting, 107–123
 - time allowed, 96
 - using gateway, 120–123
- remote control session configuration file (AWuserid.PC6), 40
- Remote Drives dialog box, 105, 150
- remote log file, 200
- remote main window, 102
- remote mouse
 - allow use in DOS applications, 91
 - disabling, 158
- Remote Online Menu, 144, 147–157, 190
 - accessing during full-screen display, 153
 - Remote Online Menu (*continued*)
 - opening when Control-menu box unavailable, 153
 - options available to both host and remote user, 144–147
 - options available to remote user, 147–157
- REMOTE OPERATION... command, 98, 101
- remote options, 99–100
- remote PC
 - calling, 110
 - changing settings online, 147–157
 - configuring, 98–100
 - contrasted to host PC, 18
 - explanation, 18
 - initiating remote control session, 116–120
 - OLE operation, 226
 - online settings, 147–157
 - Quick Start setup, 23–27
 - starting, 116
 - waits for call, 117–118
- remote report of host connections, 202
- remote user, definition, 18
- removing
 - gateway from memory, 80
 - host from memory, 115
 - pcANYWHERE from your computer, 48
- Rename button, 179
- RENAME... command (File Manager File menu), 179
- Rename dialog box, 179
- renaming files and directories, 179–180
- request to send, 213, 214, 222
- requirements to run Norton pcANYWHERE for Windows, 17
- restricting a PC to remote-only operation, 48
- RESUME SESSION command (Remote Online Menu), 156
- resuming suspended session, 156
- REVERSE TAGS command (File Manager Tag menu), 172
- RS-232-C, 214–216, 222
- RTS, 213, 222

- running
 - pcANYWHERE, 37–38
 - REGEDIT program, 227
 - script, 136, 159
- S**
- SAVE SCREEN AS ASCII command (Terminal window's File menu), 200
- SAVE SCREEN command (Remote Online Menu), 190, 198
- SAVE SCREEN command (Terminal Window's File Menu), 198
- Save Screen Control Panel button, 199
- saving
 - Quick Connect settings, 113, 120
 - recorded session to file, 196–197
 - screen captures, 197–199
- .SCN file, 194, 197
- screen, 91
 - See also* display
 - allow blanking, 95
 - blanking, 89, 152, 158
 - capturing, 21, 197–199
 - printing, 160
 - refresh rate, 91, 92
 - reviewing saved images, 198–199
 - wrapping, 127, 163
- screen file, 22
- screen scan, 91
- screen shots, 197–200
 - printing, 200
 - saving, 197–199
 - saving as ASCII files, 200
 - viewing, 199–200
- script, 22, 159
 - See also* Creating Norton pcANYWHERE
 - Scripts
 - recording automatically, 28, 136
 - running, 136
 - selecting, 159
 - starting, 159
- SCRIPTS command, 159, 189
- Scripts dialog box, 159
- scroll bars, 128, 164
- scrolling display, 163
- SECURITY... command, 87
- security features, 82–83, 87–90
- Select by Pool, 70, 72
- Select by Port, 71, 72
- Select by Register, 71, 72
- Select Macro Key File dialog box, 128
- Select Playback File dialog box, 194
- Select Raw Data File dialog box, 197
- Select Recording File dialog box, 190
- Select Some dialog box, 172
- Select Translation File dialog box, 130
- Select When Connecting check box, 69
- selecting
 - ACS server, service, and port, 69
 - cables for serial connections, 215
 - COM port, 38, 55, 58
 - directory, 35, 43
 - drive, 35, 43
 - drive in File Manager, 170
 - file overwrite preference, 187
 - file transfer protocol, 135
 - files in File Manager, 167, 171
 - gateway, 121
 - gateway options, 78
 - incoming and outgoing gateway configurations, 78
 - modem from list, 55
 - network communications device, 66, 68
 - network driver, 38
 - online service from list, 137
 - online service hardware configuration, 135
 - prefix, 134
 - program directory, 34, 35
 - record file for playback, 194
 - record file for recording, 190
 - screen file to view, 198–199
 - script to run, 159
 - suffix, 134
 - terminal emulation, 135
- Send button, 173

- SEND command (File Manager File menu), 173
- sending files. *See* file transfer, uploading files
- serial board, 208
- serial connection
 - cable selection, 214
 - definition, 19
- serial hardware configuration. *See* modem hardware configuration
- serial port, 207
 - addressing, 207
 - interrupt handling, 209
 - specifying, 38
 - technical information, 207–223
 - use for modem, 208
- server
 - selecting for ACS, 69
 - selecting for Telebit ACS, 72
- service
 - selecting for ACS, 69
 - selecting for Telebit ACS, 72
- session. *See* online service session; remote control session
- session configuration
 - explanation, 21
- session icon, 144
- Session menu (Terminal window), 160–163
- setting
 - data rate, 58
 - default caller privileges, 93–96
 - flow control, 58
 - individual privileges, 97
 - parity, 58
- setup, 27
 - See also* hardware configuration
 - Quick Start, 23–27
- shared configuration files, 29, 39–41, 44
 - creating, 45
 - protecting, 39
- sharing modems, 62, 75
- single-user installation, 33–36
- Smart Setup, 27
- Smart Setup dialog box, 38, 54
- software flow control (XON/XOFF), 214
- software requirements, 17
- sorting files in File Manager, 185–186
- source directory, 166
- source files, 174
- space parity, 220
- special keyboard handlers
 - allowing, 95
 - levels, 153–154
 - specifying, 99
 - types, 92, 153–154
- specifying
 - COM port, 38
 - network connection device, 68
 - network driver, 38
 - program directory, 43
 - special keyboard handler, 99
- speed
 - computer, 222
 - data transfer, 210, 221
 - file transfer, 175
 - modem, 210–211
 - screen refresh, 91, 92
- starting
 - DOS TSR from command line, 115–116
 - File Manager, 169
 - gateway, 79–80, 121–123
 - host with Windows, 87
 - online service session, 137–138
 - pcANYWHERE, 37–38
 - for the first time, 50
 - remote control session
 - from host, 107–116
 - from remote, 116–120
- startup files
 - AUTOEXEC.BAT, 36, 44, 47, 49, 105, 157
 - changes to, 36, 47
 - SYSTEM.INI, 43, 47
 - WIN.INI, 36, 47
- status bar, 164
- status line display, 128
- suffix
 - creating, 84
 - definition, 83

- suffix (*continued*)
 - enabling, 97
 - selecting, 134
 - using, 134
 - supervisor ID, 39
 - password-protection, 46
 - supported network protocols, 18
 - switches, modem, 212
 - switching
 - between window mode and full-screen display, 153
 - from data to voice, 155
 - from voice to data, 111, 118
 - Sync button, 182
 - SYNCHRONIZE... command (File Manager File menu), 182
 - Synchronize Directory dialog box, 183
 - synchronizing
 - directories, 182–184
 - screen display, 153
 - syntax, 225
 - system files
 - AUTOEXEC.BAT, 36, 44, 47, 49, 105, 157
 - changes performed by pcANYWHERE, 36, 47
 - SYSTEM.INI, 36, 43, 47
 - WIN.INI, 36, 47
 - SYSTEM HARDWARE... command, 53–74
 - system messages, 253–260
 - SYSTEM SETUP... command, 82
 - System Setup dialog box, 82
 - SYSTEM.INI, 47
 - modification by install program, 36, 43
 - Windows drivers, 48
- T**
- TAG ALL command (File Manager Tag menu), 171
 - TAG BY... command (File Manager Tag menu), 172
 - TAG DIRS command (File Manager Tag menu), 172
 - TAG FILES command (File Manager Tag menu), 171
 - Tag menu (File Manager), 171–172
 - target directory, 166
 - TCP/IP, 65, 73
 - support for, 18
 - TCP/IP... command button, 100, 101
 - TCP/IP host
 - adding, 100, 101
 - specifying, 100
 - TCP/IP Setup dialog box, 101
 - technical support using pcANYWHERE, 19
 - Telebit ACS, 65
 - hardware configuration, 70–72
 - port selection, 70
 - pool, 72
 - port, 72
 - register, 72
 - support for, 18
 - Telebit Asynchronous Communications Server. *See* Telebit ACS
 - telephone lines, technical information, 217–221
 - telephone number
 - entering in modem initialization string, 212
 - online service, 135
 - prefix/suffix list, 83
 - remote PC, 110
 - Telephone Setup dialog box, 37
 - Teletext terminal emulation, 236–240
 - TERMINAL... command, 162
 - terminal emulation, 126–128
 - See also* entries for specific terminal emulation types
 - ADDS Viewpoint, 230
 - ADM 3A, 230–231
 - changing during session, 162
 - common types, 135
 - configuring, 126–128
 - DG 100/200, 232–234
 - IBM, 235–236
 - macro keys, 128

- terminal emulation (*continued*)
 - reference, 229–252
 - selecting, 135
 - Teletype, 236–240
 - types, 230–249
 - Viewpoint, 230
 - VT 52, 243–244
 - VT 100/102/220, 240–242
 - Wyse, 244–246
 - X3270, 247–249
 - TERMINAL EMULATIONS... command, 126
 - Terminal Settings dialog box, 162
 - Terminal window, 137
 - adjusting display, 162
 - changing font and color, 132
 - display options, 127, 128
 - enabling scroll bars, 164
 - enabling status bar, 164
 - printing, 160
 - text
 - copying, 161
 - transferring between host and remote, 175
 - transferring to online service using clipboard, 161
 - text editor, 202
 - time allowed to log in, 90
 - timeout
 - enforcing, 96
 - gateway, 78
 - specifying length, 89, 90
 - TRANSFER CLIPBOARD... command (remote's Control-menu box), 175
 - Transfer Clipboard dialog box, 175
 - transferring clipboard contents
 - between host and remote, 175
 - to online service, 161
 - transferring files
 - between PC and online service, 164–168
 - between two PCs, 169–187
 - Transfers menu (Terminal window), 164, 165
 - Translation Table dialog box, 131
 - translation tables
 - ASCII control character set, 250
 - codes, 249
 - configuring, 130–131
 - definition, 130
 - editing, 131
 - enabling, 136, 163
 - OEM character set, 251
 - Transmission Control Protocol/Internet Protocol. *See* TCP/IP
 - transmission errors, 220
 - .TRN file extension, 130
 - troubleshooting
 - using pcANYWHERE, 18
- ## U
- UART, 209–210
 - unidirectional gateway, 76
 - what it does, 75
 - uninstalling Norton pcANYWHERE for Windows, 48
 - universal asynchronous receiver transmitter. *See* UART
 - unmapping drives, 106, 151
 - uploading files
 - allowing, 96
 - file selection, 168
 - to online service, 164–168
 - remote to host, 173–174
 - Use Gateway check box, 66
 - Use Modem button, 55
 - user, difference between host and remote, 18
 - user ID, 40, 41, 49
 - User ID dialog box, 40
 - Utilities menu, 189–206
 - ACTIVITY LOG PROCESSING... command, 189, 203–206
 - PLAYBACK SESSIONS/SCREENS... command, 189, 196, 198, 199
 - SCRIPTS command, 189

V

- video driver error, 255
- video. *See* display, screen
- viewing
 - screen shots, 199–200
- viewing clipboard, 176–177
- Visual Basic OLE functionality, 227
- VOICE command (Remote Online Menu), 155
- voice communications, 210
- voice confirmation, 111, 118
- Voice First button, 111, 118
- VOICE FIRST command (Offline Menu), 115
- VT 52 terminal emulation, 243–244
- VT 100/102/220 terminal emulation, 135, 240–242

W

- WAIT FOR A CALL command (Offline Menu), 115
- Wait for Call button, 109
- waiting for call
 - host PC, 108–109
 - remote PC, 117–118
- Waiting... dialog box, 26, 110
- warm boot, 86, 156
- wildcards, using to select files for File Manager
 - operations, 184
- WIN.INI, 47
 - DOCUMENTS= line, 185
 - modification by install program, 36
- WINAW command line syntax, 225
- WINAW directory
 - adding to path, 49
 - specifying at installation, 34
- window
 - chat, 145–146
 - File Manager, 170
 - host, 109
 - main, 30
 - remote, 102
 - Terminal, 137

Windows

- load automatically, 157
- serial port IRQs, 55
- startup files, changes to, 47
- system key execution, 99, 154–155
- Windows Clipboard. *See* clipboard
- Windows System Key Pressed dialog box, 155, 177
- Winsock, support for, 18, 28
- workstation installation, 47
- wrap, 127, 163
- Wyse terminal emulation, 244–246

X

- X3270 terminal emulation, 247–249
- XMODEM file transfer protocol, 135
- XON/XOFF, 214

Z

- ZMODEM file transfer protocol, 135, 166
 - auto download option, 167