

Using Norton pcANYWHERE™ for DOS



Using Norton pcANYWHERE™ for DOS

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

Conventions	15
-------------------	----

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
Other Features	22
Quick Start	23
Connecting Via Modems	23
Connecting Over a LAN	26
What's New in Version 5.0?	29
For Users of Earlier Versions of pcANYWHERE	30
Converting pcANYWHERE Version 4.5's Configuration Files	30
Command-Line Options	32

Chapter 2 Installation and General Setup

Standard Installation	36
Host Installation for Windows	37
Installing Norton pcANYWHERE on a LAN	39
Uninstalling Norton pcANYWHERE for DOS	44
Adjusting Your AUTOEXEC.BAT File	45
Getting Around in Norton pcANYWHERE for DOS	46
Adding Options to a Menu	51
Selecting a Pathname from a Form	52
Naming Your PC	53
Security	54
Creating a Telephone Prefix and Suffix List	54
If You Have Snow... ..	55
Customizing Display Colors	56

Chapter 3 Hardware Configurations

Creating Serial Hardware Configurations	60
Creating a Modem Hardware Configuration	60
Creating a Direct Serial Hardware Configuration	62
Creating an Interrupt 14 Hardware Configuration	64
Creating Network Hardware Configurations	65
Creating a Node Hardware Configuration	66
Creating ACS Hardware Configurations	68
Using a Telebit ACS	71
Using a Custom Port	73
Customizing the Command Set for your Modem	74
Managing Hardware Configurations	75

Chapter 4 Gateway Configurations

Gateway Concepts	78
Setting Up a Gateway	79
Specifying a Timeout for Inactivity	81
Determining How Often the Gateway Accesses the CPU	81
Assigning a Gateway to a Class	82
Giving the Gateway a Direction	82
Loading the Gateway into High Memory	82
Modifying the Gateway Setup	82
Starting a Gateway	83
Deactivating the Gateway	84

Chapter 5 Session Configurations and Remote Preferences

Creating or Modifying Session Configurations	86
Choosing or Changing the Hardware Configuration	89
Supplying the Telephone Number	90
Providing the Host's Name and Password	90
Mapping Drives	91
Choosing or Changing the Emulation Type	92
Choosing or Changing the File-Transfer Protocol	94
Specifying Macro Keys	94
Using a Translation Table	95
Setting Preferences for the Remote PC	97
Selecting a Hotkey	101
Selecting a Printing Device	102
File Transfer Preferences for Remote Control Sessions	103
Mouse Preferences for Remote Control Sessions	106
Display and Keyboard Preferences for Remote Control Sessions	108

Swap File Size for Remote Control Sessions	111
Setting Protocol Preferences for Online Sessions	111

Chapter 6 Caller Information and Host Preferences

Creating or Modifying Caller Information Configurations	120
Setting a Password for a Remote User	121
Allowing the User to Blank the Host Screen	122
Allowing the User to Reboot the Host	122
Allowing the Use of Ctrl+Break and Ctrl+C	122
Allowing the Use of Keyboard Handlers	123
Allowing the User to Change the Host Mode	123
Ending the Session Because of Inactivity	123
Specifying a Time Limit for the Session	124
Executing a Command Automatically	124
Securing Host Drives	124
Calling the Remote User Back	125
Defining Default Caller Information	126
Setting Host Preferences	127
Features Preferences	128
General Preferences	132
Security Preferences	134

Chapter 7 Remote Control Sessions

Starting the Host PC	143
Waiting for a Remote PC to Connect	144
Initiating the Session from the Host PC	146
Starting a Session with Voice Communication	148
Using the Host Hotkey to Change Host Modes	150
Using Quick Connect on the Host PC	151
Using a DOS Command to Start the Host PC	153
Canceling the Host TSR	153
Starting the Remote PC	154
Initiating the Session from the Remote PC	154
Choosing a Host PC or Gateway on a LAN	155
Waiting for a Host PC to Connect	156
Using Quick Connect on the Remote PC	157
Using a DOS Command to Start the Remote PC	159
Managing the Remote Control Session	160
Chatting with the Other User	161
Changing the Destination for Printed Output	162
Ending the Session	163
Special Options for the Host User	164
Session Options Available Only to the Remote PC	166

Transferring and Managing Files and Directories	174
Using the File Transfer Program	175
Background File Transfer	183
Transferring Files from the DOS Command Line	183
Using Automated Procedures	185
Creating and Modifying an Automated Procedure	185
Creating and Modifying an Operations File	190
Executing an Automated Procedure	194

Chapter 8 Online Sessions

Initiating the Session or Waiting to Connect	197
Using a DOS Command to Start the Remote Program	199
Using Quick Connect	199
Managing the Online Session	201
Sending a Break Signal	202
Ending the Session	202
Accessing Your PC During a Session	202
Monitoring Control Codes	203
Printing	203
Clearing the Screen	204
Changing Terminal Settings	204
Transferring Files	211

Chapter 9 Utilities

Checking Your Hardware	215
Reviewing the DOS Environment	216
Reviewing Configuration Files	216
Testing Your Hardware Configurations	217
Testing Your Video Adapter	219
Testing Your Keyboard	220
Recording Sessions	221
Playing Back Recorded Sessions	223
Saving Screen Shots	227
Displaying Screen Shots	228
Logging Remote Control and Online Sessions	230
Creating Log Reports	232
Deleting and Archiving Logged Information	237

Appendix A Technical Information

The Role of the PC	239
Serial Port Addressing	239
Hardware Interrupts	240
UARTs	241

The Role of the Modem	242
Speed	242
Data Compression	243
Modem Commands	243
Modem Switches	243
Using the PC and the Modem Together	245
Data Rate	245
Standard Serial Cables (RS-232-C)	246
Null Modem Cable	247
Special Telephone Lines	248
Error Detection and Correction	252
Options in Serial Hardware Configurations	253
Miscellaneous Options	254

Appendix B Terminal Emulation

Terminal Emulation Keys	257
ADDS Viewpoint	258
ADM 3A	258
ANSI	260
DG 100/200	260
Hazeltine 1500	264
IBM 3101	264
Teletype 912/920	266
Teletype 925	268
VT 100/102/220	270
VT 52	273
Wyse 50	275
X3270	278
Translation Table Codes	280
The ASCII Character Set	280
Converting Decimal Numbers to Hex	283

Appendix C Troubleshooting

Error Messages	285
Problem Solving	303
Serial Communications	303
Keyboard	305
Graphics	306
Other Problems	307
Tips for Remote Control of Windows	307

Glossary

Index

About This Guide

Welcome to Norton pcANYWHERE for DOS, version 5.0.

Chapter 1, "Introduction," provides an overview, a Quick Start section for experienced software users, and information important to users of earlier versions of Norton pcANYWHERE for DOS. For example, it explains how configuration files from version 4.5 can be converted automatically when you run version 5.0 for the first time.

Chapters 2 through 6 explain how to install and configure pcANYWHERE. Chapters 7 and 8 guide you through sessions in which you remotely control another PC or communicate with an online service. Chapter 9 explains a number of utilities provided with Norton pcANYWHERE for DOS. For example, you can replay recorded sessions and test hardware configurations.

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

Conventions

This guide uses a number of conventions to make procedures easier to follow and to indicate the correct syntax for DOS commands.

Convention	Meaning
INITIAL CAPS	Indicates the name of an option on a menu or form.
monospaced	Indicates something you should enter from the keyboard such as a DOS command. For example, "Type <code>install</code> to start the installation program."
[]	Indicates an optional part of the syntax for a command. Do not enter the brackets themselves.
	Indicates that you can use only one of the options separated by this vertical bar.
select	Indicates that you highlight an option using the arrow keys.
choose	Indicates that you highlight an option using the arrow keys then press Enter.

Welcome to Norton pcANYWHERE



Norton pcANYWHERE for DOS is a complete, high-speed communications solution for stand-alone 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
- Provides a "Quick Start" section for experienced software users
- 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:

- An IBM AT, PS/2, or compatible PC
- MS/DOS 3.1 or higher
- At least 400K RAM available for Norton pcANYWHERE if you use a memory manager (490K RAM with no memory manager).

Norton pcANYWHERE currently supports the Novell NetWare IPX network protocol as well as NetBIOS (a standard networking protocol introduced by IBM) and Banyan VINES. Most network operating systems (including NetWare) have support for NetBIOS. Banyan VINES should be version 5.0 or higher.

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 called the *remote PC* and you are the *remote user*. The PC you are accessing in Los Angeles is called the *host PC*. Its user, if there is one, 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 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 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 in. 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 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 physically:

- Over telephone lines via modems. This is called a *serial connection*. Modem is short for *modulator/demodulator*. It 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, and another modem converts those signals back to computer data at the other end. 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 special wire that connects two computers directly via their serial ports.

- 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 lists the devices 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 a remote control session, each user must specify a hardware configuration for his or her PC. The settings for the hardware configurations do not have to be the same. For example, the host PC may be expecting a network connection by means of a pcANYWHERE gateway, and the remote PC may be using a modem. The exception to this is when two PCs are connected by a null modem cable. Each PC uses a hardware configuration with settings identical to the other's.

Before an online session, 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. See Chapter 5, “Session Configurations and Remote Preferences.”
- *Caller information* that lists the remote PCs from which your PC, when serving as a host, will accept a connection. Caller information also specifies how the remote user can interact with the host. Different users can have different levels of access. If you don't supply caller information, the settings on the *default caller information form* are used. If you do not change the settings on the default form, any remote user can access your PC without a password and with full privileges. See Chapter 6, “Caller Information and Host Preferences.”

Norton pcANYWHERE also offers a Quick Connect feature that allows you to specify a simple, minimal connection on either the host or remote PC. Quick Connect is explained in Chapter 7, “Remote Control Sessions,” and Chapter 8, “Online Sessions.” If you plan to access more than one computer on a regular basis, it is more convenient to have formally created the hardware, session, and caller information configurations.

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 9, “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.

Recorded sessions can be saved in a Record file, which is a 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 both automated procedures and a script language that allows you to perform operations automatically and at scheduled times.

Automated procedures are the easiest of the two to create, but can be used only for remote control operations between a pcANYWHERE host and remote PCs. You can automate tasks, such as transferring files between the two PCs and executing DOS commands on the host PC. See Chapter 7, "Remote Control Sessions."

You can write scripts for remote control sessions or for online sessions. For example, you can use scripts to automate tasks such as running programs or transferring files. Scripts can be written in any text editor. They are compiled and saved in script files; then they are executed either automatically upon beginning a session or anytime during a session. For details, see the technical reference guide for the script language, *Creating Norton pcANYWHERE Scripts*.

Other Features

In addition to the features discussed earlier in this chapter, Norton pcANYWHERE:

- Allows you to set remote control and online session preferences for the remote and host PCs. For example, you can specify settings for file transfer or the use of a special keyboard handler. See Chapter 5, "Session Configurations and Remote Preferences," and Chapter 6, "Caller Information and Host Preferences."
- Offers diagnostic tests for your hardware configurations, video modes, and keyboard. See Chapter 9, "Utilities."
- Allows you to review the DOS environment, your AUTOEXEC.BAT and CONFIG.SYS files, and the number and types of your ports, keyboard, video adapters, and monitor. See Chapter 9, "Utilities."

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 of great importance to you.

When following the procedures, remember that the word *choose* means to press Enter after you have highlighted your selection using the arrow keys.

If you have used previous versions of pcANYWHERE, you should also read "For Users of Earlier Versions of pcANYWHERE," later in this chapter.

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 the floppy disk into a disk drive and run the `INSTALL` program on it. Do the Standard Installation.
- 2 Set the current path to the installed directory (for example, `C:\AW`).
- 3 To start pcANYWHERE, type `AW` at the DOS prompt then press Enter. The pcANYWHERE Main menu appears.
- 4 Choose Configure....
The Configure menu appears.
- 5 Choose System Hardware....
The Hardware Configurations menu appears.
- 6 Choose Modem.
The Configuration: Modem form appears (Figure 1-1).

Figure 1-1 The hardware configuration provides pcANYWHERE the information it needs about your modem and other hardware used to make a connection.

Configuration: Modem		
Device/Port:	Serial - COM1	
Modem:	Hayes Compatible	
Data rate:	19200	Break length: 5 10ths/sec
Parity:	None	DTR state: Always On
Flow control:	RTS/CTS	RTS state: Always On
Connection started by:	Modem Response	
Connection ended by:	Carrier Detect (DCD)	
Ring no to answer on:	1	Seconds to wait after dial: 60
Dial type:	Tone	Leased line: No
Redial attempts:	0	Seconds between redials: 10
Additional modem initialization string:		Adjust speed to modem: No

- 7 Choose Device/Port. Then choose Serial from the Comm Device menu, and the COM port for your modem from the Serial Ports menu.
- 8 Choose Modem from the configuration form. Then choose Select From Modem List... and the name of your modem (or one with a similar command set) from the list of supported modems. If your modem isn't on the list, choose Hayes Compatible (the default) as a starting point for modification. With this selection, it is important to set the Data Rate and Adjust Speed To Modem options correctly. If your modem isn't Hayes compatible, choose Custom Modem and consult your modem manual for details. Depending on the modem you select, you may see the Adjust Parameters menu. Choose Yes so pcANYWHERE will optimize the modem options for you.
- 9 Press Esc until you return to the Configure menu, choosing Yes when prompted to save changes.
- 10 Choose System Setup....
The Preferences form appears.
- 11 Type a string that will uniquely identify this computer as the setting for Your Computer Name. Then press Enter. (The remote user will need to know the name given the host PC.)
- 12 Press Esc until you return to the pcANYWHERE Main menu, choosing Yes when prompted to save changes.

At this point, configuration choices diverge. Follow the procedure “To continue setting up a remote PC” later in this section or “To continue setting up a host PC” next.

To continue setting up a host PC:

- 1 From the pcANYWHERE Main menu, choose Be A Host...
The Be A pcANYWHERE Host menu appears.
- 2 Choose Select Active Configuration...
The Hardware Configurations menu appears.
- 3 Choose Modem.
The Configuration: Modem form appears.
- 4 Press Esc to return to the Be A pcANYWHERE Host menu.
- 5 Choose Begin Host Operation...
The Begin Host Operation menu appears.
- 6 Choose either Wait For A Connection or Exit, Allow Incoming Calls.
The pcANYWHERE Host Connection Status box appears and keeps you up-to-date on the connection process. After the connection occurs, you can press Alt+RightShift, the host hotkey, to display the Host Session Options menu.

To continue setting up a remote PC:

- 1 Confirm that the host PC is waiting for a call.
- 2 From the pcANYWHERE Main menu, choose Call A pcANYWHERE Host...
The Call A pcANYWHERE Host menu appears.
- 3 Choose Connect To A Host...
The Select Host For Connection menu appears.
- 4 Choose the pcANYWHERE Host Via Modem session configuration.
The Connect Options menu appears.
- 5 Choose View/Modify Host Entry.
The pcANYWHERE Host Via Modem form appears (Figure 1-2).

Figure 1-2 You may want to rename this session configuration later. Often the name indicates which host it is used to call.

pcANYWHERE Host: pcANYWHERE Host via modem	
Configuration name:	Modem
Phone number:	
prefix:	
suffix:	
Host computer name:	
Host password:	
Log session:	No
Data recording:	Initially Off
Script file:	[None]
Drive mapping:	Disabled

- 6 Select Phone Number and enter the telephone number of the host PC you want to connect to. You can type any prefix or suffix you need as part of the telephone number or select a prefix or suffix from the Phone Number Prefix or Phone Number Suffix forms.
- 7 Select Host Computer Name and type the name of the host PC with which you plan to connect. Then press Enter.
- 8 Press Esc to return to the Connect Options menu, choosing Yes to save your changes when prompted.
- 9 Choose Call.

The Connection Status box appears and keeps you up-to-date on the connection process. 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 press Ctrl+RightShift, the remote hotkey, to display a Session Options menu or type AWSEND to transfer files.

Connecting Over a LAN

The following procedures explain how to set up a remote control session for two PCs on the same LAN. It assumes that your network administrator has already 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 permissions 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 Set the current path to the installed directory (for example, F:\AW).
- 2 To start pcANYWHERE, type AW at the DOS prompt then press Enter.
- 3 Every time you access a network installation of Norton pcANYWHERE, you must identify yourself by typing in the same personal ID (up to six characters).

The pcANYWHERE Main menu appears.

- 4 Choose Configure....

The Configure menu appears.

- 5 Choose System Hardware....

The Hardware Configurations menu appears.

- 6 Choose Network or the hardware configuration for the network set up by your administrator.

The configuration form for the hardware configuration you chose appears (Figure 1-3).

Figure 1-3 The hardware configuration provides pcANYWHERE the information it needs about your network to make a connection.

Configuration: Network	
Device/Port:	NetWare IPX
Use gateway:	No

- 7 If Device/Port is not set to the correct type of network driver (NetWare IPX, NetBIOS, or Banyan), choose Device/Port then choose the correct driver.
- 8 If this configuration specifies a gateway, choose Use Gateway, then No. This procedure is not for calling a computer that is not on the network.
- 9 Press Esc until you return to the Configure menu, choosing Yes if you are prompted to save changes.
- 10 Choose System Setup....
The Preferences form appears.

- 11 Type a string that will uniquely identify this computer as the setting for Your Computer Name. Then press Enter. (The remote user will need to know the name given the host PC.)
- 12 Press Esc until you return to the pcANYWHERE Main menu, choosing Yes when prompted to save changes.

At this point, configuration choices diverge. Follow the procedure “To continue setting up a remote PC” later in this section or “To continue setting up a host PC” next.

To continue setting up a host PC:

- 1 Choose Be A Host...
The Be A pcANYWHERE Host menu appears.
- 2 From the menu choose Select Active Configuration...
The Hardware Configurations menu appears.
- 3 Choose Network or the hardware configuration for the network set up by your administrator.
The configuration form for the hardware configuration you chose appears.
- 4 Press Esc to return to the Be A pcANYWHERE Host menu.
- 5 From this menu choose Begin Host Operation...
The Begin Host Operation menu appears.
- 6 Choose either Wait For A Connection or Exit, Allow Incoming Calls.
The pcANYWHERE Host Connection Status box appears and keeps you up-to-date on the connection process. After the connection occurs, you can press Alt+RightShift, the host hotkey, to display the Host Session Options menu.

To continue setting up a remote PC:

- 1 Confirm that the host PC is waiting for a call.
- 2 From the pcANYWHERE Main menu, choose Call A pcANYWHERE Host...
The Call A pcANYWHERE Host menu appears.
- 3 Choose Connect To A Host...
The Select Host For Connection menu appears.
- 4 Choose the pcANYWHERE Host Via Network session configuration or choose one set up by your network administrator.

The Connect Options menu appears.

NOTE: You may want to rename this session configuration later. Often the name indicates which host it is used to call.

5 Choose View/Modify Host Entry.

The form for the session configuration you chose now appears.

6 Select Host Computer Name and type the name of the host PC with which you plan to connect. Then press Enter.

7 Press Esc to return to the Connect Options menu, choosing Yes to save your changes when prompted.

8 Choose Call.

The Connection Status box appears and keeps you up-to-date on the connection process. If the connection is successful, an image of the host screen appears on remote PC. Your keystrokes and mouse movements are sent to and processed by the host PC. You can press Ctrl+RightShift, the remote hotkey, to display a Session Options menu or type AWSEND to transfer files.

What's New in Version 5.0?

The features that are new in Norton pcANYWHERE version 5.0 are:

- Drive mapping which allows you to make the drives of the remote PC appear as additional drives on the host PC.
- Support for super VGA adapters when remotely controlling a host PC that is running Windows.
- The WINHOST.EXE file. When Windows is launched on the host, a pcANYWHERE icon appears at the bottom of the screen. This gives you access to a menu of session options available to the host.
- 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 (or a reasonable alternative) cannot be found in the list of modems supported by Norton pcANYWHERE, you can customize the modem command set using this new feature.
- Automatic use of upper memory blocks (UMBs) by the host TSR.

- Host 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.
- 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 5.0 to use encryption.
- Additional commands in the script language allow you to write scripts that automate remote control sessions. The additional commands start with the reserved word `Session` or `SessOpr` and are explained in the reference guide, *Creating Norton pcANYWHERE Scripts*.

For Users of Earlier Versions of pcANYWHERE

Users of earlier version of pcANYWHERE need to be aware of the following:

- The main menu is new. From it you can choose either host or remote operation. Remote operation has been divided into Calling A Host PC... and Calling An Online Service.... Host operation is called Be A Host....
- You will have to change any DOS commands that launch pcANYWHERE from your AUTOEXEC.BAT or another batch file. The AWREMOTE.EXE and AWHOST.EXE files have been consolidated into AW.EXE. Command-line options have a different appearance—although the meanings of most options have not changed. For example, `-M=A` is now `/M:A`.
- A computer running terminal-emulation software can no longer access a pcANYWHERE host PC. This discontinued feature was referred to in the 4.5 user's guide as "Calling a Host from a Terminal."
- The programmable function keys (used during online sessions) have been replaced by macro keys. You can now program Alt+0 through Alt+9. See Chapter 5, "Session Configurations and Remote Preferences."

Converting pcANYWHERE Version 4.5's Configuration Files

If you want to use your Norton pcANYWHERE version 4.5 configuration files (files that contain hardware configurations, session configurations, and caller information) with pcANYWHERE version 5.0, copy the old configuration files

into the directory or directories that you tell pcANYWHERE version 5.0 to use for configuration files. When you start pcANYWHERE version 5.0 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 5.0 for the first time using the ID @@@.

What are the names of the configuration files?

For a standalone installation, the filenames match the specification AW.?.?1.

For a network installation, the filenames of personal configuration files match the specification AW`userid`.?.?1 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 Chris, the filenames match the specification AWCHRIS_.?.?1. The filenames for shared configuration files match the specification AW.?.?1. The default configuration files (used as a starter set for each new user) match the specification AW@@@____.?.?1.

Where are the 4.5 configuration files now?

For a standalone installation, if you are using the AW environment variable in your AUTOEXEC.BAT file, you will find the 4.5 configuration files in the directory specified by that variable. Otherwise, the configuration files are in the directory where you installed pcANYWHERE 4.5.

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 4.5. Shared files are in the directory that was designated for shared files during that installation. If your network administrator did not do an advanced installation, both the personal directory and the shared directory are the directory where Norton pcANYWHERE 4.5 was installed.

Where do I move the files to?

For a standalone installation, put the files in the directory to be specified by the AW environment variable or the directory where you will install pcANYWHERE version 5.0.

For a network installation, put the personal files in the directory to be specified by the AW environment variable or the directory your network administrator chose for personal files when pcANYWHERE version 5.0 was installed. The network administrator should copy the shared files to the directory specified for shared files in pcANYWHERE version 5.0.

NOTE: If you installed Norton pcANYWHERE/LAN on your personal PC—even if only for your own use, your configuration files currently match the specification *AWuserid.??1*. If you want your configuration files automatically converted, you must change their names of those files to *AW.??1* before running Norton pcANYWHERE version 5.0.

Command-Line Options

The syntaxes for the AW command line are as follows:

```
AW [/I:userid] [/O:R] [/M:D|W|V|P|S]
  [/N:session_config|procedure_name|script_name]
```

```
AW [/I:userid] [/O:S] [/M:D|W|S]
  [/N:session_config|script_name]
```

```
AW [/I:userid] [/O:H] [/C:hdwe_config]
  [/N:phone_number]
```

```
AW [/I:userid] [/O:G]
```

/I	User ID (used for network installations); pc ANYWHERE asks network users for an ID
/O	Operation type
	R Call a host PC (that is, be a remote PC)
	H Be a host PC
	S Call an online service
	G Be a gateway
/M	Mode for your PC
	A Allow incoming connections (for host PC only)
	H Use hotkey to activate host (for host PC only)

W	Wait for a connection (for host or remote PC)
D	Initiate the connection (for host or remote PC)
V	Voice-first (for a remote PC)
P	Run an automated procedure (for a remote PC)
S	Run a script (for a remote PC)

/C Add the name of a hardware configuration

/N Additional information:

With /M:D, add the name of a session configuration

With /M:S, add the name of a script

With /M:P, add the name of an automated procedure

With /O:H, add the telephone number for a remote PC

Installation and General Setup

2

This chapter explains:

- Installation.

If you are installing Norton pcANYWHERE on your own PC, see “Standard Installation” next.

If you are on a network and your LAN administrator has already installed Norton pcANYWHERE in a directory accessible by all users, see “Adjusting Your AUTOEXEC.BAT File” later in this chapter. If you plan to use your PC as a host and allow remote users to run Windows on it, you should also read “Host Installation for Windows.” You may need to consult your LAN administrator because he or she may have already made adjustments for you.

If you are installing Norton pcANYWHERE for multiple users on a network, see “LAN Installation.”

- Navigation: How to move from option to option and setting to setting within the menus, forms, and boxes that appear on your monitor while you are using Norton pcANYWHERE.
- General setup, which includes the following:
 - Naming your PC.
 - Setting up a master password for security purposes.
 - Creating a general prefix and suffix list for telephone numbers.
 - Eliminating snow (if it is a problem on your monitor).
 - Selecting your own colors for the menus, forms, and so forth that appear on the screen.

Creating hardware and session configurations are also part of setting up your PC to work with Norton pcANYWHERE. However, each of these is covered elsewhere. Hardware configurations are explained in Chapter 3, “Hardware Configurations,” and session configurations are covered in Chapter 5, “Session Configurations and Remote Preferences.”

Standard Installation

The Standard Installation installs all the files needed by one user. When it is complete, you have the option of selecting the special host installation for Microsoft Windows. For details, see “Host Installation for Windows” next.

To install Norton pcANYWHERE:

- 1 Insert the floppy disk in drive A or B.
- 2 At the DOS prompt, type `a:install` or `b:install` then press Enter.

The installation menu appears.

- 3 Choose Standard Installation.

The Select A Drive For Installation menu appears. (If you have only one drive, you do not see this menu.)

- 4 Choose a drive letter from the menu.

The installation program suggests the AW directory on the selected drive. For example, you may see:

```
C:\AW
```

- 5 Type the complete pathname to the directory where you want to install Norton pcANYWHERE. Then press Enter.

The licensee identification form appears.

- 6 Type your name then press Enter.

The installation program keeps you up-to-date on the installation process.

- 7 When the installation is complete, choose Exit or Do Special Host Installation For Windows from the menu.

If you choose Do Special Host Installation For Windows, follow the steps in “Host Installation for Windows” (starting with step 3) then return to this procedure.



WARNING: If you have Norton pcANYWHERE for Windows, you must uninstall its host portion if you are going to use the DOS version of the host program.

- 8 If you choose Exit or when you return from the special host installation for Windows, you are asked if you want to browse the README.TXT file.

- 9 Press Y to view the file. Use the PgDn or PgUp keys to move forward or backward through the file. Press Home to return to the beginning of the file or End to go to the end of the file. Press Esc twice to exit.

Or,

Press N twice to exit the installation program without browsing the README file.

TIP: Before installing Norton pcANYWHERE, you should copy the installation floppy disk. This way, if something happens to the original disk, you still have a backup copy. To make the copies, you can use DISKCOPY.COM. See your DOS manual for details. If you have a diskless workstation, contact the network administrator about copying the disk and installing Norton pcANYWHERE for you.

Host Installation for Windows

If your PC will be a host PC and has Windows installed, choose the Do Special Host Installation For Windows option to speed up screen updates when a remote user accesses Windows on your PC. If you are selecting this option as part of the original installation of Norton pcANYWHERE, start with step 2 of the following procedure.

This installation program copies special driver files to your Window's SYSTEM directory and modifies both your SYSTEM.INI and WIN.INI files.

In the [boot] section of your SYSTEM.INI file, changes are made to the following lines to use pcANYWHERE drivers:

```
display.drv=
keyboard.drv=
mouse.drv=
```

In the [386Enh] section, the TimerCriticalSection statement, the NetHeapSize statement, and the following device= statements are modified as follows:

```
TimerCriticalSection=500
NetHeapSize=24
device=vpcaw.386
device=aw_vcd.386
```

The original driver names are stored in PCAW.INI. Please do not modify this file because it is used to restore your SYSTEM.INI file to its original state if you decide to uninstall pcANYWHERE.

In the WIN.INI file, the WINHOST.EXE file is appended to the load= line so that it is loaded when Windows starts. When Windows is launched on the host, a pcANYWHERE icon appears at the bottom of the screen. This gives you access to a menu of session options available to the host.

If you don't need this installation now, you can perform it at a future time from within the installed directory by re-running `INSTALL.EXE` and choosing only the special host installation for Windows. In this way, you install the special files for Windows without reinstalling the rest of the Norton pcANYWHERE files.

NOTE: The remote user must have either an EGA or VGA monitor to be able to run Windows remotely while accessing your PC as a host.

To speed up screen updates in Windows:

- 1 From the directory where Norton pcANYWHERE is installed, type `install` at the DOS prompt then press Enter.
An installation menu appears.
- 2 Choose Do Special Host Installation For Windows.
A form explains the changes that will be made to the SYSTEM.INI and WIN.INI files in your Windows directory.
- 3 Press any key to continue.
The Current Hardware Settings form and the Select Option menu appear.
- 4 If the display type is incorrect, choose Change Display Type.
When the Display Type menu appears, choose VGA, EGA, or Monochrome VGA.
You return to the Select Option menu.
- 5 If the keyboard type is incorrect, choose Change Keyboard Type from the Select Option menu.
When the Keyboard Type menu appears, choose IBM Compatible, Hewlett-Packard, or Olivetti.
You return to the Select Option menu.
- 6 When both the display and keyboard types are accurate, choose Accept Current Hardware Settings from the Select Option menu.
Several driver files are copied to your Window's SYSTEM directory.

A backup copy of your SYSTEM.INI file is made, and the SYSTEM.INI file is changed.

- 7 Press any key to continue.

A backup copy of your WIN.INI file is made, and the WIN.INI file is changed.

NOTE: For precautionary reasons, the special host installation program creates a backup of the Windows SYSTEM.INI and WIN.INI files each time the special host installation for Windows alters them. The backups are labeled as SYSTEM.01 or WIN.01 through SYSTEM.99 or WIN.99.

- 8 Press any key to exit the special host installation program.

If you selected this option during the standard installation of Norton pcANYWHERE, you return to step 8 of the procedure in “Standard Installation,” earlier in this chapter.

For additional information on running Norton pcANYWHERE with Windows, see the “Tips for Remote Control of Windows” in Appendix C, “Troubleshooting.”

Installing Norton pcANYWHERE on a LAN

You can do a standard network or an advanced network installation when installing Norton pcANYWHERE. The standard network installation is the simplest.

With the standard network installation, you automatically use the default settings shown in Figure 2-1. However, S:\AW will be replaced by the pathname you provide during installation. The pcANYWHERE program files are shared by all users and always go in a shared directory on the network. Configuration and information files are, by default, personal files because they can vary from user to user. Personal files go in a personal directory. However, both the shared and personal file directories default to the directory where pcANYWHERE is installed. 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. 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. If the network administrator

specifies a master password, no other user can view the shared configuration files.

For a 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.

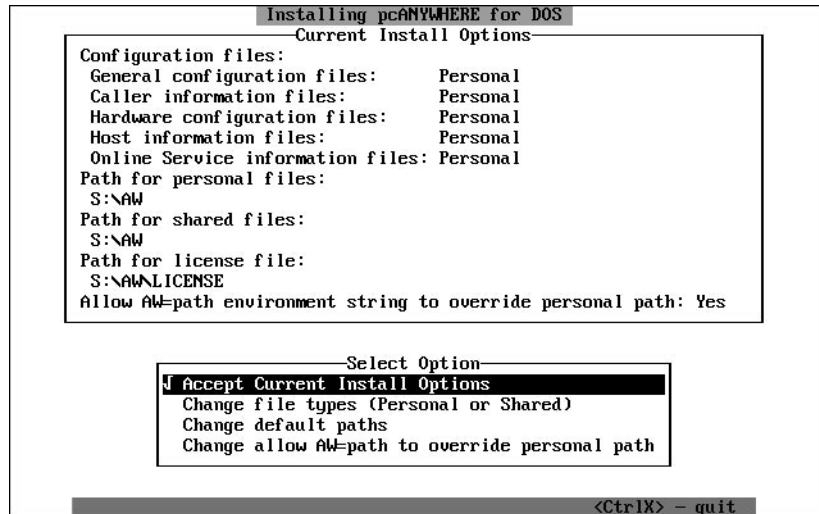
The following files can be personal or shared files:

- The caller information file (*AWuserid.CI6*)
- The hardware configuration file (*AWuserid.HW6*)
- The remote control session configuration file (*AWuserid.PC6*)
- The online session configuration file (*AWuserid.OS6*)
- The file for automated procedures (*AWuserid.AP6*)

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.

If you don't 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" for more details.
- Use the advanced network installation to create a separate directory for personal files.

Figure 2-1 The default options for a network installation

If you do an advanced network installation, you can:

- Change files labeled “Personal” to “Shared,” with the exception of general configuration files that are always labeled “Personal.” Personal files are installed in the personal directory, and shared files are installed in the shared directory.
- Provide your own pathnames for the personal, shared, and license directories.
- Disable the use of the AW environment variable. This ensures that only the directories you specify are searched for configuration files.

No matter what installation you choose:

- Each user needs full read and write access to the shared and license directories as well as to any personal directory for the user.
- The shared directory (which contains all the pcANYWHERE program files) should be in each user’s path (in the AUTOEXEC.BAT) so the user can start pcANYWHERE from any directory.

To install Norton pcANYWHERE:

- 1 Insert the floppy disk in drive A or B.
- 2 At the DOS prompt, type `a:install` or `b:install` then press Enter.

The installation menu appears.

- 3 Choose LAN Administrator Installation from the menu.
The Select A Drive For Installation menu appears.
- 4 Choose a drive letter from the menu.
The installation program suggests the AW directory on the selected drive. For example, you may see:

S:\AW

TIP: If you are going to use Norton pcANYWHERE gateways, make sure the PC where the gateway is located has access to the network drive where Norton pcANYWHERE is installed even when its user is not logged in. For example, on Novell networks, users can access the F:\LOGIN drive with read-only rights without being logged in.

- 5 Type the complete pathname to the directory where you want to install Norton pcANYWHERE. Then press Enter.
The licensee identification form appears.
- 6 Type your name, then press Enter.
The Select Install Option menu appears. Follow the steps in either “To perform a standard network installation” next or “To perform an advanced network installation,” which follows.

To perform a standard network installation:

- 1 Choose Standard Network Installation from the Select Install Option menu.
The installation program keeps you up-to-date on the installation process.
- 2 When the installation is complete, press any key to continue.
You are asked if you want to browse the README.TXT file.
- 3 Press Y to see the file. Use the PgDn or PgUp keys to move forward or backward through the file. Press Home to return to the beginning of the file or End to go to the end of the file. Press Esc twice to exit.
Or,
Press N twice to exit the installation program.

To perform an advanced network installation:

- 1 Choose Advanced Network Installation from the Select Install Option menu.

The Current Install Options form and the Select Option menu appear (Figure 2-1).

- 2 To change one of the file types for a configuration or information file from “Personal” to “Shared,” choose Change File Types (Personal Or Shared) from the Select Option menu.

The Change File Types menu appears.

- a Choose the option for the file type you want to change: Change Caller Information File Type, Change Hardware Configuration File Type, Change Host Information File Type, or Change Online Service File Type. (The host information and online service file types refer to session configuration files.)

The label for the type of file selected changes from “Personal” to “Shared” or vice versa. The Select Option menu reappears.

- b Repeat step 2 to change another type of file.

- 3 To change the default path for the personal, shared, or license directory, choose Change Default Paths from the Select Option menu.

The contents of the Select Option menu changes.

- a Choose the option for the path you want to change: Change Path For Personal Files, Change Path For Shared Files, or Change Path For License File.

A form appears that asks for a pathname.

- b Type the new pathname, then press Enter.

The new pathname appears in the form and the original contents of the Select Option menu reappear.

- c Repeat step 3 to change another path.

NOTE: Use the full pathname, but do not include a server or volume name. Be sure that the users can access these files using the pathnames you enter.

- 4 To disable the use of the AW environment variable, choose the Change Allow AW=Path To Override Personal Path option. (When enabled, the AW environment variable overrides the current setting for personal files.)

The Yes at the end of line about the environment variable changes to No (or vice versa), and the Select Option menu reappears.

- 5 To accept the current install options in the form, choose Accept Current Install Options.

The installation program keeps you up-to-date on the installation process.

- 6 When the installation is complete, press any key to continue.

You are asked if you want to browse the README.TXT file.

- 7 Press Y to see the file. Use the PgDn or PgUp keys to move forward or backward through the file. Press Home to return to the beginning of the file or End to go to the end of the file. Press Esc twice to exit.

Or,

Press N twice to exit the installation program without browsing the README file.

Uninstalling Norton pcANYWHERE for DOS

If your installation for Norton pcANYWHERE is not on a network, you can uninstall the following:

- The changes made for Windows to your SYSTEM.INI and WIN.INI files.
- The program files for Norton pcANYWHERE.

To uninstall Norton pcANYWHERE:

- 1 From the directory where Norton pcANYWHERE is installed, type `install /u` at the DOS prompt then press Enter.

A form explains what the uninstall program does.

- 2 Press any key to continue.

Depending on what you installed, you may not be asked all of the following questions.

- 3 If asked if you want to remove the pcANYWHERE Windows files from your system, do one of the following:

- Type Y for Yes if you want to uninstall them. Both your SYSTEM.INI and WIN.INI files will be altered.

Backup copies of your SYSTEM.INI and WIN.INI files are created. The SYSTEM.INI file is modified to remove references to pcANYWHERE drivers. These drivers are deleted from your WINDOWS\SYSTEM directory, and WINHOST.EXE is deleted from the load= statement in your WIN.INI. Press any key to continue when messages appear on the screen.

Or,

- Type N for No.

NOTE: You can exit the uninstallation program at any time by pressing Ctrl+X.

- 4 If you are asked if you want to remove the program files, do one of the following:
 - Type Y for Yes. The Norton pcANYWHERE program files are deleted. This empties the directory that stored them; later you may want to delete the directory itself using the RD command from DOS.

Or,

 - Type N for No.
- 5 Press any key to exit the program.

Adjusting Your AUTOEXEC.BAT File

You may want to adjust your AUTOEXEC.BAT (or, if you are a network administrator, a user's) file in one or both of the following ways:

- Add the name of the directory where pcANYWHERE program files are stored to your path. This allows you to start pcANYWHERE from any directory.

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

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

- Add the AW environment variable. Norton pcANYWHERE will store your personal configuration and information files in the directory specified by the AW environment variable—unless your network administrator has disabled the use of the variable. (You may need to talk to your administrator about this.)

For example, the following line in Anita M's AUTOEXEC.BAT file puts her configuration files (which contain the telephone numbers she calls using pcANYWHERE, and so forth) in her HOME directory on a network drive named F.

```
SET AW=F:\HOME\ANITAM
```

If you want to add a command line that starts Norton pcANYWHERE automatically, see Chapter 7, “Remote Control Sessions,” and Chapter 8, “Online Sessions.”

Getting Around in Norton pcANYWHERE for DOS

Norton pcANYWHERE lets you connect to a host PC running pcANYWHERE, an online service that communicates with your PC (which acts as a terminal), or set up your PC as a host. You will find it easy to move from menu to menu and supply the information needed by pcANYWHERE to make the connection to another computer—especially after reading this section that explains the menus and boxes that appear on the screen.

To start Norton pcANYWHERE:

- Type `AW` at the DOS prompt, then press Enter.
(Precede `AW` with the complete pathname to the directory where Norton pcANYWHERE is installed if that directory is not the current directory and is not in your `PATH`.)

The pcANYWHERE Main menu appears (Figure 2-2).

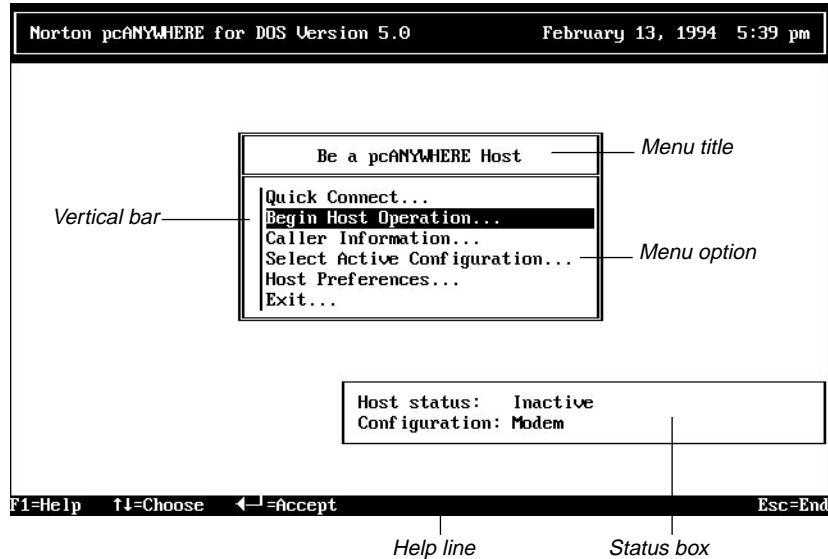
Figure 2-2 Use the Main menu to choose a type of operation



Norton pcANYWHERE has the following types of menus, forms, and boxes:

- Menus can be identified by the vertical bar that precedes the list of options (Figure 2-3). See the procedure “To choose an option from a menu,” later in this section.

Figure 2-3 A menu contains a list of options.



- Forms are lists of preferences or other options (Figure 2-4). Each has a default setting immediately following it. To change the settings for some options, you highlight the setting using the arrow keys, type the new setting, then press Enter. To change the settings for other options, you highlight the setting, press Enter, and choose the new setting from a menu. To clearly indicate which options are changed in which way, the procedures in this guide ask you to *select* an option when you are to highlight its setting. The next step in the procedure will ask you to type a new setting then press Enter. When a procedure asks you to *choose* an option, you highlight its setting then immediately press Enter to see a menu of possible settings. See the procedure “To select or choose an option from a form,” later in this section.

Figure 2-4 Form displays options and their settings.

The screenshot shows a window titled "Call Host Quick Connect" with a "Data Rate" menu open. The main form contains the following fields:

- Device/Port type: Serial - COM1
- Data rate: 19200
- Flow control: RTS/CTS
- Modem: Hayes Compatible
- Phone number:
- Adjust speed to modem: No
- Additional modem initialization string:

The "Data Rate" menu is open, showing a list of options: 75, 300, 600, 1200, 2400, 4800, 9600, 19200 (highlighted), 38400, 57600, and 115200. Annotations include:

- "Option that has a menu of settings" pointing to the "Data rate" field.
- "Option that you must type a setting for" pointing to the "Additional modem initialization string" field.
- "Menu of settings for the Data Rate option" pointing to the open menu.

- Status boxes which provide information such as the configurations being used and whether or not a host PC or gateway is active or inactive (Figure 2-3). Status boxes appear and disappear when appropriate. They require no keystrokes.
- The terminal window which appears when a connection has been made. For an online session, the terminal window displays the commands you type and the data displayed by the online service (Figure 2-5). For remote control sessions, terminal windows disappear when the host screen appears on the remote PC.

Figure 2-5 Terminal windows are used primarily for online sessions.

```

1 Shop by Department
2 Shop by Merchant (Alphabetic Listings)
3 Merchants Shipping Outside the US

4 Product Category Index
5 Directory of Catalogs

Enter choice !1

The Electronic Mall  SM-34

MALL DEPARTMENTS

1 Apparel/Department Stores
2 Arts/Music/Video
3 Auto/Boat/RV
4 Books/Periodicals
5 Clubs/Memberships
6 Computer Hardware/Supplies
7 Computer Software
8 Cosmetics/Jewelry
9 Gifts/Flowers/Gourmet Foods

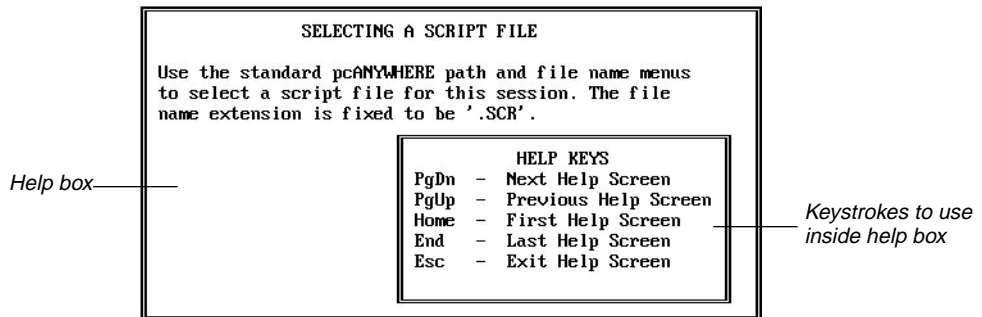
Enter choice or <CR> for more !
Menu: <Ctrl R-Shift>          57600 7E1      ANSI      Online

```


- Help boxes appear when you press F1 (Figure 2-6). They provide help with the option currently selected on the active form or menu. Sometimes the help box explains all the options on a menu. Press F1 a second time to see a list of the keystrokes you can use while reading the contents of a help box. Press Esc to return to the form or menu.

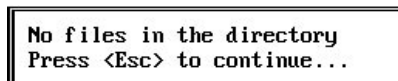
A help line at the bottom of the screen (Figure 2-3) lets you know what keystrokes can be used in the active menu or form. You do not need to press F1 to see the help line. It is always displayed.

Figure 2-6 Even help boxes have help.



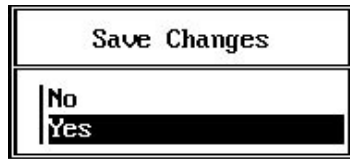
- Error/Warning boxes appear on the screen when an error occurs (Figure 2-7). Press Esc to make the box disappear. See Appendix C, "Troubleshooting," for a list of error messages.

Figure 2-7 The Error/Warning box alerts you to a problem.



- Yes/No menus appear on the screen when a Yes/No choice needs to be made (Figure 2-8). For example, when the Save Changes menu appears, you choose Yes to save changes made to a form, or choose No to exit without saving the changes.

Figure 2-8 Yes/No menus confirm your changes and deletions.



To move from option to option on a menu or form:

- Use the arrow keys.
The current option becomes highlighted.

TIP: On a menu, you can move quickly to an option by typing the first letter (or first few letters) in its name. Pressing Home or End takes you to the beginning or end of the menu. Pressing PgUp and PgDn scrolls up and down the options on a long menu.

To choose an option from a menu:

- Use the arrow keys to highlight the option then press Enter.

To select or choose an option from a form:

- 1 Use the arrow keys to highlight the setting for the option.
- 2 Do one of the following:
 - When you *select* an option, such as a password, you type in the setting, then press Enter.
 Or,
 - When you *choose* an option, pressing Enter (or any key) makes a menu appear. Use the arrow keys to highlight an option from the menu then press Enter to actually choose the option that is highlighted.

TIP: When an option on a form has a menu of possible settings, highlight the option. Then, instead of pressing Enter, type the first letter (or first few letters) of the setting you want from the menu. When the menu appears, that setting will already be highlighted.

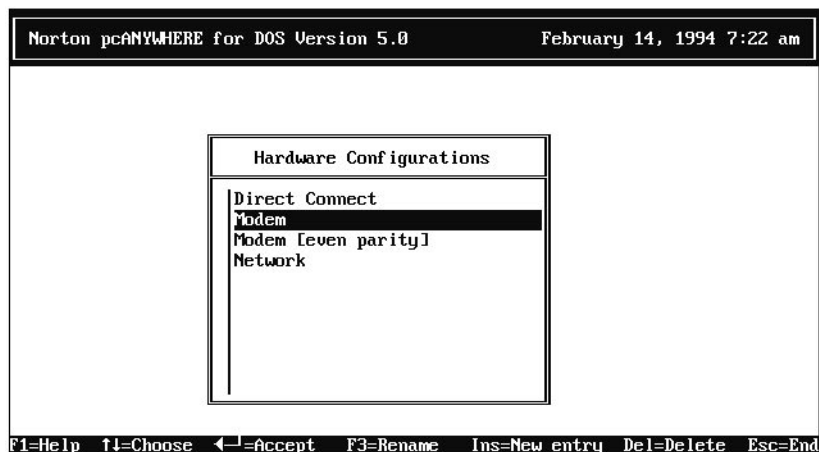
To exit a menu or a form (with or without saving your changes):

- Press Esc.
If you have made changes, a Save Changes menu appears from which you can choose Yes or No.

Adding Options to a Menu

You can add, delete, and rename the options on some menus (Figure 2-9). The options on these menus are the names of hardware configurations, session configurations, caller information configurations, and automated procedures. The help line at the bottom of the screen lists the keystrokes you use to add, delete, and rename options.

Figure 2-9 You can add, delete, and rename some menu options.

**To add an option from a menu:**

- 1 Press Insert.
The Name To Add form appears.
- 2 Type the name for the menu option then press Enter.
- 3 If additional forms appear, fill them in.

To delete an option to a menu:

- 1 Select the name of the configuration or procedure.

- 2 Press Delete.
The Delete form appears.
- 3 Choose Yes.

To rename an option on a menu:

- 1 Press F3.
The New Name form appears.
- 2 Type the name then press Enter.

Selecting a Pathname from a Form

The Select Path form (Figure 2-10) is a common form that assists you as you choose a file, such as script file or a spool file.

Figure 2-10 The Select Path form is used to identify the directory that stores the desired file.

Select Path For Operations File
F:\AWDOS

To select a file using a Select Path form:

- 1 Do the bulleted step or substeps a through e:
 - From the Select Path form, type the pathname to the file you want then press Enter. (Do not include the filename at this step.)

Or,

- a Press DownArrow.

The Directories menu appears (Figure 2-11).

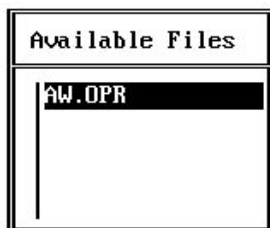
Figure 2-11 The Directories menu makes it easy to locate a directory.

Directories
.
INST
SAVE

- b** Choose “..” or the name of a subdirectory to change directories.
The contents of the Directories menu displays the subdirectories for the directory you choose, and the Select Path form displays the path to that directory.
- c** Repeat step b until the pathname you want appears in the Select Path form.
- d** Press Esc to exit the menu.
- e** Press Enter.

The Available Files menu (Figure 2-12) shows the names of all the files in the directory.

Figure 2-12 The Available Files menu makes it easy to select a file.



- 2** Choose the file.

Naming Your PC

Choose a name for your PC that is meaningful and easy to remember. You can use up to 24 characters.

To name your PC:

- 1** Choose Configure... from the pcANYWHERE Main menu.
The Configure menu appears.
- 2** Choose System Setup...
The Preferences form appears with the Your Computer Name option highlighted.
- 3** Type the name for your PC then press Enter.
- 4** Press Esc as many times as necessary to return to a menu you want to use. When you see the Save Changes menu (as you exit from the Preferences form), choose Yes.

Security

For security purposes, you can set a master password that stops anyone from changing or viewing any configuration or preference information without knowing the password.

You must know the master password to access any of the following. However, once you provide the password, you will not be asked for it again in that session.

- Configure... on the pcANYWHERE Main menu
- Remote Preferences... on the Call A pcANYWHERE Host menu
- Online Service Preferences... on the Call An Online Service menu
- Host Preferences... on the Be A pcANYWHERE Host menu
- Gateway Preferences... on the Be A pcANYWHERE Gateway menu
- Anytime you attempt to add an additional or modify a current session or hardware configuration

To set or change a master password:

- 1 Choose Configure... from the pcANYWHERE Main menu.
The Configure menu appears. (You may be asked for the current master password.)
- 2 Choose System Setup....
The Preferences form appears.
- 3 Choose Master Password.
If there is a current master password, it appears in the space for the setting.
- 4 Type a master password then press Enter.
- 5 Press Esc to exit the Preferences form.
The Save Changes menu appears.
- 6 Choose Yes.
- 7 Press Esc to return to the pcANYWHERE Main menu.

Creating a Telephone Prefix and Suffix List

A *prefix* is an optional number or group of numbers added to the beginning of a telephone 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 credit card number is an example of a suffix. You can create a list of up to ten prefixes and suffixes that you commonly use when calling or you can add the correct prefix or suffix to each telephone number. Having a list to select from can be a major convenience. For example, if you need to add a credit card number to telephone calls, you don't have to look it up or worry about mistyping it every time you create a new session configuration.

To create a prefix/suffix list or add to the current one:

- 1 Choose Configure... from the pcANYWHERE Main menu.
The Configure menu appears.
- 2 Choose Dialing Prefix/Suffix...
The Prefix/Suffix form appears.
- 3 To modify the default settings for Outside Line, Cancel Call Waiting, or Credit Card:
 - a Select that option from the form.
 - b Press Enter twice.
 - c Type the new number, then press Enter.
- 4 To add a new prefix or suffix:
 - a Press DownArrow until you reach an empty line (or a line you want to replace).
 - b Type the name (up to 20 characters) for the prefix or suffix, then press Enter.
 - c Type the new number (up to 30 characters), then press Enter.
- 5 Press Esc until you reach a menu you want to use.

If You Have Snow...

Some color displays (such as older CGAs) occasionally display snow on the screen, just like the snow or static on a TV set. The Eliminate Snow preference allows you to clear up snow on your computer's screen whether it is used for host or remote operation.

NOTE: You can test for snow using Hardware Diagnostics. See Chapter 9, "Utilities."

To eliminate snow:

- 1 Choose Configure... from the pcANYWHERE Main menu.
The Configure menu appears.
- 2 Choose System Setup....
The Preferences form appears.
- 3 Choose Eliminate Snow.
The Eliminate Snow menu appears.
- 4 Choose Yes.
Or,
If you want to eliminate snow on menus only, choose Menus Only.
- 5 Press Esc as many times as necessary to return to a menu you want to use. When you see the Save Changes menu (as you exit from the Preferences form), choose Yes.

Customizing Display Colors

Each displayable object, such as a menu or form, has fields that are predefined as having normal, intense, or reverse video attributes. For example, the options listed on a menu are *normal*; the selected option or setting is *reverse*, and both the menu's title and border are *intense*.

You can select the background and foreground colors for the normal and reverse attributes. You can select only the foreground color for the intense attribute which always uses the background color specified for normal.

To customize colors:

- 1 Choose Configure... from the pcANYWHERE Main menu.
The Configure menu appears. (You may be required to input a master password.)
- 2 Choose System Setup....
The Preferences form appears.
- 3 Choose Program Colors.
The Program Colors menu appears.
- 4 Choose User Defined.
The Color Selection menu appears. Each type of object that can appear on the screen has a color palette. For example, Color Palette 4 is for most menus.

NOTE: From the Program Colors menu, you can choose Monochrome to see everything in black, white, and light gray only. Or, you can choose Default to return to the color scheme (primarily blue, white, and yellow) that comes with Norton pcANYWHERE for DOS.

- 5 Choose a color palette.
The Edit Attribute menu appears from which you select an attribute's foreground or background color. The Current Palette form also appears. It displays the current color settings for each attribute.
- 6 Choose an option from the Edit Attribute menu. For example, you may want to select a color for Foreground Intense.
When selecting a background color, a menu of 8 colors appears.
When selecting a foreground color, a menu of 16 colors appears.
- 7 Choose a color.
- 8 Repeat steps 6 and 7 for other attributes on the same color palette.
- 9 Repeat steps 5 through 8 for other color palettes.
- 10 Press Esc as many times as necessary to return to the pcANYWHERE Main menu. When you see the Save Changes menu (as you exit from the Color Palette menu), choose Yes.

Hardware Configurations

3

A hardware configuration is the physical description of how your PC will connect to another computer, regardless of whether your PC is acting as the host or the remote.

This chapter explains how to create hardware configurations for the following types of serial and network connections:

- Modem (serial)
- Direct (serial)
- Interrupt 14 (serial)
- Network node
- NACS/NASI (network)
- Telebit ACS (network)

The chapter also explains the following:

- How to tell Norton pcANYWHERE that you have customized a serial port for an internal modem or other add-on serial board
- How to customize the modem command set in case you can't find your modem (or any reasonable alternative) in the list of modems supported by Norton pcANYWHERE.
- Managing hardware configurations: modifying them, creating new ones from existing ones, renaming them, and deleting them.

Although you can create and modify hardware configurations from several places in Norton pcANYWHERE, it is easiest to set things up in the beginning.

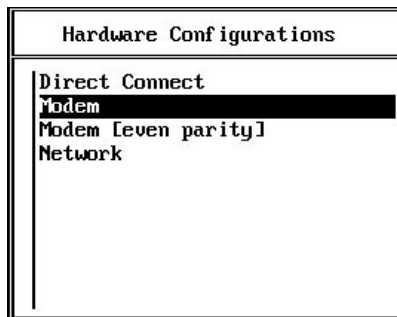
A hardware configuration becomes part of the information about each gateway and session configuration. Many types of hardware configurations require modem information. For an explanation of modem communications and much of the terminology you see on the hardware configuration forms, see Appendix A, "Technical Information," or the Glossary.

You will need one hardware configuration for each method by which you use Norton pcANYWHERE to connect to another computer. For example, if

your PC is not on a LAN and you will be connecting to other computers only through a modem, you probably need only a modem hardware configuration. If you are on a network and have a modem, you probably need at least a modem and a node hardware configuration. The node hardware configuration allows you to connect to other PCs on the network. If the network has a gateway, you need an additional node hardware configuration allowing you to use the gateway for off-LAN connections. If your modem is used in a gateway configuration on the network, you can only access your modem as a gateway using a node hardware configuration.

Norton pcANYWHERE comes with four default configurations (Figure 3-1). Most users modify the default configurations to meet their needs. If your network administrator has added configurations, or changed and renamed the set of defaults, your screen may not show the same configuration names.

Figure 3-1 Use the Hardware Configurations menu to customize the default hardware configurations to match your system.



Creating Serial Hardware Configurations

Serial hardware configurations can be used by both stand-alone and network installations of Norton pcANYWHERE. The only requirement is that the PC be able to connect to another computer via a serial communications port.

Creating a Modem Hardware Configuration

You can customize the default hardware configuration named Modem for your own use by changing the settings for one or more of its options.

To create a hardware configuration for a modem:

- 1 Choose Configure... from the pcANYWHERE Main menu.

The Configure menu appears. (You may have to enter the master password before you can see the menu.)

- 2 Choose System Hardware....

The Hardware Configurations menu appears (Figure 3-1).

- 3 Choose Modem.

The Configuration: Modem form appears (Figure 3-2) with the Device/Port option selected.

Figure 3-2 The Configuration: Modem form lets you modify the hardware configuration settings.

Configuration: Modem		
Device/Port:	Serial - COM1	
Modem:	Hayes Compatible	
Data rate:	19200	Break length: 5 10ths/sec
Parity:	None	DTR state: Always On
Flow control:	RTS/CTS	RTS state: Always On
Connection started by:	Modem Response	
Connection ended by:	Carrier Detect (DCD)	
Ring no to answer on:	1	Seconds to wait after dial: 60
Dial type:	Tone	Leased line: No
Redial attempts:	0	Seconds between redials: 10
Additional modem initialization string:		Adjust speed to modem: No

TIP: If you want an additional hardware configuration for a modem, choose Modem then press Insert and provide the name for a new configuration based on the current Modem configuration.

- 4 If the current communications port is the correct one, go on to step 7. Otherwise, press Enter.

The Comm Device menu appears.

- 5 Choose Serial.

The Serial Ports menu appears.

- 6 Choose the name of the correct port (COM1 through COM4). If you are using a customized serial port, see "Using a Custom Port" later in this chapter.

The Configuration: Modem form reappears with the Modem option selected.

- 7 Press Enter twice.

The Supported Modems menu appears.

- 8 Choose the name of your modem.

A form appears suggesting options (parameters) for the selected modem. The Adjust Parameters menu also appears.

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.

- 9 Choose Yes so pcANYWHERE will optimize the modem options for you.

See Appendix A, "Technical Information," or the Glossary for more information about settings on the configuration form.

NOTE: A leased line is a dedicated line between two modems that are leased-line compatible. If you are using a leased line, the option for Leased Line must be set to Yes in the hardware configurations for both remote and host PCs. The most common usage of leased lines is between multiplexers. For more information, see Appendix A, "Technical Information."

To accept the form's settings:

- 1 Press Esc to exit the form.
The Save Changes menu appears.
- 2 Choose Yes.

Creating a Direct Serial Hardware Configuration

Direct serial connections require a special cable, 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."

The configurations for both the remote and host PCs must have identical Data Rate, Flow Control, and Parity settings.

To create a hardware configuration for use with a null modem cable:

- 1 Choose Configure... from the pcANYWHERE Main menu.

The Configure menu appears. (You may have to enter the master password before you can see the menu.)

- 2 Choose System Hardware....

The Hardware Configurations menu appears (Figure 3-1).

- 3 Choose Direct Connect.

The Configuration: Direct Connect form appears (Figure 3-3) with the Device/Port option selected.

Figure 3-3 When configuring a direct connection, make sure settings for Data Rate, Parity, and Flow Control are identical on both the host and remote PCs.

Configuration: Direct Connect		
Device/Port:	Serial - COM1	
Modem:	None	
Data rate:	19200	Break length: 5 10ths/sec
Parity:	None	DTR state: Always On
Flow control:	RTS/CTS	RTS state: Always On
Connection started by:	Carrier Detect (DCD)	
Connection ended by:	Carrier Detect (DCD)	

- 4 If the current communications port is the one to which your modem is attached, go on to step 7. Otherwise, press Enter.

The Comm Device menu appears.

- 5 Choose Serial.

The Serial Ports menu appears.

- 6 Choose the name of the correct port (COM1 through COM4).

The Configuration: Direct Connect form reappears with the Modem option selected and already set correctly to None.

- 7 Choose Data Rate.

The Data Rate menu appears.

- 8 Choose 9600 at first and experiment later with the faster speeds available through the PCs' communications ports.

- 9 Choose the Flow Control option.

The Flow Control menu appears.

- 10 Choose RTS/CTS. (Make sure your null modem cable supports RTS and CTS signals.)

To accept the form's settings:

- 1 Press Esc to exit the form.
The Save Changes menu appears.
- 2 Choose Yes.

Creating an Interrupt 14 Hardware Configuration

Some network communications products use Interrupt 14, the standard serial port support built into the BIOS. With the use of an Interrupt 14 driver, users on a network can share modems. The Interrupt 14 driver must be loaded before Norton pcANYWHERE is launched. Refer to the manual for your network communications product for more information on installing and configuring the Interrupt 14 software.

To create a hardware configuration using an Interrupt 14 device:

- 1 Choose Configure... from the pcANYWHERE Main menu.
The Configure menu appears. (You may have to enter the master password before you can see the menu.)
- 2 Choose System Hardware....
The Hardware Configurations menu appears (Figure 3-1).
- 3 Press Insert, type the name for this hardware configuration, then press Enter.
The configuration form appears. In its title is the name of the hardware configuration you chose. The Device/Port option is selected.
- 4 Press Enter.
The Comm Device menu appears.
- 5 Choose Int14.
The Serial Ports menu appears.
- 6 Choose the name of the correct port (COM1 through COM16). For more information on Interrupt 14 COM port addressing, refer to your Interrupt 14 manual.
The configuration form reappears with the Modem option selected.
- 7 Press Enter twice.
The Supported Modems menu appears.

- 8 Choose the name of your modem.

A form appears suggesting options (parameters) for the modem. The Adjust Parameters menu also appears.

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

- 9 Choose Yes so pcANYWHERE will optimize the modem options for you.

See Appendix A, “Technical Information,” or the Glossary for more information about settings on the configuration form.

NOTE: Norton pcANYWHERE supports the standard Interrupt 14 speeds, which only go up to 9600 bps. You may need to change the Data Rate accordingly.

To accept the form’s settings:

- 1 Press Esc to exit the form.
The Save Changes menu appears.
- 2 Choose Yes.

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), 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. Off-LAN connections made with a gateway require a different configuration from off-LAN connections made with an ACS.

If you are attached to a network, you can create a network hardware configuration even if Norton pcANYWHERE was installed on your PC using a stand-alone Norton pcANYWHERE installation. The difference between using

a network installation and a stand-alone installation on a PC connected to a network is the location of the pcANYWHERE data and program files and how they are accessed. See Chapter 2, “Installation and General Setup.”

Creating a Node Hardware Configuration

A PC attached to a network is often referred to as a *node* on that network. Node hardware configurations are used 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 network administrator.



Network

NETWORK USERS: The way in which your network administrator configured Norton pcANYWHERE during installation determines whether or not you can create or edit hardware configurations. Ask your network administrator before attempting this.

Norton pcANYWHERE is supplied with three device drivers that can be used for node connections across a network:

- NetWare IPX
- NetBIOS
- Banyan

Choose the device driver appropriate for the network on which Norton pcANYWHERE is installed.

To create a hardware configuration for a network node:

- 1 Choose Configure... from the pcANYWHERE Main menu.
The Configure menu appears. (You may have to enter the master password before you can see the menu.)
- 2 Choose System Hardware....
The Hardware Configurations menu appears (Figure 3-1).
- 3 Choose Network.
The Configuration: Network form appears (Figure 3-4) with the Device/Port option selected.

Figure 3-4 Use the Configuration: Network form to create a node hardware configuration.

Configuration: Network	
Device/Port:	NetWare IPX
Use gateway:	Yes
Gateway name:	<input type="text"/> Class:
Parity:	None

TIP: If you want an additional hardware configuration for a node, choose Network then press Insert and provide the name for a new configuration based on the current Network configuration.

- 4 If NetWare IPX is the communications device supported by your network, go on to step 6. Otherwise, press Enter.

The Comm Device menu appears.

- 5 Choose the correct communications device.

If you are unsure which to choose, contact your network administrator.

NOTE: For node-to-node connections, the setting for Device/Port must be identical for both remote and host computers.

- 6 If your PC will act as the remote PC and use a gateway, choose Use Gateway, then Yes.

Configuring the Gateway Name, Class, and Parity settings enables pcANYWHERE to automatically connect to the specified gateway name and/or class.

Gateway options include:

- Name. Type the gateway's name so Norton pcANYWHERE automatically chooses that gateway, then press Enter. If no name is entered, a list of available gateways appears when you attempt to make a connection. Enter an asterisk (*) to allow Norton pcANYWHERE to choose any gateway. (The name is really the computer name for the PC where the gateway has been configured.)

- **Class.** Type the gateway's class if several gateways exist with different classes, then press Enter. If no class is entered, a list of available gateways and classes appears when you attempt to make a connection. A common way to classify gateways is by the speed of their modems. For example, the 9600 class would be for 9600-bps modems. Enter an asterisk (*) to allow pcANYWHERE to choose any class.
- **Parity.** Set Parity to dial out with a different parity than that configured in the gateway's outgoing hardware configuration. In most cases the gateway's hardware configuration is configured with no parity. Connection to pcANYWHERE hosts requires no parity, but if you need to connect to an online service, such as CompuServe, your parity must be set to Even. Setting parity from the remote node's hardware configuration is easier than changing the gateway's parity.

For more information on gateways, see Chapter 4, "Gateway Configurations."

To accept the form's settings:

- 1 Press Esc to exit the form.
The Save Changes menu appears.
- 2 Choose Yes.

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 somewhat like 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 multi-port serial card. Several of these cards can be added to an ACS creating a large 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 to 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.

- The server defines which ACS Norton pcANYWHERE will attach to.
- The service defines which multi-port serial card to use within the ACS.
- The port defines which serial port to use on the multiport serial card within the ACS.

To create a hardware configuration for an ACS:

- 1 Choose Configure... from the pcANYWHERE Main menu.
The Configure menu appears. (You may have to enter the master password before you can see the menu.)
- 2 Choose System Hardware....
The Hardware Configurations menu appears (Figure 3-1).
- 3 Press Insert, type the name for this hardware configuration, then press Enter.
The configuration form appears. In its title is the name of the configuration you chose. The Device/Port option is selected.
- 4 Press Enter.
The Comm Device menu appears.
- 5 Choose NASI/NCSI.
The NASI/NCSI Device form appears (Figure 3-5).

Figure 3-5 You can specify a server, service, and port now or at the time you use the ACS.

NASI/NCSI Device	
Server:	<any>
Service:	<any>
Port:	<any>
Select later:	No

6 Specify how the ACS port is to be selected.

By default, the Server, Service, and Port settings are <any>. This causes Norton pcANYWHERE to attach to any available server, service, and port. Use the default settings, follow the bulleted step below to choose settings at the time of connection, or follow substeps a through c to specify specific settings now.

- To choose the server, service, and port at the time of connection, choose Select Later. (You will have to confirm that selection by choosing Yes from the Select Later menu.)

Or,

- a To specify a specific server, service, or port other than <any>, choose that option.

The Select Options menu appears.

- b Choose Select From List to select from a menu of currently available servers, services, or ports.

Or,

Choose Enter Name (or Enter Number for a port), type the setting for the option in the form that appears, then press Enter. (This allows you to specify a device that is not currently available.)

- c Repeat steps a and b for each of the options.

NOTE: Using the <any> option works only if you are dialing out of an ACS as a remote. If you plan to wait for a call as a host, Norton pcANYWHERE requires that you specify a specific Server, Service, and Port.

The configuration form reappears with the Modem option selected.

7 Press Enter twice.

The Supported Modems menu appears.

8 Choose the name of the ACS modem with which you are connecting. (You may need to get the name from your network administrator.)

A form appears suggesting options (parameters) for the modem. The Adjust Parameters menu also appears.

9 Choose Yes so pcANYWHERE will optimize the modem options for you.

See Appendix A, "Technical Information," or the Glossary for more information about settings on the configuration form.

To accept the form's settings:

- 1 Press Esc to exit the form.
The Save Changes menu appears.
- 2 Choose Yes.

Using a Telebit ACS

The Telebit 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 Device form (Figure 3-6 through 3-8) displays the necessary options.

Do not use Register for remote configurations because it is a host function only.

To create a hardware configuration for a Telebit ACS:

- 1 Choose Configure... from the pcANYWHERE Main menu.
The Configure menu appears. (You may have to enter the master password before you can see the menu.)
- 2 Choose System Hardware....
The Hardware Configurations menu appears (Figure 3-1).
- 3 Press Insert, type in the name for this hardware configuration, then press Enter.
The configuration form appears. In its title is the name of the configuration you chose. The Device/Port option is selected.
- 4 Press Enter.
The Comm Device menu appears.
- 5 Choose Telebit ACS.
The Telebit ACS Device form appears (Figure 3-6).

Figure 3-6 Select by Pool

Telebit ACS Device	
Port select method:	Pool
Server:	<any>
Pool name:	<any>

Figure 3-7 Select by Port

Telebit ACS Device	
Port select method:	Port
Server:	<any>
Gateway:	<any>
Port:	<any>

Figure 3-8 Select by Register

Telebit ACS Device	
Port select method:	Register
Server:	<any>

- 6** If Pool is not the correct Port Select Method, press Enter. Otherwise, go to step 8.

The Port Selection Method appears.

- 7** Choose the correct method.

The Telebit ACS Device form appears (Figure 3-7 or 3-8).

For any option on the form, choose <any>, choose a specific setting from a list, or type a name as the setting. Press Esc to exit the form.

The configuration form reappears with the Modem option selected (unless Register is the Port Select method).

- 8** Press Enter twice.

The Supported Modems menu appears.

- 9** Choose the name of the ACS modem with which you are connecting.

A form appears suggesting options (parameters) for the modem. The Adjust Parameters menu also appears.

- 10** Choose Yes so pcANYWHERE will optimize the modem options for you.

See Appendix A, “Technical Information,” or the Glossary for more information about settings on the configuration form.

To accept the form’s settings:

- 1** Press Esc to exit the form.

The Save Changes menu appears.

- 2** Choose Yes.

NOTE: Refer to the Telebit ACS manual for configuration details.

Using a Custom Port

You use a custom port when you have an internal modem or another add-on serial board that uses a non-standard I/O address or hardware interrupt (IRQ). Many internal modems are not configured to use one of the first two communications ports (COM1 or COM2) because that would make the port unavailable for some other peripheral, such as a mouse. For example, an internal modem is sometimes assigned to COM3 or COM4.

Normally, COM1 and COM3 share IRQ 4, and COM2 and COM4 share IRQ 3. This can create a conflict. To prevent this, one of the devices, typically the modem, must be configured to use a different IRQ. For more information on COM ports and I/O addresses, see Appendix A, "Technical Information."

Look in your modem or serial board manual to determine which I/O address, in hexadecimal code, and IRQ number to use.

CAUTION: Before using a custom port in Norton pcANYWHERE, configure your internal modem or serial board for the COM port and IRQ line needed. You must have the COM port base address and the IRQ line before proceeding. Entering incorrect information can cause other devices within your computer to stop functioning until the computer is reset.

To specify a custom port within a hardware configuration:

- 1 Choose Configure... from the pcANYWHERE Main menu.
The Configure menu appears. You may have to enter the master password before you can see the menu.
- 2 Press Enter.
The Comm Device menu appears.
- 3 Choose Serial.
The Serial Ports menu appears.
- 4 Choose Custom.
The Custom Port Parameters form appears (Figure 3-9).

Figure 3-9 Specify an IRQ value and I/O address to define a custom port. A common choice is IRQ5 and 3E8 (for COM3) or 2E8 (for COM4).

Custom port parameters	
IRQ (0-7):	5
Address:	3F8

- 5 Type in the IRQ number then press Enter.
- 6 Type in the I/O address then press Enter.
- 7 Press Esc.

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 supported, do one of the following:

- Ask your modem manufacturer which modem in the list has a similar command set and use 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.
- Define a custom modem. The settings you define are stored in the personal file, AW.INI or AW*userid*.INI file (if you use a network installation of pcANYWHERE). See the following procedure for details.

To create a custom modem setup:

- 1 Choose Modem from the hardware configuration form.
The Modem menu appears.
- 2 Choose Custom Modem...
The View/Edit Custom Modem Settings menu appears.
- 3 Choose Yes.

The Custom Modem Setup form appears (Figure 3-10).

Figure 3-10 The default settings for a custom modem

Custom Modem Setup	
Modem name:	Custom Modem
Initialization:	AT&F&E0U1
Dial Prefix:	ATDT
Dial Suffix:	
Answer:	ATS0=1
Disconnect:	~+++~ATHS0=0
Data rate:	19200
Use RTS/CTS flow control:	Yes
Adjust speed to modem:	No
Connect Response:	CONNECT *
Error Response:	NO ERROR
No Carrier Response:	NO CARRIER
Busy Response:	BUSY
No Dialtone Response:	NO DIALTONE
No Answer Response:	NO ANSWER
No Connect Response 1:	
No Connect Response 2:	
No Connect Response 3:	

- 4 Use your modem's manual to determine what settings to use for each option. You type in all the settings except for Data Rate, Use RTS/CTS Flow Control, and Adjust Speed To Modem, which have menus from which you select a speed or yes or no.

- 5 Press Esc to exit the form.

The Save Changes appears if you modified the settings.

- 6 Choose Yes.

The Adjust Parameters menu appears.

- 7 Choose Yes so that pcANYWHERE modifies the settings in the hardware configuration form to reflect your changes to the custom modem settings.

Managing Hardware Configurations

Occasionally, you may want to modify, rename, or delete a hardware configuration. If you change your modem, for example, you may want to modify or delete hardware configurations used by the old modem.

You can modify the setting for options in a hardware configuration directly (by following the steps earlier in this chapter) or while modifying any session configuration that specifies that hardware configuration. Remember that the same hardware configuration may be specified in several session configurations. Because modifying it for one session configuration modifies it

for all session configurations, you may prefer to create a new hardware configuration from the existing one rather than make a modification that will apply to only one session configuration. To create the new configuration, select the existing one, then press Insert to add a new configuration to the Hardware Configurations menu.

You can delete a hardware configuration from the Hardware Configurations menu by selecting the configuration and pressing Delete. However, if you select a configuration that is used in a session configuration, Norton pcANYWHERE won't allow you to delete it until you modify the session configuration. Remember that the same hardware configuration may be used in several session configurations. If the hardware configuration is specified in only one session configuration, delete the hardware configuration while modifying the session configuration.

Gateway Configurations

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.”

Only one gateway can be configured per PC. Information about the gateway is stored in the *AW.BIN* or *AWuserid.BIN* file, depending on whether your installation of Norton pcANYWHERE was for a standalone PC or a network.

New with this release of pcANYWHERE, 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.

One of the benefits of using a Norton pcANYWHERE gateway instead of a modem on an ACS is that any number of off-LAN users can call the same modem. As long as the modem is not in use at the moment the user calls, the user sees a list of available hosts from which to select. When you use an ACS, each modem is dedicated to a particular host, whether or not a call is even made.

This chapter covers:

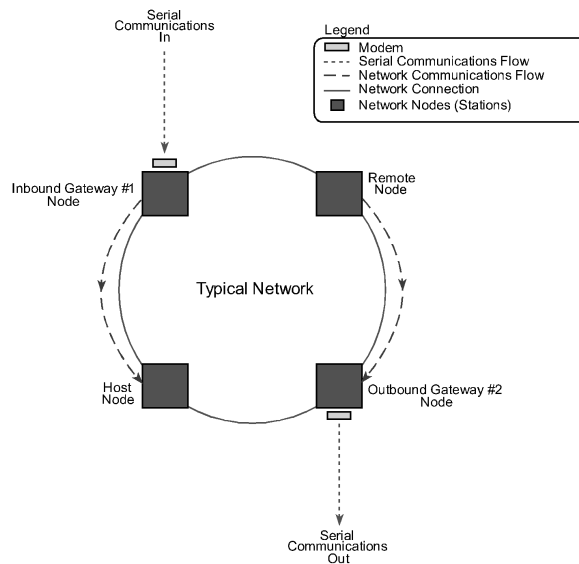
- Gateway concepts
- Setting up a gateway and modifying it
- Activating and deactivating the gateway

Gateway Concepts

A gateway is a small memory-resident program (TSR) that resides on a PC that both is 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 another communications device). Which configuration you designate as the incoming configuration and which you designate as the outgoing configuration is unimportant 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 both an inbound gateway that accepts calls from a modem and sends data over a LAN, and an outbound 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.

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 the network.

Setting Up a Gateway

The network administrator can set up the gateway while remotely controlling the PC, or the user can set it up from the PC.

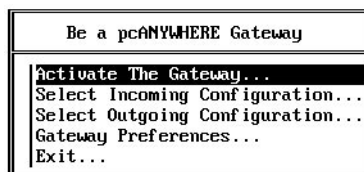
To configure a unidirectional gateway, you must first determine in which direction your gateway is to operate as described in “Gateway Concepts,” the previous section.

To set up a PC on a network with a modem as a gateway:

- 1 While at the PC or remotely controlling it, choose Gateway... from the pcANYWHERE Main menu.

The Be A pcANYWHERE Gateway menu appears along with the gateway status box that shows the current state of the gateway and the hardware configurations set as the incoming and outgoing configurations (Figure 4-2).

Figure 4-2 The status of the gateway may be active or inactive.



```

Gateway status: Inactive
Incoming configuration: Modem
Outgoing configuration: Network
  
```

- 2 Choose Select Incoming Configuration....

The Hardware Configurations menu appears.

- 3 Choose an appropriate configuration. For a unidirectional gateway, choose the device from which the gateway receives information.

The configuration form for the hardware configuration you chose appears.

- 4 Unless you wish to modify this configuration, press Esc to return to the Be A pcANYWHERE Gateway menu.

If you want to modify the configuration you have chosen, see Chapter 3, “Hardware Configurations,” for details.



Network

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.

- 5 Choose Select Outgoing Configuration....

The Hardware Configurations menu appears.

- 6 Choose an appropriate configuration. For a unidirectional gateway, choose the device to which the gateway sends information.

The configuration form for the hardware configuration you chose appears.

- 7 Unless you wish to modify the configuration, press Esc to return to the Be A pcANYWHERE Gateway menu.

- 8 Choose Gateway Preferences....

(You may have to enter the master password before you can see the form.)

The Gateway Preferences form appears (Figure 4-3). For details about setting each preference, see the corresponding procedure in one of the next few sections.

Figure 4-3 Use the Gateway Preferences form to determine how often the gateway accesses the CPU or make the gateway unidirectional.

Gateway Preferences	
Inactivity timeout:	0 minutes (0 for unlimited)
Maximum CPU usage:	7 (1-10, 7 is normal)
Gateway class:	
Bidirectional:	Yes
Load into high memory:	Yes

- 9 Press Esc to exit the menu.

Specifying a Timeout for Inactivity

An inactivity timeout is a number of minutes of inactivity before the gateway automatically ends an idle session. Inactivity is defined as the absence of data transfer. See Chapter 6, “Caller Information and Host Preferences,” or the Glossary for more information about inactivity timeouts.

To specify the inactivity timeout:

- 1 Select Inactivity Timeout from the Gateway Preferences form.
- 2 Type 0 (the default) to indicate no inactivity timeout or a number of minutes of inactivity from 1 to 999, after which the session will end. Then press Enter.

Determining How Often the Gateway Accesses the CPU

To determine how often the gateway accesses the CPU (the PC's central processing unit), you choose a frequency level from 1 to 10. If you choose 10, the gateway uses the CPU every timer tick (approximately once every 55 milliseconds). If you choose 1, the gateway uses the CPU every tenth tick (approximately once every half-second). The default value is 7, which would rarely interfere with the normal use of the PC. The number 10, however, is the best choice for PCs that are dedicated solely to gateway use.

To determine how often the gateway accesses the PC's CPU:

- 1 Select Maximum CPU Usage from the Gateway Preferences form.
- 2 Type a number from 1 to 10 then press Enter. (The default is 7.)

Assigning a Gateway to a Class

You can assign the gateway to a class, or group, of gateways. Classes are commonly based on the speed of the modem. For instance, a network administrator might create a class of 9600-bps gateways called 9600.

To assign the gateway to a class, or group, of gateways:

- 1 Select Gateway Class from the Gateway Preferences form.
- 2 Type a name of up to four characters, then press Enter.

Giving the Gateway a Direction

You can designate the gateway as either a bidirectional or unidirectional gateway.

To indicate whether the gateway is bidirectional or unidirectional:

- 1 Choose Bidirectional from the Gateway Preferences form.
The Make Gateway Bidirectional menu appears.
- 2 Choose No for a unidirectional gateway or Yes (the default) for a bidirectional gateway.

Loading the Gateway into High Memory

Loading the gateway TSR into high memory gives you more efficient use of memory on the PC.

To load the gateway TSR into high memory:

- 1 Choose Load Into High Memory from the Gateway Preferences form.
The Load Into High Memory menu appears.
- 2 Choose No or Yes (the default).

Modifying the Gateway Setup

To modify the gateway's configurations or preferences, follow the procedures in the previous sections. The use of the gateway is suspended while you make changes. If someone else is using the gateway when you choose

Gateway... from the pcANYWHERE Main menu, you see the following warning message:

```
Warning: The gateway is currently active. You may cancel
but this will immediately break the connections to the
host and remote computers. Cancel gateway session:
Yes/No.
```

Canceling the gateway operation at this point will definitely disrupt the gateway users. It may be best to choose No and check again in a few minutes to see if the gateway is inactive.

After making your changes, the gateway must be reactivated.

To reactivate the gateway:

- Choose Activate the Gateway... from the Be A pcANYWHERE Gateway menu.
- Or,
- Press Esc to exit the menu. Norton pcANYWHERE assumes you want to reactivate the gateway and does so.

Starting a Gateway

The gateway can be used only when it is active. After configuring the gateway, you activate it to make it available to all network users running Norton pcANYWHERE.

You may prefer to activate the gateway from the PC's AUTOEXEC.BAT file so you won't have to consciously reactivate the gateway every time the PC is turned on (a cold boot) or restarted (a warm boot). The PC should be restarted whenever the gateway stops working for any reason.

To start the gateway manually:

- Choose Activate The Gateway... from the Be A pcANYWHERE Gateway menu.

CAUTION: When using the network as one of the gateway's two device configurations, make sure you have all the necessary network drivers loaded. If you do not have the network drivers loaded, the gateway TSR will not work properly. If you are using a modem, make sure the modem is installed correctly and turned on.

To start the gateway automatically:

- For network installations of Norton pcANYWHERE, type `pathname\AW_GATE /I:userid` at the DOS prompt. 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. If you have a standalone installation of Norton pcANYWHERE, omit `/I:userid` from the command line.

TIP: For network installations, make sure the PC where the gateway is located has access to the network drive where Norton pcANYWHERE is installed even when its user is not logged in. For example, on Novell networks, users with read-only rights can access the F:\LOGIN drive without being logged in.

Deactivating the Gateway

When you wish to turn off the gateway, you can use the Be A pcANYWHERE Gateway menu or a command-line option.

To deactivate the gateway manually:

- 1 Choose Gateway... from the pcANYWHERE Main menu.
The Be A pcANYWHERE Gateway menu appears.
- 2 Choose Exit And Remove From Memory....

To deactivate the gateway automatically:

- For network installations of Norton pcANYWHERE, type `pathname\AW_GATE /I:userid /C` at the DOS prompt. If you have a standalone installation of Norton pcANYWHERE, omit `/I:userid` from the command line.

Session Configurations and Remote Preferences

5

This chapter explains how to create the remote control and online session configurations your PC will use when it acts as a remote PC. It also covers the preferences you can set to make those sessions operate more smoothly.

Each session configuration should specify all the information Norton pcANYWHERE needs to connect your PC to either a host PC or an online service. Usually you create a session configuration for each computer your PC will connect to while acting as a remote. Each session configuration must include the name of the hardware configuration that the remote PC will use to make the connection. Of the other session configuration options, some apply to both remote control and online sessions, but a few apply to only one type of session or the other. For example, dialing instructions apply to any type of session that uses a modem, but only an online service session requires that you specify a type of terminal emulation.

While a session configuration is for all sessions with a particular host PC or online service, the remote preferences you set for the remote PC are not host-dependent. They may apply to all sessions or all sessions of a certain type (such as all remote control sessions or all online sessions), but the host PC or online service to which you are connected is not important. You (or the host user, when there is one) can reset many of these preferences during a particular session when a preference is not appropriate. See Chapter 7, “Remote Control Sessions,” and Chapter 8, “Online Sessions.” For example, some preferences control how files are transferred during a remote control session. While usually you choose not to overwrite duplicate files, you may need to overwrite those files during a particular file transfer. In this case, you override your usual preference during the session.

Regardless of your setting, some configuration options and session preferences can be put into effect during a remote control session only with the host user’s permission. For example, the host user may not allow you to map drives from the remote PC as additional drives on the host PC. See Chapter 6, “Caller Information and Host Preferences,” for details.

Creating or Modifying Session Configurations

You can connect to a host PC or online service without a session configuration, but if you intend to connect to the same host more than once, you will save time if you have a configuration set up to define that connection.



NETWORK USERS: If your network administrator specified a *shared* session configuration file for remote control sessions during network installation, you cannot add to or modify the configurations. You can access only the hosts specified by your network administrator. You may need to check with your network administrator before attempting to create a configuration.

To create or modify a remote control session configuration:

- 1 Choose Call A pcANYWHERE Host... from the pcANYWHERE Main menu.

The Call A pcANYWHERE Host menu appears.

- 2 Choose View/Modify List of Hosts....

The Host Names menu appears (Figure 5-1). It displays the names of the existing session configurations. It is like a telephone book for the hosts you call and control.

Figure 5-1 The Select Host For Connection menu shows the default remote control session configurations that were created when Norton pcANYWHERE was installed. Your menu may be different.



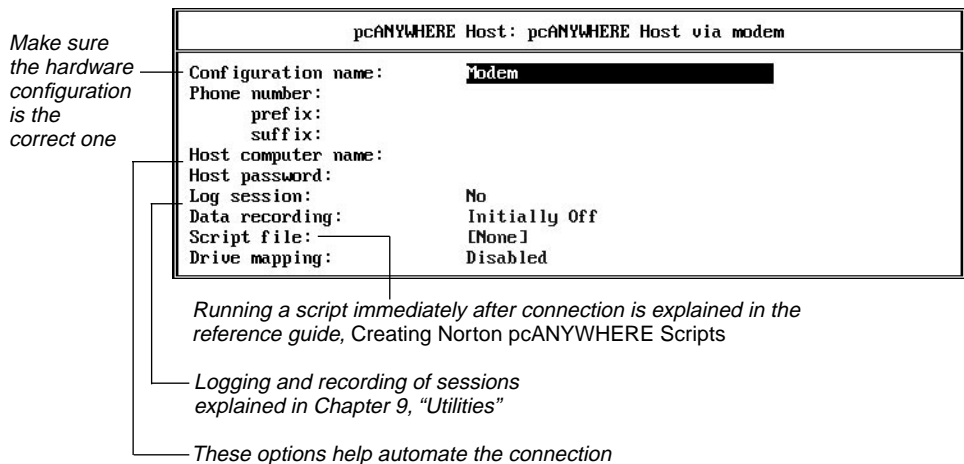
NOTE: This eventually lists all the host PCs that you call. Use it like a telephone book of host PCs.

- 3 Do one of the following:
 - To create a new configuration, press Insert, type a descriptive name for this configuration in the Host Name To Add form, then press Enter.
 - Or,
 - To modify an existing configuration, choose that configuration's name.

TIP: To base a new configuration on an existing one, choose the name of that configuration prior to pressing Insert. (For example, you may want to choose one that already specifies the hardware configuration you intend to use for the new session configuration.)

The session configuration form appears (Figure 5-2). The words "pcANYWHERE Host" and the name for this configuration appear in the form's title. For details about setting each option on the form, see the corresponding procedure in one of the next few sections.

Figure 5-2 Use the session configuration form to let Norton pcANYWHERE know how to connect to a particular host PC.



- 4 Press Esc until you return to a menu you want to use.

To create or modify an online service session configuration:

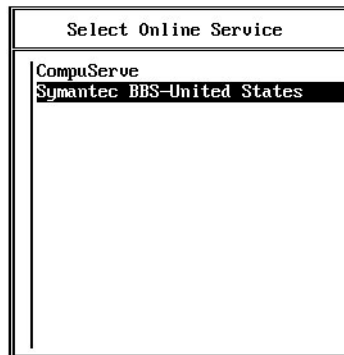
- 1 Choose Call An Online Service... from the pcANYWHERE Main menu.

The Call An Online Service menu appears.

- 2 Choose View/Modify List of Services... to add a session configuration that defines the connection with the new host PC.

The Select Online Service menu appears (Figure 5-3).

Figure 5-3 The Select Online Service menu shows the default online session configurations that were created when Norton pcANYWHERE was installed. Your menu may be different.



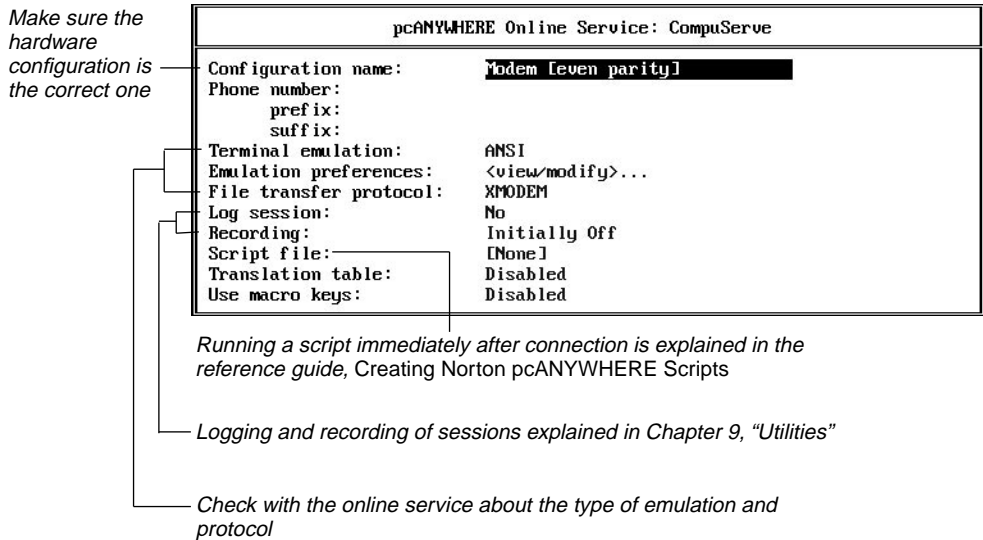
NOTE: This eventually lists all the online services that you call. Use it like a telephone book of services.

- 3 Do one of the following:
 - To create a new configuration, press Insert, type a name for this configuration, then press Enter.
 - Or,
 - To modify an existing configuration, choose that configuration's name then press Enter.

TIP: To base a new configuration on an existing one, choose the name of that configuration prior to pressing Insert. (For example, you may want to choose one that already specifies the hardware configuration you intend to use for the new session configuration.)

The session configuration form appears (Figure 5-4). The words “pcANYWHERE Online Service” and the name for this configuration appear in the form’s title. For details about setting each option on the form, see the corresponding procedure in one of the next few sections.

Figure 5-4 Use the session configuration form to let Norton pcANYWHERE know how to connect to a particular online service.



- 4 Press Esc until you return to a menu you want to use.

Choosing or Changing the Hardware Configuration

Each session configuration, whether for a remote control or an online session, must have a hardware configuration. If the session configuration specifies a hardware configuration that you won't be using, you must change it to the one you will be using.

To choose a hardware configuration:

- 1 Choose Configuration Name from the session configuration form.
The Hardware Configurations menu appears.
- 2 Choose the correct hardware configuration.
The Configuration form appears.

- 3 Press Esc—unless you want to modify this hardware configuration for all the session configurations that use it. (See Chapter 3, “Hardware Configurations,” for details about modifying a configuration or creating a new one.)

Supplying the Telephone Number

Telephone numbers are needed only for remote control or online sessions that connect via a modem. If the telephone number for the host is included in the session configuration, you won't be prompted for it as the session begins.

To supply or change the telephone number for your modem:

- 1 Select Phone Number from the session configuration form.
- 2 Type the telephone number for the host PC, then press Enter.
You can type any prefix or suffix as part of the telephone number. However, if you have already created a list of prefixes and suffixes, go on to steps 3 and 4.
- 3 Choose Prefix or Suffix from the session configuration form.
Depending on which you chose, the Phone Number Prefix or Phone Number Suffix menu appears.
- 4 Choose a prefix or suffix.
The name of the prefix or suffix you choose appears in the session configuration form.
- 5 Repeat steps 3 and 4 if you want both a prefix and a suffix.

See “Creating a Telephone Prefix and Suffix List,” in Chapter 2, “Installation and General Setup Information,” for more information.

Providing the Host's Name and Password

You can automate some of the connection process for a remote control session by entering the host PC's computer name and the password the host PC is expecting from you. The remote's settings for the Host Computer Name and Host Password options must match those defined on the host PC.

You can omit Host Computer Name if there is only one possible host to connect to. If you omit the name when there are several possible hosts, such as on a network, you can choose a host PC from a menu at the time of the connection.

If you omit the password, you will be prompted for it—if it is required in the caller information on the host PC.

To enter the host PC's name and password:

- 1 Select Host Computer Name from the session configuration form.
- 2 Type the host PC's name, then press Enter.
- 3 Select Host Password.
- 4 Type the password that the host is expecting from you, then press Enter.

Mapping Drives

For remote control sessions, you can map your drives to the host PC. Your drives appear as additional drives on the host. For example, if the host does not have a T: drive, you could map the remote's C: drive as the host's T: drive. Then as the remote user, you can type T: at the host's DOS prompt and access the files on your C: drive.

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.

Your settings are ignored if the host PC does not allow drive mapping. See "Feature Preferences" in Chapter 6, "Caller Information and Host Preferences."

To map remote drives to the host PC:

- 1 Choose Drive Mapping from the session configuration form.
The Remote Drive Mapping menu appears.
- 2 Choose Enabled.
The Drive Mapping For Host Applications menu appears.
- 3 Choose the letter for a host drive. This is the letter that the remote drive will have on the host PC. Usually, you choose a letter currently unused by the host PC.
The Remote Drive menu appears showing all the drives available on the remote PC.
- 4 Choose the letter of the remote drive that will be accessed from the host PC.

NOTE: If you wanted your C: drive to be the host's T: drive, you would choose T: in step 3 and C: in step 4.

- 5 Repeat steps 4 and 5 for each remote drive you want to map.

To disable drive mapping:

- 1 Choose Drive Mapping from the session configuration form.
The Remote Drive Mapping menu appears.
- 2 Choose Disabled.

Choosing or Changing the Emulation Type

For online sessions, your PC simulates (*emulates*) the type of terminal required to gain access to the online service. You specify the emulation type that the service is expecting and specify preferences for screen wrapping, line wrapping, the use of the backspace when it is typed from the keyboard, and the interpretation of each transmitted carriage return. These preferences cannot be changed during a session.

To change the default terminal emulation:

- 1 Choose Terminal Emulation from the session configuration form.
The Terminal Emulation menu appears.
- 2 Choose the correct emulation type.

To change terminal emulation preferences:

- 1 Choose Emulation Preferences from the session configuration form.
The Terminal Emulation Session Preferences form appears (Figure 5-5).

Figure 5-5 Set preferences for the terminal emulation.

Terminal Emulation Session Preferences	
Line wrap:	No
Screen wrap:	No
<BS> key:	Non-Destructive
Received <CR>:	CR

- 2 To change the Line Wrap option:
 - a Choose Line Wrap.
The Line Wrap menu appears.

- b** Choose No (the default) if you want the line to end with the last character position in the line.
Or,
Choose Yes if you want lines to wrap to the next line when the number of characters exceeds the length of the line.
- 3** To change the Screen Wrap option (which works only when Line Wrap is On):
 - a** Choose Screen Wrap.
The Screen Wrap menu appears.
 - b** Choose No (the default) if you want the screen to end with the last character position in its line.
Or,
Choose Yes if you want lines to wrap from the bottom of the screen to the top when the number of characters in the last line exceeds the length of the screen.
- 4** To change the use of the backspace key:
 - a** Choose BS Key.
The BS Key menu appears.
 - b** Choose Non-Destructive (the default) if you want pressing the backspace key to simply move the cursor backward *without* deleting any characters.
Or,
Choose Destructive if you want pressing the backspace key to delete the characters to the left of the cursor as the cursor moves backward.
- 5** To change the interpretation of carriage returns that are received from the online service:
 - a** Choose Received CR.
The Received CR menu appears.
 - b** Choose CR (the default) if you want each carriage return to be interpreted as a carriage return only.
Or,
Choose CR/LF if you want each carriage return to be interpreted as a carriage return/linefeed.
- 6** Press Esc to return the session configuration form.

Choosing or Changing the File-Transfer Protocol

Norton pcANYWHERE supports a number of popular file transfer protocols. You can switch from one protocol to another during the session if you need to.

If you select ASCII or ZMODEM, the protocol has a number of preferences you can set. See “ASCII Protocol Preferences” and “ZMODEM Protocol Preferences,” later in this chapter.

To choose the file-transfer protocol:

- 1 Choose File Transfer Protocol from the session configuration form. The Select Protocol menu appears.
- 2 Choose the protocol you want to use during the session.

Specifying Macro Keys

The macro keys can be specified as part of the session configuration or during the session. You assign string expressions to the keys Alt+0 through Alt+9 and store them in a file with the extension .MK6. The string expressions can include control characters, such as ^M for a carriage return or ^J for a linefeed. You can have several .MK6 files, and you can assign the same .MK6 file to more than one session configuration.

NOTE: If you are using macro keys with a direct connection, you need to use a data rate of 19,200 or lower.

To specify or modify a set of macro keys:

- 1 Choose Macro Keys. The Macro Keys menu appears.
- 2 Choose Enabled. The Select Path For Macro Key File form appears.
- 3 You can accept the default directory (where Norton pcANYWHERE is installed) or type the path to a new directory. Then press Enter. Do not include the filename at this step. The Available Files menu appears. The default file is AW.MK6.
- 4 Do one of the following:

- Choose the .MK6 file which contains the macro keys you want to use.
- Press Insert to create a new file for macro keys.
- The Enter File Name form appears. Type the name of the file, then press Enter.

The Macro Keys form displays the macro keys from the selected file. The macro keys are Alt+0 through Alt+9.

- 5 If you want to make additions or modifications:
 - a Select a key.
 - b Type the characters you want to send to the service when the selected key is pressed. Then press Enter.
- 6 Repeat step 5 for any other keys you want add or modify.
- 7 Press Esc to exit the Macro Keys form.

To disable the use of macro keys:

- 1 Choose Macro Keys.
The Macro Keys menu appears.
- 2 Choose Disabled.

Using a Translation Table

Translation tables are used by terminal emulations for character substitutions. When a character is received, the part of the table for received characters is checked. The character's translation is displayed or processed instead of the character itself. The same is true for characters that are being sent, except the part of the table for sent characters is checked. 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 session configuration.

You can also specify, modify, or disable the translation table during the online session.

To specify or modify the translation table:

- 1 Choose Translation Table.
- 2 Choose Enabled.
The Select Path For Translation Table form appears.
- 3 You can accept the default directory (where Norton pcANYWHERE is installed) or type the path to a new directory. Then press Enter.

Do not type the filename at this step.

The Available Files menu appears. The default file is AW.TRN.

4 Do one of the following:

- Choose the .TRN file which contains the translation table you want to use.
- Press Insert to create a new file for a translation table.

The Enter File Name form appears. Type the name of the file then press Enter.

The Translation Table menu appears. Each translation table has two parts: one for received characters, and one for transmitted characters.

5 Choose Receive or Transmit, depending on which part of the table you want to specify or modify.

The Receive Translation Table form or the Transmit Translation Table form appears.

The form displays the hex codes for the 256 characters (00 to FF) in the extended ASCII set (see Appendix B, “Terminal Emulation”). The form has 16 rows and 16 columns; the rows represent the first digits of the hex codes (0 to F) and the columns represent the second digits. As you select a code, the character it represents appears in the upper-right corner of the form. For example, 41 is “A” and 61 is “a”. If you change the hex code 41 to 61 in the Receive Translation Table, “a” will be displayed for every “A” that is received.

- 6** Select the hex code for a character you want to change, then type in the hex code for its translation.
- 7** Repeat step 6 for any characters you want to modify.

8 Repeat steps 5 through 7 for the other translation table form.

9 Press Esc twice to exit.

To disable the use of the translation table:

1 Choose Translation Table.

The Translation Table menu appears.

2 Choose Disabled.

Setting Preferences for the Remote PC

Tables 5-1 and 5-2 show all the preferences that can be set for remote control and online sessions, respectively. When a preference can also be set from the session (as explained in the Alternatives... column of each table), the settings you choose as remote preferences provide only a default environment for a session. When there is no alternative, the setting you provide here is the setting for every session.

When you can change the setting for a preference during a session, you press the remote hotkey and select an option from either the Session Options menu (for remote control sessions) or the Terminal Options menu (for online sessions). For more information, see Chapter 7, “Remote Control Sessions,” and Chapter 8, “Online Sessions.”

Table 5-1 Preferences for Remote Control Sessions

If you are going to...	Set this preference...	On this preference form...	Alternatives...
Display image of host screen on remote PC	Attribute Translation	Remote Control Session Preferences	Can be reset by remote user during a session.
	Blink Attribute Support	Remote Control Session Preferences	Can be reset by remote user during a session.
	Synchronized Screen Display	Remote Control Session Preferences	Can be reset by remote user during a session.
Display graphics from host PC	Full Graphics	Remote Control Session Preferences	Can be reset by remote user during a session.
	Graphics Translation Favor	Remote Control Session Preferences	Can be reset by remote user during a session.

Table 5-1 Preferences for Remote Control Sessions (*continued*)

If you are going to...	Set this preference...	On this preference form...	Alternatives...
Print output	Print Destination	Remote Control Session Preferences	Can be reset by either host or remote user during a session.
	Remote Print Device	Remote General Preferences	No alternative; used for both remote control and online sessions.
Run applications on the host PC (if host makes drive accessible)	Special Keyboard Handler (host user must set type of handler and give you permission to use it)	Remote Control Session Preferences	Use of handler can be disabled and Level of Type 1 handler can be changed by remote user during a session.
Run Windows on the host PC (if installation of correct files performed)	Windows pcANYWHERE Swap File Size	Remote Control Session Preferences	No alternative.
Transfer files (if host makes drive accessible)	Allow Deletion Of Directories	File Transfer Preferences	Can be changed using the menu available from the file transfer window.
Transfer files (if host makes drive accessible)	Compression	File Transfer Preferences	Can be changed using the menu available from the file transfer window.

Table 5-1 Preferences for Remote Control Sessions (*continued*)

If you are going to...	Set this preference...	On this preference form...	Alternatives...
	Crash Recovery	File Transfer Preferences	Can be changed using the menu available from the file transfer window.
	Destination File	File Transfer Preferences	Can be changed by running AWSEND with appropriate command-line option during session. Can also be changed using the menu available from the file transfer window.
Use the hot-key to access the session menu	Remote Hotkey	Remote General Preferences	No alternative; used for both remote control and online sessions.
Use the mouse (if permitted by host)	Acceleration Factor	Mouse Preferences	Can be reset by remote user during a session.
	Double Speed Rate	Mouse Preferences	Can be reset by remote user during a session.
	Remote Mouse Mode	Mouse Preferences	Can be reset by remote user during a session.

Table 5-2 Preferences for Online Sessions

If you are going to...	Set this preference...	On this preference form...	Alternatives...
Use the hotkey to access the session menu	Remote Hotkey	Remote General Preferences	No alternative; used for both remote control and online sessions.
Print output	Remote Print Device	Remote General Preferences	No alternative; used for both remote control and online sessions.
Transfer files using ASCII or ZMODEM as the file transfer protocol	ASCII ZMODEM	ASCII Preferences or ZMODEM Preferences	Can be reset by remote user during a session—if either protocol is being used.

To specify preferences for remote control sessions:

- 1 Choose Call A pcANYWHERE Host... from the pcANYWHERE Main menu.

The Call A pcANYWHERE Host menu appears.

- 2 Choose Remote Preferences....

The Remote Preferences menu appears.

- 3 Do one of the following:

- Choose General....

The Remote General Preferences form appears (Figure 5-6, later in the chapter).

- Choose File Transfer....

The File Transfer Preferences form appears (Figure 5-7, later in the chapter).

- Choose Mouse....

The Mouse Preferences form appears (Figure 5-8, later in the chapter).

- Choose Remote Control Session....

The Remote Control Session Preferences form appears (Figure 5-9, later in the chapter).

- 4 For details about setting each preference on the form, see the corresponding procedure in one of the next few sections.
- 5 Press Esc to exit the File Transfer Preferences form.
The Save Changes menu appears.
- 6 Choose No or Yes.
- 7 Press Esc until you return to a menu you want to use.

To specify preferences for online sessions:

- 1 Choose Call an Online Service... from the pcANYWHERE Main menu.

The Call An Online Service menu appears.

- 2 Choose Online Service Preferences....

The Online Service Preferences menu appears.

- 3 Do one of the following:

- Choose General....

The Remote General Preferences form appears (Figure 5-6, later in the chapter). These are the same general preferences available from the Remote Preferences menu.

- Choose File Transfer Protocol....

The Protocol Preferences menu appears.

- 4 For details about setting each preference on the form, see the corresponding procedure in one of the next few sections.
- 5 Press Esc to exit the File Transfer Preferences form.
The Save Changes menu appears.
- 6 Choose No or Yes.
- 7 Press Esc until you return to a menu you want to use.

Selecting a Hotkey

Pressing the remote hotkey makes the Session Options menu appear on the screen during a remote control session or the Terminal Options menu appear during an online session. These menus allow you to change many of the preferences explained in this chapter.

To change the remote PC's hotkey:

- 1 Choose Remote Hotkey from the Remote General Preferences form (Figure 5-6).

The Remote Hotkey menu appears.

- 2 Choose a new hotkey. (The default is Ctrl+RightShift.)

Figure 5-6 Use the Remote General Preferences form to change the remote PC's hotkey and print device.

Remote General Preferences	
Remote hot key:	Ctrl R-Shift
Remote print device:	LPT1

Selecting a Printing Device

As the remote user, you have two printing preferences to specify:

- You indicate which print device (a port or a spool file) will be used by the remote PC, regardless of the type of session.
- For remote control sessions, you can also specify where the output will go. The host PC's printed output can be discarded, sent to both host and remote printers, or sent to just the host's or the remote's printer. The print destination can be changed during a remote control session.

To change the remote PC's print device:

- 1 Choose Remote Print Device from the Remote General Preferences form (Figure 5-6).

The Remote Print Device menu appears.

- 2 Choose the appropriate print device for your PC from LPT1, LPT2, LPT3, PRN, or Spool File. (The default is LPT1.)

If you choose Spool File, the default spool file AW.SPL is used.

To change the spool file:

- 1 Choose Remote Print Device from the Remote General Preferences form.

The Remote Print Device menu appears.

- 2 Choose Select Spool File....

The Select Path For Spool File form appears.

- 3 Use the default directory (where the pcANYWHERE files are installed) or type in the name of a new one. Then press Enter.
The Available Files menu appears.
- 4 Do one of the following:
 - Choose the .SPL file that you want to use.
 - Press Insert to create a new spool file.
The Enter File Name form appears. Type the name of the file then press Enter.

To specify a print destination:

- 1 Choose Print Destination from the Remote Control Session Preferences form (Figure 5-9).
The Print Options menu appears.
- 2 Choose one of the following:
 - Discard Printer Output (the default). Nothing is printed.
 - Print To Host Only. Output is printed from the host PC.
 - Print To Remote Only. Output is printed from the remote PC.
 - Print To Host And Remote. Output is printed from both the host and remote PCs.

File Transfer Preferences for Remote Control Sessions

The remote PC's file transfer preferences (Figure 5-7) affect AWSEND.EXE, the Norton pcANYWHERE file-transfer program which you can launch during remote control sessions, and background file transfers. For example, the file transfer preferences determine how duplicate files are handled and enable file compression and crash recovery.

For details about how these options can be changed while you are using the file-transfer program or typing the AWSEND command, see "Changing File Transfer Preferences" and "Transferring Files from the DOS Command Line" in Chapter 7, "Remote Control Sessions."

For background file transfers, you must have host permission. See "Allowing Background File Transfers" in Chapter 6, "Caller Information and Host Preferences."

Figure 5-7 Use the File Transfer Preferences form to control a variety of options that affect file transfers.

File Transfer Preferences	
Destination file:	Verify Before Overwriting
Allow deletion of directories:	No
Compression:	Enabled
Crash recovery:	On

Controlling Transfers

This section explains how to use the Destination File preference to control the transfer of duplicate files and the names of transferred files in the destination directory. For example, if you use the setting Always Ask For Destination Name, you can give the transferred file a different name in the destination directory than it had in the source directory.

To change how duplicate files are handled:

- 1 Choose Destination File from the File Transfer Preferences form (Figure 5-7).

The Destination File Options menu appears.

- 2 Choose one of the following:
 - Verify Before Overwriting (the default). During file transfer, you will be asked if a duplicate file is to be overwritten or renamed. You can also cancel the transfer of the duplicate file.
 - Always Overwrite Duplicate Files. Duplicate files are automatically overwritten during a file transfer.
 - Never Overwrite Duplicate Files. Duplicate files are not transferred to the destination directory.
 - Overwrite Older Files Only. Duplicate files are transferred to the destination directory only if they have a more recent date than the file with that name in the destination directory.

To be asked for a file destination for every file:

- 1 Choose Destination File from the File Transfer Preferences form (Figure 5-7).

The Destination File Options menu appears.

- 2 Choose Always Ask For Destination Name. During file transfer, you are asked for the name of each transferred file. If you use a name

that already exists in the destination directory, Norton pcANYWHERE asks you for verification before it overwrites the file.

Allowing Deletions

You may want to delete some files and directories from the remote and host PCs while using the file transfer window during a remote control session. You can only do so if you have selected Yes and given yourself permission.

Despite the setting for this option, if the host user has not given you read/write access to a host drive, you cannot delete files and directories on that particular host drive. See “Restricting Access to Types of Host Drives” in Chapter 6, “Caller Information and Host Preferences.”

To allow directories to be deleted:

- 1 Choose Allow Deletion of Directories from the File Transfer Preferences form (Figure 5-7).
The Allow Deletion of Directories menu appears.
- 2 Choose No (the default) or Yes.

Using Compression

The Compression preference allows you to enable or disable file compression during transfers. When it is enabled, the compression type used is displayed in the file transfer window. You may see:

- Quick. This compresses repeated characters. It is used in network connections and background file transfers. It uses very little memory.
- Maximum (1). This compression method is used when either or both PCs are running an older version of AWSEND.
- Maximum (2). This compression method is new with this version, but can be used only when both PCs are running Norton pcANYWHERE version 5.0.

When file compression is disabled, you see the word Off in the file transfer window.

To enable or disable compression:

- 1 Choose Compression from the File Transfer Preferences form (Figure 5-7).
The Compression menu appears.
- 2 Choose Disabled or Enabled (the default).

Recovering from a Crash

If you allow crash recovery, file transfer will resume at the place in the file where it left off when the crash occurred when more than 10K was transferred successfully. When less than 10K was transferred, information about the file is not saved, and the entire file must be resent.

To enable or disable crash recovery:

- 1 Choose Crash Recovery from the File Transfer Preferences form (Figure 5-7).

The Crash Recovery menu appears.

- 2 Choose Off or On (the default).

Mouse Preferences for Remote Control Sessions

The remote PC's mouse preferences (Figure 5-8) affect the movement of the mouse cursor. For example, they determine its acceleration rate. All of these preferences can be changed during the remote control session.

To use the remote mouse, you must have host permission. See "Allowing the User of the Remote Mouse" in Chapter 6, "Caller Information and Host Preferences."

For details about setting each preference on the form, see the corresponding procedure in one of the next few sections.

Figure 5-8 Use the Mouse Preferences form to control the use of the mouse.

Mouse Preferences	
Acceleration factor:	50 (1-100)
Double speed rate:	50 (1-100)
Remote mouse mode:	Enabled - track always

Changing Acceleration

You can change the acceleration rate, which controls the movement of the mouse cursor in relationship to the movement of the mouse. The range is from 1 to 100 (1 is slowest and 100 is fastest).

To change the acceleration factor:

- 1 Select Acceleration Factor from the Mouse Preferences form (Figure 5-8).
- 2 Type in a number from 1 to 100. (The default is 50.)

Changing the Double-Speed Rate

You can change the double-speed rate, which determines how fast the mouse must move before the mouse cursor switches to *double speed* and moves across the screen faster. The range is from 1 to 100 (1 disables the use of double speed and 100 interprets any movement as double speed).

To change the double speed rate:

- 1 Select Double Speed Rate from the Mouse Preferences form (Figure 5-8).
- 2 Type in a number from 1 to 100. (The default is 50.)

Controlling the Mouse Cursor

You can enable or disable the mouse cursor. This applies only to DOS applications because Windows handles the mouse differently.

To change the mouse cursor's movement (for DOS applications):

- 1 Choose Remote Mouse Mode from the Mouse Preferences form (Figure 5-8).
The Remote Mouse Option menu appears.
- 2 Choose one of the following. (The default is Enabled - Track Always.)
 - Disabled. The mouse cursor is not used.
 - Enabled - Track Always. Two mouse cursors appear on the remote screen. You control the remote mouse and tracking information is continuously sent to the host PC to update the host mouse.
 - Enabled - Track Always, One Mouse. Only the host mouse cursor appears on the remote screen. This can be difficult to use because with slow connections the mouse cursor moves much more slowly than the mouse moves.
 - Enabled - Track When Button Pressed. Two mouse cursors appear on the remote screen, but the host mouse cursor is

updated only when a button is pressed. This option works well with applications that react to the mouse's position only when a button is pressed.

You can experiment with each option to determine which is best for controlling your applications.

Display and Keyboard Preferences for Remote Control Sessions

Several preferences (Figure 5-9) affect the appearance of data and graphics on the screen and one preference affects the use of the keyboard. For example, if the graphics are unclear, you may need to enable the Full Graphics preference.

For details about setting each preference on the form, see the corresponding procedure in one of the next few sections.

Figure 5-9 Use the Remote Control Session Preferences form to control a variety of display preferences.

Remote Control Session Preferences	
Attribute translation:	Yes
Blink attribute support:	Yes
Full graphics:	Yes
Graphics translation favor:	Color
Print destination:	Discard Printer Output
Special keyboard handler:	Disabled
Synchronized screen display:	No
Windows pcANYWHERE swap file size:	640K

Of these preferences, only the swap file size cannot be changed during the session

Translating Attributes

Use the Attribute Translation preference when one PC has a monochrome display and the other has a color display. This preference can be changed during a session.

To translate attributes:

- 1 Choose Attribute Translation from the Remote Control Session Preferences form (Figure 5-9).

The Attribute Translation menu appears.

- 2 Choose No or Yes (the default).

Control Blinking

The Support Blink Attribute preference allows Norton pcANYWHERE to display blinking characters. Set this preference to No only if you experience unexpected blinking during a session. It can also be changed during a session.

To display blinking characters:

- 1 Choose Blink Attribute Support from the Remote Control Session Preferences form (Figure 5-9).
The Blink Attribute menu appears.
- 2 Choose No or Yes (the default).

Using Full Graphics

Use the Full Graphics preference when you want the most accurate representation of DOS graphics as possible. Disable the preference to improve speed, when an approximation of graphics is acceptable. It can also be changed during a session.

To use full graphics:

- 1 Choose Full Graphics from the Remote Control Session Preferences form (Figure 5-9).
The Full Graphics menu appears.
- 2 Choose No or Yes (the default).

Choosing Between Color and Resolution

If the host and remote PCs have different color monitors, their resolutions and the number of colors they can display may be different. You can favor color or favor resolution while translating graphics. This Graphics Translation Favor preference can also be changed during a session.

To favor color or resolution when translating graphics:

- 1 Choose Graphics Translation Favor from the Remote Control Session Preferences form (Figure 5-9).
The Graphics Translation Favor menu appears.

- 2 Choose whichever of the following is most important to you:
 - Color (the default)
 - Resolution

Using a Keyboard Handler

Some host applications handle keyboard input in a non-standard fashion. To operate the host PC effectively in this situation you may need to specify a special keyboard handler. Otherwise, for example, the application may not accept your keystrokes and appear to have crashed. There are two types of handlers, one of which has three levels. As the remote user, you can use or disable the use of the handler specified by the host user. If that handler is the Type 1 handler, you can change the level of it that is used. For example, Level 1 is best for Microsoft editors. See the Glossary for a complete description of the keyboard handlers. This preference can be changed during a session.

To use a special keyboard handler:

- 1 Choose Special Keyboard Handler from the Remote Control Session Preferences form (Figure 5-9).

The Special Keyboard Handler menu appears.
- 2 Choose one of the following:
 - Disabled (the default). No keyboard handler is used.
 - Level 1.
 - Level 2.
 - Level 3.

Synchronizing the Displays

The Synchronized Screen Display preference slows the host application to the rate at which the remote can display screen activity. If this preference is disabled, 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 the characters, such as with a lengthy database indexing procedure, disable this option. This preference can also be changed during a session.

To synchronize the screen displays:

- 1 Choose Synchronized Screen Display from the Remote Control Session Preferences form (Figure 5-9).
The Synchronized Display menu appears.
- 2 Choose No (the default) or Yes.

Swap File Size for Remote Control Sessions

You can specify the size of the swap file (AW.SWP) that Norton pcANYWHERE uses on the remote PC when Windows is executed on the host PC. The size of this file depends on the amount of available space on your hard disk. You should make the file as large as possible to speed updates to the image of the host screen on the remote PC.

To specify the size of the AW.SWP swap file:

- 1 Choose Windows pcANYWHERE Swap File Size from the Remote Control Session Preferences form (Figure 5-9).
The Windows Swap File Size menu appears.
- 2 Choose one of the sizes, which range from 64K to 960K (640K is the default).

NOTE: AW.SWP is stored in the same directory as your configuration files. You can change its location by setting the environment variable AWSWAP to the desired pathname. You can delete AW.SWP from the remote PC when you are not running pcANYWHERE. It will be recreated the next time it is needed.

Setting Protocol Preferences for Online Sessions

If you will use either the ASCII or ZMODEM file transfer protocol during an online session, you need to set preferences for it.

To specify preferences for a protocol:

- 1 Choose File Transfer Protocol... from the Online Service Preferences menu.
- 2 Choose ASCII... or ZMODEM...

The ASCII Preferences form or the ZMODEM Preferences form appears (Figures 5-10 and 5-11, later in this chapter).

- 3 For details about setting each preference on the form, see the corresponding procedure in one of the next few sections.
- 4 Press Esc to exit the preferences form.
The Save Changes menu appears.
- 5 Choose No or Yes.
- 6 Press Esc until you return to a menu you want to use.

ASCII Protocol Preferences

ASCII is a minimal file-transfer protocol that uses no error checking. Use it only when no other protocol is available. Figure 5-10 shows the preferences for the ASCII file-transfer protocol. For details about setting each preference on the form, see the corresponding procedure in one of the next few sections. The settings for these preferences can be changed during a session.

Figure 5-10 The ASCII Preferences form lets you set preferences for the ASCII protocol.

ASCII Preferences	
Character pacing:	0 1/10 seconds
Line pacing:	0 1/10 seconds
Pace character:	0 decimal
Download timeout:	30 seconds
Upload options:	
<CR> translation:	None
<LF> translation:	None
Download options:	
<CR> translation:	None
<LF> translation:	None

Changing the Pace and the Pace Character

You can change the pace at which characters and lines are transmitted, and the character that is used as the pace character between lines. The transmitting computer sends a line then waits for the pace character before sending another line.

To change the pace at which ASCII characters are transmitted:

- 1 Select Character Pacing from the ASCII Preferences form (Figure 5-10).
- 2 Type the number of one-tenths of a second allowed for each character then press Enter. (The default is 0 seconds which does not set a pace.)

To change the pace at which lines of ASCII characters are transmitted:

- 1 Select Line Pacing from the ASCII Preferences form (Figure 5-10).
- 2 Type the number of one-tenths of a second allowed for each line, then press Enter. (The default is 0 seconds which does not set a pace.)

To set the pace character:

- 1 Select Pace Character from the ASCII Preferences form (Figure 5-10).
- 2 Type the ASCII value for the character you want to use, then press Enter. (The default is 0 which does not set a character.)

Setting a Timeout for Downloading Files

You can set the download timeout—the number of seconds of idleness after which the downloading will be terminated.

To set the download timeout:

- 1 Select Download Timeout from the ASCII Preferences form (Figure 5-10).
- 2 Type the number of seconds you want for the timeout, then press Enter. (The default is 30 seconds.)

Translating Carriage Returns and Linefeeds

You decide how carriage returns are translated while either uploading or downloading. For example, if the lines of data in a host file end with single carriage returns, you may want to interpret each carriage return as a carriage return/linefeed when downloading the file. Then you can view the file correctly in your editor. If the data files on the host computer end lines with single carriage returns, you may want to strip the linefeeds when uploading files.

To decide how ASCII carriage returns are translated:

- 1 Choose either the upload or download CR Translation option from the ASCII Preferences form (Figure 5-10).
The Translation menu appears.
- 2 Choose one of the following:
 - None (the default). This translates a carriage return as a carriage return.

- Strip. This deletes all the carriage returns.
- Add LF. This adds a linefeed after each carriage return.

To decide how ASCII linefeeds are translated:

- 1 Choose either the upload or download LF Translation option from the ASCII Preferences form (Figure 5-10).

The Translation menu appears.

- 2 Choose one of the following:
 - None (the default). This translates a linefeed as a linefeed.
 - Strip. This deletes all linefeeds.
 - Add CR. This adds a carriage return before each linefeed.

ZMODEM Protocol Preferences

The ZMODEM protocol is commonly used by online services. It is preferable to the ASCII protocol because it has error-checking and other useful features not available with the ASCII protocol. Figure 5-11 shows the preferences for the ZMODEM file-transfer protocol. For details about setting each preference on the form, see the corresponding procedure in one of the next few sections. The settings for these preferences can be changed during a session.

Figure 5-11 The ZMODEM Preferences form lets you set preferences for the ZMODEM protocol.

ZMODEM Preferences	
Error checking method:	32-bit CRC
Crash recovery:	On
Data window:	None
Allow auto downloading:	Yes

Choosing the Error-Checking Method

You can choose either the 15-bit or 32-bit CRC error-checking methods. The more accurate, but slower, method is 32-bit.

To change the ZMODEM error checking method:

- 1 Choose Error Checking Method from the ZMODEM Preferences form (Figure 5-11).

The Error Checking Method menu appears.

- 2 Choose one of the following:
 - 16-bit CRC
 - 32-bit CRC (the default)

Allowing Crash Recovery

If you allow crash recovery, file transfer can resume at the place in the file where it left off when the crash occurred.

To allow crash recovery:

- 1 Choose Crash Recovery from the ZMODEM Preferences form (Figure 5-11).
The Crash Recovery menu appears.
- 2 Choose one of the following:
 - On (the default). This retains the information necessary to complete the transfer. Partially received files are saved so you can continue where you left off.
 - Protect. This does not re-transfer incomplete files. The partially transferred file is left in the destination directory.
 - Overwrite. This re-transfers entire incomplete files. It doesn't start where it left off.

Sizing the Window for Data to be Transmitted

The transmitting computer waits for acknowledgment of each buffer or window's contents before sending more data. When few transmission errors occur, as when you use a modem with error-checking, data is transmitted more quickly without a window. When using a window for the most possible accuracy, the larger the window the better, because there are fewer acknowledgments to make. Try the 4K window, then reduce to the 2K window if you have problems. With non-error-checking modems, you may want to use a 2K window so a smaller amount of data is retransmitted.

To specify the size of a data buffer or window:

- 1 Choose Data Window from the ZMODEM Preferences form (Figure 5-11).
The Data Window menu appears.
- 2 Choose one of the following:

- None (the default). This is the fastest if few transmission errors occur.
- 2K Window. The size of the window is 2K.
- 4K Window. The size of the window is 4K.

Downloading Files Automatically

When you download files, ZMODEM can start the transfer automatically. You tell the online service what you want to download and the status box for ZMODEM appears.

To automatically download files transferred with the ZMODEM protocol:

- 1 Choose Allow Auto Downloading from the ZMODEM Preferences form (Figure 5-11).
The Allow Auto Downloading menu appears.
- 2 Choose No or Yes (the default).

Caller Information and Host Preferences

6

When your PC is acting as a host PC, you can control which remote users are allowed access to it. You can also stipulate what privileges each user will have. For example, you can make all remote users identify themselves with the same password or with separate passwords, have the host PC call users back, set a time limit for the session, and control the types of drives the users can access.

To treat each user or group of users differently, you create a caller information configuration for each.

When you want all users to have the same privileges, you use the default caller information form. The default caller information form that comes with Norton pcANYWHERE allows anyone complete control of your PC without a password. You can modify this form to suit your needs.

This chapter explains how to:

- Create individual caller information configurations.
- Redefine the default caller information form.
- Set other host preferences, such as the number of attempts allowed to enter a password. These preferences apply to all remote users.

Table 6-1 shows how the host user can control the remote control session—even when the session is unattended.

Table 6-1 Setting Host Preferences

If you want to...	Set this preference...	On this preference form...	Comments or Alternatives...
Blank the host screen	Allow Caller To Blank Host Screen	Caller Information	If set, remote user can blank screen during session.
	Blank Host Screen	Security	
Call a remote user	Default Phone Number Prefix Suffix	General	

Table 6-1 Setting Host Preferences (*continued*)

If you want to...	Set this preference...	On this preference form...	Comments or Alternatives...
Call a remote user back	Callback Phone Number Prefix Suffix	Caller Information	
	Callback Remote User	Caller Information	
	Delay Before Callback Attempted	General	
Use the same caller information for everyone	Default Caller Entry	Security	
Use a caller information configuration per user or group	Use Caller Information List	Security	
Execute a DOS command automatically	Command To Execute	Caller Information	If used, AWLOGOFF must be executed or host must be rebooted at end of session.
Display graphics	Advanced Graphics Mode Detection	Features	
Update the display quickly	Allow Scanning While Host Is Busy	Features	
	Maximize Display Speed	Features	
	Time Between Host Screen Scans	General	
Assign drive privileges	Allow Drive Security	Features	
	Drive Security	Caller Information	
Use third-party data encryption	Use Data Encryption	Security	

Table 6-1 Setting Host Preferences *(continued)*

If you want to...	Set this preference...	On this preference form...	Comments or Alternatives...
Let remote user halt programs	Allow Use Of Ctrl+Break	Caller Information	
Change host mode	Allow Caller To Change Host Mode	Caller Information	If set, at end of session, remote user can choose host mode.
	Reboot On Disconnect	Security	Rebooting can reset host mode if AUTOEXEC.BAT launches host TSR.
Change hotkey	Host Hotkey	General	
Control inactivity timeout	Allow Any Password On Reconnect	Security	Otherwise, remote user can only use last or master password after inactivity timeout or abnormal disconnection.
	Caller Subject To Inactivity Timeout	Caller Information	
	Inactivity Timeout	Security	
Control keyboard	Active Keyboards During Session	Security	Host user can enable or disable remote user's keyboard during the session.
	Lock Host While Waiting	Security	Host keyboard is locked anytime host PC is put in waiting mode.

Creating or Modifying Caller Information Configurations

For security reasons, you will probably want to create a caller information configuration for each user or group of users that will use your PC as a host.



Network

NETWORK USERS: Sometimes the network administrator specifies that the caller information 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.

To create or modify an individual caller information configuration:

- 1 Choose Be A Host... from the Norton pcANYWHERE Main menu.
The Be A pcANYWHERE Host menu appears.
- 2 Choose Caller Information...
The Caller Names menu appears.
- 3 Do one of the following:
 - To create a new configuration, press Insert, type a name for this configuration, then press Enter.

Or,

 - To modify an existing configuration, choose that configuration's name.

TIP: If a new configuration will be very similar to another, choose the name of that configuration prior to pressing Insert.

The caller information configuration form appears (Figure 6-1). The words "Caller Information for" and the name for this particular configuration appear in the form's title.

Figure 6-1 Use the caller information configuration form to specify what a remote user can and cannot do.

Caller Information for: joan

Password: *****

Allow caller to blank host screen: Yes

Allow caller to reboot host: Yes

Allow use of <Ctrl><Break>: <Ctrl>-C And <Ctrl><Break>

Allow special keyboard handler: Yes

Allow caller to change host mode: Yes

Caller subject to inactivity time: No

Log calls from this caller: No

Time allowed online: 0 min (0=unlimited)

Command to execute:

Drive security: Disabled

Callback remote user: Yes

Callback phone number: 917146438973

prefix:

suffix:

(If you leave the callback number blank, the caller will be asked for the number after the connection is made.)

— Logging sessions is explained in Chapter 9, “Utilities”

- 4 For details about setting each option on the form, see the corresponding procedure in one of the next few sections. To log sessions, see “Logging Remote Control and Online Sessions” in Chapter 9, “Utilities.”
- 5 Press Esc until you return to a menu you want to use.
If No is the current setting for the Use Caller Information List option (a host security preference explained in “Security Preferences,” later in this chapter), the Use Caller Information List menu appears as you exit from Caller Names menu.
- 6 Choose Yes if the menu appears.

Setting a Password for a Remote User

Each caller information configuration requires a unique password of up to 16 characters.

To assign a password:

- 1 Select Password from the caller information form (Figure 6-1).
There is no default password.
- 2 Type in up to 16 characters, then press Enter.
The password setting becomes hidden by asterisks (*).

Allowing the User to Blank the Host Screen

You can allow the remote user to blank the host screen, making it visible only on the remote PC. The remote user can blank the screen during a session. See “Blanking the Host Screen,” later in this chapter if you want the host screen blanked automatically for all remote control sessions.

To allow the remote user to blank the host screen:

- 1 Choose Allow Caller To Blank Host Screen from the caller information form (Figure 6-1).
The Allow Caller To Blank Host Screen menu appears.
- 2 Choose No or Yes (the default).

Allowing the User to Reboot the Host

You can allow the remote user to reboot the host PC. The remote user can reboot the host during a session or at the end of the session.

To allow the remote user to reboot the host PC:

- 1 Choose Allow Caller To Reboot Host from the caller information form (Figure 6-1).
The Allow Caller To Reboot Host menu appears.
- 2 Choose No or Yes (the default).

Allowing the Use of Ctrl+Break and Ctrl+C

Depending on your setting for Allow Use of Ctrl+Break, the remote user can halt programs running on the host PC by pressing Ctrl+C and/or Ctrl+Break during the session.

To allow the remote user to halt applications running on the host PC:

- 1 Choose Allow Use Of Ctrl+Break from the caller information form (Figure 6-1).
The Allow Use Of Ctrl+Break menu appears.
- 2 Choose one of the following:
 - No. This prevents the remote user from using Ctrl+C or Ctrl+Break to halt programs.
 - Ctrl+C Only.
 - Ctrl+C and Ctrl+Break (the default).

Allowing the Use of Keyboard Handlers

You can allow the remote user to use the special keyboard handler you have selected. For example, a handler may be required for some Microsoft editors. For more information about keyboard handlers, see the Glossary. To select the handler, see “Specifying the Type of Keyboard Handler” later in this chapter.

To allow the remote user to use special keyboard handlers:

- 1 Choose Allow Special Keyboard Handler from the caller information form (Figure 6-1).
The Allow Special Keyboard Handler menu appears.
- 2 Choose No or Yes (the default).

Allowing the User to Change the Host Mode

You can allow the remote user to change the host mode (the mode in which the host PC waits for a connection). As the session ends, this option allows the remote user to select the host mode or disable the host PC for future incoming calls.

To allow the remote user to change the mode in which the host PC waits for a connection:

- 1 Choose Allow Caller To Change Host Mode from the caller information form (Figure 6-1).
The Allow Caller To Change Host Mode menu appears.
- 2 Choose No or Yes (the default).

Ending the Session Because of Inactivity

You can cause the remote control session to end automatically because of inactivity when no screen data has changed and no keystrokes have been entered for some time. While you control whether or not a particular user is subject to activity timeouts here, the number of minutes for the inactivity timeout is set as a host security preference. See “Security Preferences,” later in this chapter, to set the amount of time.

To end the session because of inactivity:

- 1 Select the Caller Subject To Inactivity Timeout from the caller information form (Figure 6-1).

The Caller Subject To Inactivity Timeout menu appears.

- 2 Choose No (the default) or Yes.

Specifying a Time Limit for the Session

You can limit the amount of time the remote user can use the host PC. When the time limit expires, Norton pcANYWHERE automatically ends the remote control session.

To set a time limit for host use:

- 1 Select Time Allowed Online from the caller information form (Figure 6-1).
- 2 Type a number of minutes from 0 to 9999, then press Enter. Zero (the default) means an unlimited amount of time.

Executing a Command Automatically

You can specify a command to be executed immediately after the remote user makes a connection. For example, you may want to launch a word processor or spreadsheet application for the user. If the remote PC will be running an automated procedure, you can allow file transfers by making this command AWSEND.

When a command is executed in this way, the session must end in one of the following ways:

- The remote user uses the AWLOGOFF program to end the session
- The remote user reboots the host PC
- The host PC is rebooted automatically

To execute a command when the connection occurs:

- 1 Select Command To Execute from the caller information form (Figure 6-1).
There is no default.
- 2 Type a DOS command, then press Enter.

Securing Host Drives

You can restrict the types of drives available to the remote user. For example, you 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. A features preference enables and disables the use of drive restrictions in general. See “Allowing Drive Security” later in this chapter.

To restrict the drives available to the remote user:

- 1 Choose Drive Security from the caller information form (Figure 6-1).

The Drive Security menu appears.

- 2 Do the bulleted step below or substeps a through e:

- Choose Disabled (the default) to allow access to all drives.

Or,

- a Choose Enabled to restrict this remote user's use of the drive.

The Host Drive Security form appears.

- b Choose one of the types of drives: Floppy Drives, Fixed Drives, or Network Drives.

Depending on your choice, the Floppy Drive Access, Fixed Drive Access, or Network Drive Access menu appears.

- c Choose the type of access you want the remote user to have: No Access (the default), Read-Only, or Read/Write.

- d Repeat steps b and c for additional types of drives.

- e Press Esc to return to the caller information form.

Calling the Remote User Back

When the connection is made using a modem, the host PC can call the remote user back. A callback is useful when communications lines must be available to outside users, data must be protected from unauthorized intruders, or the call is to be paid for by the host. The host PC hangs up upon connection and dials the remote user at the specified telephone number.

If a number is not specified, the host PC will prompt the remote user for a phone number when the original connection is made. Asking the user for the number changes this feature from a security option to a billing option.

If you want to specify a number of seconds as a delay before the host PC makes the call back to the remote PC, you set the Delay Before Callback Attempted option, which is on the Host General Preferences form. See “Specifying a Wait Before a Callback,” later in this chapter.

To have the host PC call the remote user back:

- 1 Choose Callback Remote User from the caller information form (Figure 6-1).

The Callback Remote User menu appears.

- 2 Choose No (the default) or Yes.

The Callback Phone Number option is automatically selected from the caller information form (Figure 6-1).

- 3 Type the telephone number for the host PC, then press Enter. (If left blank, the remote user will be asked for the telephone number after the connection is made.)

You can type any prefix or suffix as part of the telephone number. However, if you have already created a list of prefixes and suffixes, perform steps 4 and 5.

- 4 Choose Prefix or Suffix from the caller information form.

The Phone Number Prefix or Phone Number Suffix menu appears.

- 5 Choose a prefix or suffix.

The name of the prefix or suffix you chose appears in the caller information form.

- 6 Repeat steps 4 and 5 if you want both a prefix and a suffix.

See “Creating a Telephone Prefix and Suffix List,” in Chapter 2, “Installation and General Setup Information,” for more information.

Defining Default Caller Information

When the default caller information form is used (as it is when you first install Norton pcANYWHERE and any other time the use of the caller information configurations is disabled), the settings for options in the default caller information form apply to all remote users. For example, if you set a password, all remote users must know it to access your PC as a host. Unlike caller information configurations, a password is not required for the default caller information form.



NETWORK USERS: The settings for the default caller information form are always stored in a personal file, so you can make changes to it if you want to.

To change the default caller information form:

- 1 Choose Be A Host... from the pcANYWHERE Main menu.
The Be A pcANYWHERE Host menu appears.
- 2 Choose Host Preferences....
The Host Preferences menu appears.
- 3 Choose Security....
The Host Security Preferences form appears.
- 4 Choose Default Caller Entry.
The default caller information form appears.
- 5 Follow the procedures in “Creating or Modifying Caller Information Configurations,” earlier in this chapter. To log sessions, see “Logging Remote Control and Online Sessions” in Chapter 9, “Utilities.”
- 6 Press Esc to exit the default caller information form.
The Save Changes menu appears.
- 7 Choose No or Yes.
- 8 Press Esc until you return to a menu you want to use.

Setting Host Preferences

As the host user, you can place restrictions on the remote user and modify certain host functions. If you think of the host PC as an electronic innkeeper, and remote users as guests, then the host preferences are the house rules. Once set, these preferences affect *every* remote control session using the PC as a host.

Host preferences fall into three categories: features, general, and security preferences.

The features preferences affect how the host screen is displayed and updated, how keystrokes and mouse movements from the remote PC are interpreted, whether or not drives can be mapped, and how file transfers are done.

The general preferences provide a default phone number for calling a remote PC, set time limits, specify the host PC's hotkey, and determine if the host will be loaded into high memory.

Some security preferences determine whether or not the remote user can blank the host screen, reboot the host, or encrypt data. Others regulate the

input of passwords and the display of prompts, the use of caller information and caller information defaults, and which keyboards are active. Still others control whether or not the host is locked while waiting for a connection and if the session will be ended because of inactivity. Even though the logging of failed connections is a security preference, it is explained in “Logging Remote Control and Online Sessions” in Chapter 9, “Utilities,” where you will find all the information about logging sessions.

Features Preferences

The features preferences control the display of the host screen, the interpretation of keystrokes and mouse movements, drive mapping, and file transfers.

To configure the host features preferences:

- 1 Choose Be A Host... from the pcANYWHERE Main menu.
The Be A pcANYWHERE Host menu appears.
- 2 Choose Host Preferences....
The Host Preferences menu appears.
- 3 Choose Features....
The Host Features Preferences form appears (Figure 6-2).

Figure 6-2 Use the Host Features Preferences form to control operation during a remote control session.

Host Features Preferences	
Advanced graphics mode detection:	No
Allow scanning while host busy:	Yes
Allow pop-up file transfer:	No
Allow remote drive mapping:	No
Allow remote mouse:	Yes
Maximize display speed:	No
Special keyboard handler type:	Type 1
Allow drive security:	Yes

- 4 For details about setting each preference on the form, see the corresponding procedure in one of the next few sections.
- 5 Press Esc to exit the Host Features Preferences form.
The Save Changes menu appears.
- 6 Choose No or Yes.
- 7 Press Esc until you return to a menu you want to use.

Detecting Non-Standard Graphics

The host PC can detect non-standard graphics in DOS applications. Use this feature only when the graphics from a host application are difficult to view because this feature slows Norton pcANYWHERE down.

To detect non-standard graphics in DOS applications:

- 1 Choose Advanced Graphics Mode Detection from the Host Features Preferences form (Figure 6-2).

The Advanced Graphics Mode Detection menu appears.

- 2 Choose No (the default) or Yes.

Updating the Remote Display

The following preferences affect updates to the image of the host screen displayed on the remote PC.

- Allow Scanning While Host Busy. To keep the display as current as possible, you can scan for updates while the host is busy, or you can wait until the host is done and then update the screen.
- Maximize Display Speed. Norton pcANYWHERE uses a compression technique when sending data to the remote PC. However, you can speed up 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 affect on Windows or on DOS text-mode applications.) It increases the size of the host TSR by 46K.

To scan the host screen for updates while the host is processing:

- 1 Choose Allow Scanning While Host Busy from the Host Features Preferences form (Figure 6-2).

The Scan When Host Is Busy menu appears.

- 2 Choose No or Yes (the default).

To maximize display speed:

- 1 Choose Maximize Display Speed from the Host Features Preferences form (Figure 6-2).

The Maximize Display Speed menu appears.

- 2 Choose No (the default) or Yes.

Allowing Background File Transfers

If you allow background file transfers, the remote user can perform file transfers at any time—even when another application is running on the host PC. Using this feature requires 17K of extra memory. It adds File Transfer... to the remote user's Session Options menu.

To perform file transfers at any time:

- 1 Choose Allow Pop-Up File Transfer from the Host Features Preferences form (Figure 6-2).
The Allow Background File Transfer menu appears.
- 2 Choose No (the default) or Yes.

Allowing Drive Mapping

You can allow the remote PC to map its drives to the host PC. 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” in Chapter 5, “Session Configurations and Remote Preferences.”

To allow the remote PC to map its drives to the host PC:

- 1 Choose Allow Remote Drive Mapping from the Host Features Preferences form (Figure 6-2).
The Allow Remote Drive Mapping menu appears.
- 2 Choose No (the default) or Yes.

Allowing the Use of the Remote Mouse

You can allow the remote user to use his or her mouse in DOS applications run on the host. Using this feature requires 1K of extra memory. The remote user controls the acceleration rate of the mouse cursor and so forth. See “Mouse Preferences for Remote Control Sessions,” in Chapter 5, “Session Configurations and Remote Preferences.”

To allow remote users to use their mouse devices with DOS applications:

- 1 Choose Allow Remote Mouse from the Host Features Preferences form (Figure 6-2).
The Allow Remote Mouse menu appears.
- 2 Choose No or Yes (the default).

Specifying the Type of Keyboard Handler

You choose which of the two special keyboard handlers will be used on the host PC. A handler is needed only for certain applications (most notably many 3270 terminal emulation programs). 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. 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. For more details, see *keyboard handler* in the Glossary. To allow the use of the selected handler, see “Allowing the Use of Keyboard Handlers,” earlier in this chapter.

To use a special keyboard handler on the host PC:

- 1 Choose Special Keyboard Handler Type from the Host Features Preferences form (Figure 6-2).

The Special Keyboard Handler Type menu appears.

- 2 Choose one of the following:
 - None. No keyboard handler will be used.
 - Type 1 (the default).
 - Type 2.

Allowing Drive Security

If you allow drive security, you can restrict the remote user’s access to particular types of host drives. Drive security requires about 1K of extra memory.

The access to the drives is set in the caller information form. See “Securing Host Drives,” earlier in the chapter.

To allow the use of drive security:

- 1 Choose Allow Drive Security from the Host Features Preferences form (Figure 6-2).

The Allow Drive Security menu appears.

- 2 Choose No or Yes (the default).

General Preferences

The General preferences provide a default phone number for calling a remote PC, set time limits, specify the host PC's hotkey, and determine if the host will be loaded into high memory.

To configure the host general preferences:

- 1 Choose Be A Host... from the pcANYWHERE Main menu.
The Be A pcANYWHERE Host menu appears.
- 2 Choose Host Preferences....
The Host Preferences menu appears.
- 3 Choose General...
The Host General Preferences form appears (Figure 6-3).

Figure 6-3 The Host General Preferences form lets you control a variety of preferences.

Select Online Service
CompuServe
Symantec BBS-United States

- 4 For details about setting each preference on the form, see the corresponding procedure in one of the next few sections.
- 5 Press Esc to exit the Host General Preferences form.
The Save Changes menu appears.
- 6 Choose No or Yes.
- 7 Press Esc until you return to a menu you want to use.

Setting a Default Telephone Number

Use the telephone number of the remote user you call most often as the default telephone number. Each time you call a remote PC, the default number appears on the screen. You can change it when it is not the number you want to call.

To set a default telephone number for calls to remote PCs:

- 1 Select Default Phone Number from the Host General Preferences form (Figure 6-3).

- 2 Type the telephone number for the remote then press Enter.
There is no default.

You can type any prefix or suffix as part of the telephone number. However, if you have already created a list of prefixes and suffixes, perform steps 3 and 4.

- 3 Choose Prefix or Suffix from the Host General Preferences form.
The Phone Number Prefix or Phone Number Suffix menu appears.

- 4 Choose a prefix or suffix.
The name of the prefix or suffix you choose appears in the Host General Preferences form.

- 5 Repeat steps 3 and 4 if you want both a prefix and a suffix.

See “Creating a Telephone Prefix and Suffix List,” in Chapter 2, “Installation and General Setup Information,” for more information.

Changing the Host Hotkey

You can set the host hotkey that displays the Host Session Options menu.

To change the host PC's hotkey:

- 1 Choose Host Hotkey from the Host General Preferences form (Figure 6-3).

The Host Hotkey menu appears.

- 2 Choose a new hotkey. The default is Alt+RightShift.

Using High Memory

If you decide to use high memory, as many segments of the host TSR as possible will be loaded into upper memory blocks.

To load the host TSR into high memory:

- 1 Choose Load Host Into High Memory from the Host General Preferences form (Figure 6-3).

The Load Host Into High Memory menu appears.

- 2 Choose No or Yes (the default).

Setting a Scan Interval

You can control the interval between scans. Scanning updates the host screen displayed on the remote PC.

To control the interval between scans:

- 1 Select Time Between Host Screen Scans from the Host General Preferences form (Figure 6-3).
- 2 Type in a number from 1 to 99 then press Enter. (The default is 10 which is approximately .5 seconds.) The number becomes the number of 55-millisecond delays between scans.

Specifying a Wait Before a Callback

You can control how long the host waits before making a callback. This setting is meaningless unless the caller information specifies a callback. See “Calling the Remote User Back,” earlier in this chapter.

To control how long the host waits before making a callback:

- 1 Select Delay Before Callback Attempted from the Host General Preferences form (Figure 6-3).
- 2 Type in a number of seconds from 5 to 99 then press Enter. (The default is 10.)

Security Preferences

Some security preferences determine whether or not the remote user can blank the host screen, reboot the host, or encrypt data. Others regulate the input of passwords and the display of prompts, the use of caller information and caller information defaults, the logging of failed connections, and which keyboards are active. Still others control whether or not the host is locked while waiting for a connection and if the session will be ended for inactivity.

To configure the host security preferences:

- 1 Choose Be A Host... from the pcANYWHERE Main menu.
The Be A pcANYWHERE Host menu appears.
- 2 Choose Host Preferences....
The Host Preferences menu appears.
- 3 Choose Security....
The Host Security Preferences form appears (Figure 6-4).

Figure 6-4 The Host Security Preferences menu lets you control a variety of preferences.

Host Security Preferences	
Reboot on disconnect:	No
Use caller information list:	Yes
Default caller entry:	<view/modify>...
Allow any password on reconnect:	No
Passwords are case sensitive:	No
Password attempts allowed:	3 (0 for unlimited)
Password entry timeout:	3 minutes
Log failed connections:	No
Active keyboards during session:	Host And Remote
Inactivity timeout:	0 minutes (0 for no timeout)
Blank host screen:	No
Lock host while waiting:	No
Prompt on connection:	No
Prompt timeout:	5 seconds (range: 5-120)
Use data encryption:	No

— Logging is explained in Chapter 9, "Utilities"

— See "Defining Default Caller Information," earlier in this chapter

- 4 For details about setting each preference on the form, see the corresponding procedure in one of the next few sections. To log failed connections, see "Logging Remote Control and Online Sessions" in Chapter 9, "Utilities."
- 5 Press Esc to exit the Host Security Preferences form.
The Save Changes menu appears.
- 6 Choose No or Yes.
- 7 Press Esc until you return to a menu you want to use.

Automatically Reboot the Host PC

You can reboot the host PC automatically 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. When rebooting is enabled, Norton pcANYWHERE is often launched on the host PC from the AUTOEXEC.BAT file.

TIP: If you usually perform remote tasks with long processing times, such as operations on large database files, you may want to specify 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. This also prevents data loss if there is unsaved data at the time of an unexpected interruption.

To allow the remote user to reboot the host on disconnection:

- 1 Choose Reboot On Disconnect from the Host Security Preferences form (Figure 6-4).

The Reboot On Disconnect menu appears.

- 2 Choose one of the following:
 - No (the default). If No is selected, the host PC will never automatically reboot.
 - Yes - Coldboot Always.
 - Yes - Warmboot Always.
 - Yes - Coldboot If Connection Lost.
 - Yes - Warmboot If Connection Lost.

Specifying What Caller Information to Use

You can use individual caller information configurations or the setting in the default caller information form. When the caller information configurations are not used, the settings in the default caller information form apply to all connections.

To use caller information configurations:

- 1 Choose Use Caller Information List from the Host Security Preferences form (Figure 6-4).

The Use Caller Information List menu appears.

- 2 Choose No (the default) or Yes.

Managing Passwords

When it comes to passwords, you can:

- Determine what passwords are accepted after an inactivity timeout or an abnormal disconnection. You can stipulate that the only passwords used to reconnect are the host's master password or the most recently used password. If it is not necessary to protect the previous remote user in this way, you can allow any valid password to connect to the host PC.
- Make all passwords either case-sensitive or insensitive. When the passwords are case-sensitive, the correct combination of uppercase and lowercase letters must be entered.
- Limit the number of attempts to enter a password. The default value is three attempts, and zero indicates an unlimited number of retries.
- Limit the amount of time for entering a password. The default value is three minutes.

Passwords are specified as part of the caller information. See "Setting a Password for a Remote User," earlier in this chapter. Creating a master password is part of the system setup. See "Security" in Chapter 2, "Installation and General Setup."

To determine what passwords are accepted after an inactivity timeout or abnormal disconnection:

- 1 Choose Allow Any Password On Reconnect from the Host Security Preferences form (Figure 6-4).

The Allow Any Password On Reconnect menu appears.

- 2 Choose No (the default) if only the master and the most recently used password are acceptable.

Or,

Choose Yes if any valid password can be used.

To make passwords case-sensitive:

- 1 Choose Passwords Are Case Sensitive from the Host Security Preferences form (Figure 6-4).

The Passwords Are Case Sensitive menu appears.

- 2 Choose No (the default) or Yes.

To limit the number of attempts to enter a password:

- 1 Select Password Attempts Allowed from the Host Security Preferences form (Figure 6-4).
- 2 Type in a number of attempts from 0 to 99 then press Enter. The default is 3.

To limit the amount of time for entering a password:

- 1 Select Password Entry Timeout from the Host Security Preferences form (Figure 6-4).
- 2 Type in a number of minutes from 1 to 99 then press Enter. (The default is 3.)

Setting a Time Limit for Inactivity

You can specify the time length for an inactivity timeout. If this value is not zero, 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 when done using the host PC or when the host PC crashes. Whether or not the time limit is enforced for a particular remote user depends on the setting for Caller Subject to Inactivity Timeout in the caller information. See “Ending the Session Because of Inactivity,” earlier in this chapter.

To specify the time length for an inactivity timeout:

- 1 Select Inactivity Timeout from the Host Security Preferences form (Figure 6-4).
- 2 Type in a number of minutes from 0 to 999, then press Enter. Zero (the default) indicates that there is no time limit.

Specifying Active Keyboards

You can decide what keyboards are active at the beginning of a session. You can disable the host keyboard to be sure that the remote user’s session is not interrupted in any way; you can disable the remote keyboard so that the remote user is only an observer of what is happening on the host; or you can make both keyboards active.

To specify which keyboards are active:

- 1 Choose Active Keyboards During Session from the Host Security Preferences form (Figure 6-4).
The Active Keyboards During Session menu appears.
- 2 Choose one of the following.
 - Host And Remote (the default). Both keyboards are active.
 - Host Only. The remote user can only observe what the host is doing.
 - Remote Only. The host user cannot interfere with the remote user's activity.

Blanking the Host Screen

You can blank the host screen automatically during all sessions to preserve the remote user's privacy. Since this cannot be overridden by the remote user, you probably don't want to set this preference unless the host PC is always unattended. See "Allowing the User to Blank the Host Screen," earlier in this chapter for an alternative.

To keep the host screen blank during sessions:

- 1 Choose Blank Host Screen from the Host Security Preferences form (Figure 6-4).
The Blank Host Screen menu appears with your choice highlighted.
- 2 Choose No (the default) or Yes.

Locking the Host Keyboard While Waiting

You can lock the host keyboard while the host PC is waiting for a connection. Then no one can change the mode of the host PC without the master password. This prevents others at the host site from using your PC while it waits for a remote user to call.

To lock the host PC while it is waiting for a connection:

- 1 Choose Lock Host While Waiting from the Host Security Preferences form (Figure 6-4).
The Lock Host While Waiting menu appears.
- 2 Choose No (the default) or Yes.

Prompting the Host User About Connections

You can prompt the host user about each connection attempt. When this option is enabled and a remote user is attempting a connection, the host user sees the prompt: “Press Enter to accept or Esc to reject.” No response from the host user can stop the connection or allow it after a short timeout period.

You can also specify the timeout for an unanswered prompt. This preference indicates the number of seconds the prompt is displayed for the host user.

To prompt the host user about each connection attempt:

- 1 Choose Prompt on Connection from the Host Security Preferences form (Figure 6-4).

The Prompt on Connection menu appears.

- 2 Choose one of the following.
 - No (the default). The connection is made without prompting the host user.
 - Yes - Connect On Timeout. If the host user does not respond to the prompt before the timeout expires, the connection is made anyway.
 - Yes - No Connect On Timeout. The connection is only made when the host user presses Enter in response to the prompt.

To specify the timeout for an unanswered prompt:

- 1 Select Prompt Timeout from the Host Security Preferences form (Figure 6-4).
- 2 Type in a number of seconds from 5 to 999 then press Enter.
The default is 5.

Allowing Encryption of Data

You can refuse, allow, or insist on data encryption for all data transmitted during a remote control session.

Setting this preference allows you to take advantage of third-party applications that use encryption algorithms that comply with Norton pcANYWHERE's API (applications programming interface) for data encryption.

To allow the use of data encryption:

- 1 Choose Use Data Encryption from the Host Security Preferences form (Figure 6-4).

The Use Data Encryption menu appears.

- 2 Choose one of the following.
 - No (the default). Data encryption is never used.
 - Yes - If Available. Data encryption is available if the remote PC is running Norton pcANYWHERE version 5.0.
 - Yes - Always. Data encryption must be used.

NOTE: When you choose Yes - Always, the remote user is asked for a password even when no connection can occur because the remote PC is using an older version of Norton pcANYWHERE. The check for encryption capability is done after the password verification.

Remote Control Sessions

7

This chapter explains how to start a Norton pcANYWHERE remote control session, a session in which one PC remotely controls another. Whether you are connecting over telephone lines to a PC in another city or over a LAN to a PC down the hall, the 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 the caller information used by the host PC. Be sure to complete the necessary installation and configuration procedures described in the preceding chapters before beginning. 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 covers:

- Initiating a remote control session from either the host or remote PC while the other waits
- Controlling the session from the Session Options menus for either the host or remote
- Transferring files during a session
- Automating a session using an automated procedure. Procedures are most commonly used for *unattended sessions*, sessions performed when neither user is present.

You can also initiate a session or unattended session with a script. For more detailed information see *Creating Norton pcANYWHERE Scripts*, which accompanies this user's guide. Only the remote PC can run automated procedures or scripts.

Starting the Host PC

To make your PC the host PC, you launch the host TSR. It can be activated using the menus provided by Norton pcANYWHERE or with a DOS command that bypasses one or more of the menus. You can type the

command at the DOS prompt or put it in the AUTOEXEC.BAT or another batch file. See “Using a DOS Command to Start the Host PC,” later in this chapter.

While you can initiate a remote control session from the host PC, it is much more common to start the PC in one of the following modes:

- **Waiting mode.** The host TSR is active, and the host PC can do nothing while it waits for a remote user to attempt a connection. This mode dedicates the host PC to pcANYWHERE. It is often used when the host PC is unattended. See “Waiting for a Remote PC to Connect,” next.
- **Incoming-call mode.** The host TSR is active, but you can still use the PC. Whenever a connection is made, your activities are interrupted momentarily but not halted. This mode allows the remote user to start a long job on the host PC and check on the job by periodically reconnecting. See “Waiting for a Remote PC to Connect,” next.
- **Hotkey mode.** The host TSR is loaded into memory but inactive. You can use the PC, but, to allow a connection, you must press the host hotkey and change modes. See “Using the Host Hotkey to Change Host Modes,” later in this chapter.

This mode is used when:

- Voice confirmation precedes the connection. See “Starting a Session with Voice Communication,” later in this chapter.
- The host user plans to accept calls on-and-off all day, but doesn’t want any unannounced interruptions.

It is never used when the host PC is unattended.

Waiting for a Remote PC to Connect

As the host user, you typically set up the host PC to wait for a connection from a remote PC, using either waiting or incoming-call mode. Using one of these modes is critical when you will not be at your PC during the remote control session.

Waiting mode dedicates the host PC to pcANYWHERE. It can be very useful when several remote users access the host PC and complete their jobs before exiting.

The benefit of using the incoming-call mode is that the remote user can start a long job on the host PC and check on it periodically instead of waiting for

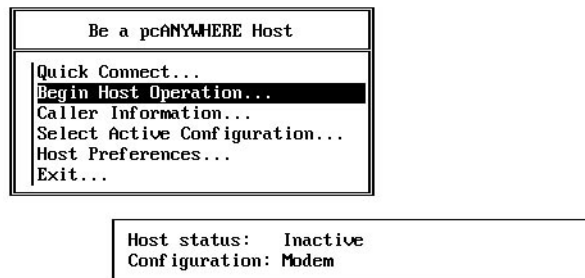
it to complete. The job continues, interrupted long enough to make a connection, but is not halted.

To put the host PC in waiting or incoming-call mode:

- 1 Choose Be A Host... from the pcANYWHERE Main menu.

The Be A pcANYWHERE Host menu appears (Figure 7-1). So does a status box that displays the current hardware configuration and the current status of the host TSR (active or inactive).

Figure 7-1 Starting the Host PC.



- 2 If the hardware configuration is *not* the one you want to use:
 - a Choose Select Active Configuration...
The Hardware Configurations menu appears. See Chapter 3, "Hardware Configurations," if you want to modify the configuration or create a new one.
 - b Choose the hardware configuration to be used by the host PC.
The hardware configuration form for your choice appears.
 - c Press Esc to return to the Be A pcANYWHERE Host menu.
- 3 Choose Begin Host Operation....
The Begin Host Operation menu appears (Figure 7-2).

Figure 7-2 Choose a Host Mode.

- 4 Choose one of the following options:
 - Wait For A Connection. The host TSR is active and your PC waits for the remote PC to make a connection.
The Connection Status form appears.
 - Exit, Allow Incoming Calls. The host TSR is active, but you can use the host PC for other applications.
The DOS prompt appears.

NOTE: If you haven't already provided a name for your PC, you are asked for one.

If you are not going to be at your PC, you may want to:

- Stop anyone from using the host keyboard by making the remote keyboard the only active keyboard.
- Blank the host screen for privacy.
- Allow a remote user to change the host mode. This lets users switch back and forth between waiting and incoming-call modes. For network connections, users can suspend their connection to your host PC. This makes it easier to switch from host to host. The host TSR remains active and ready to accept another connection. However, the suspended users are not asked for a password when they reconnect.

See Chapter 6, "Caller Information and Host Preferences," for more information.

Initiating the Session from the Host PC

If the host PC is using a serial hardware configuration, you (as the host user) can initiate the remote control session from the host PC. You can also initiate a session by switching from a telephone connection with the remote user to

modem connection. See “Starting a Session with Voice Communication,” next.

Upon connection, the remote user is prompted for a password if the host PC requires one and no password is specified in the remote PC’s session configuration. The remote PC displays Terminal mode, then the host screen appears and the remote control session begins.

To initiate a session with a remote PC:

- 1 Confirm with the remote user that the remote PC is waiting for a connection.
- 2 Choose Be A Host... from the pcANYWHERE Main menu.

The Be A pcANYWHERE Host menu appears (Figure 7-1). So does a status box that displays the current hardware configuration and the current status of the host TSR (active or inactive).

- 3 If the hardware configuration is *not* the one you want to use:
 - a Choose Select Active Configuration...
The Hardware Configurations menu appears. See Chapter 3, “Hardware Configurations,” if you want to modify the configuration or create a new one.
 - b Choose the hardware configuration to be used by the host PC.
The hardware configuration form for your choice appears.
 - c Press Esc to return to the Be A pcANYWHERE Host menu.
- 4 Choose Begin Host Operation...
The Begin Host Operation menu appears (Figure 7-2).
- 5 Choose Call A Remote.

NOTE: If you haven’t already provided a name for your PC, you are asked for one.

The Phone Number To Dial form appears.

- 6 A default telephone number appears in the form if one is specified as a host general preference. See “Setting a Default Telephone Number” in Chapter 6, “Caller Information and Host Preferences.” Type a telephone number or accept the default. Then press Enter.
Norton pcANYWHERE displays the current status of the connection while waiting for the remote PC to respond.

NOTE: If you are in hotkey mode, you can initiate a remote control session by pressing the host hotkey and choosing Call Remote User from the pcANYWHERE Host menu.

Starting a Session with Voice Communication

A remote control session can start with voice communication and switch to data communication if:

- Both users are using a modem hardware connection.
- Each user has a telephone and modem that share a telephone line.

Either user can make the telephone call, and both users' PCs must be ready to make the switch.

The remote user can initiate a switch back from data communication to voice communication during the session. See "Switching from Data Communication to Voice," later in this chapter.

To set up the host PC for the switch:

- 1 Choose Be A Host... from the pcANYWHERE Main menu.
The Be A pcANYWHERE Host menu appears (Figure 7-1). So does a status box that displays the current hardware configuration and the current status of the host TSR (active or inactive).
- 2 If the hardware configuration is *not* the one you want to use:
 - a Choose Select Active Configuration....
The Hardware Configurations menu appears. See Chapter 3, "Hardware Configurations," if you want to modify the configuration or create a new one.
 - b Choose the hardware configuration to be used by the host PC.
The hardware configuration form for your choice appears.
 - c Press Esc to return to the Be A pcANYWHERE Host menu.
- 3 Choose Begin Host Operation....
The Begin Host Operation menu appears (Figure 7-2).
- 4 Choose Exit, Hotkey To Activate so that the host TSR is loaded into memory.

NOTE: If you haven't already provided a name for your PC, you are asked for one.

- 5 Press the host hotkey.
The pcANYWHERE Host menu appears.
- 6 Choose Voice-First Connection from the pcANYWHERE Host menu.
Norton pcANYWHERE prompts you through this process.
- 7 Hang up the telephone receiver when a message to do so appears on your PC. Then press Enter.
Norton pcANYWHERE displays the current status of the connection while waiting for the session to begin.

To set up the remote PC for the switch:

- 1 Choose Call A pcANYWHERE Host... from the pcANYWHERE Main menu.
The Call A pcANYWHERE Host menu appears.
- 2 Choose Connect To A Host....
The Select Host For Connection menu appears.

NOTE: If you haven't already provided a name for your PC, you are prompted for one.

- 3 Choose the session configuration for the host PC with which you want to connect.
The Connect Options menu appears.
- 4 Choose Voice-First Connection.
Norton pcANYWHERE prompts you through this process.
- 5 Hang up the telephone receiver when a message to do so appears on your PC. Then press Enter.
Norton pcANYWHERE displays the current status of the connection while waiting for the session to begin.

Upon connection, the remote user is prompted for a password if the host PC requires one and no password is specified in the remote PC's session configuration. The remote PC displays Terminal mode; then the host screen appears, and the remote control session begins.

Using the Host Hotkey to Change Host Modes

If you want to work between calls without interruption, you load the host TSR and choose hotkey mode. Remote users then must notify you when they want to make a connection.

To put the host PC in hotkey mode:

- 1 Choose Be A Host... from the pcANYWHERE Main menu.
The Be A pcANYWHERE Host menu appears (Figure 7-1). So does a status box that displays the current hardware configuration and the current status of the host TSR (active or inactive).
- 2 If the hardware configuration is *not* the one you want to use:
 - a Choose Select Active Configuration...
The Hardware Configurations menu appears. See Chapter 3, "Hardware Configurations," if you want to modify the configuration or create a new one.
 - b Choose the hardware configuration to be used by the host PC.
The hardware configuration form for your choice appears.
 - c Press Esc to return to the Be A pcANYWHERE Host menu.
- 3 Choose Begin Host Operation...
The Begin Host Operation menu appears (Figure 7-2).
- 4 Choose Exit, Hotkey To Activate.
The DOS prompt appears, and you can use the host PC.

NOTE: If you haven't already provided a name for your PC, you are asked for one.

To make the TSR active and change modes for a connection:

- 1 Press the host hotkey (initially Alt+RightShift).
The pcANYWHERE Host menu appears.
- 2 Choose one of the following:
 - Wait For A Call. The TSR is active and the host PC is in waiting mode.
 - Exit, Allow Incoming Calls. The TSR is active and the host PC is in incoming-call mode.

- Call Remote User. Your PC initiates the connection to a remote PC. The remote PC must be waiting for a connection. (If you are using a network hardware configuration, this option does not appear on the menu.)
- Voice-First Connection. This option allows you switch from a voice communication over the telephone to a data communication between two PCs.

For more information about these modes of host operations, see “Starting the Host PC,” earlier in this chapter.

NOTE: Exit And Remove From Memory appears on the Be A pcANYWHERE Host menu and Cancel And Remove From Memory appears on the Begin Host Operation menu if you have already loaded the TSR into memory and you retype `AW` at the DOS prompt.

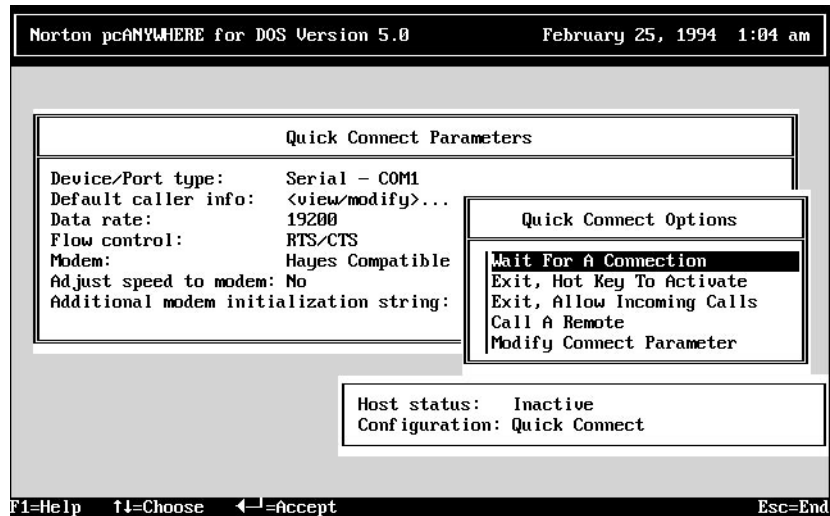
Using Quick Connect on the Host PC

You can connect to a remote PC without setting up a hardware configuration. You provide the minimal information necessary and pcANYWHERE makes the connection. It is more convenient in the long run to create the configurations if you use more than one communications device. For example, you may have a modem attached to your PC and also be on a network.

To make a quick connection:

- 1 Choose Be A Host PC... from the pcANYWHERE Main menu.
The Be A pcANYWHERE Host PC menu appears (Figure 7-1).
- 2 Choose Quick Connect...
The Quick Connect Parameters form appears (Figure 7-3) along with the Quick Connect Options menu.

Figure 7-3 Quick Connect is a fast way to make a connection.



- 3 Choose Modify Connect Parameters from the Quick Connect Options menu.

The Quick Connect Parameters form becomes active.

- 4 All the parameters are hardware configuration options. See Chapter 3, "Hardware Configurations," for more information. For example, if you will connect to the remote PC using a modem attached to your PC, see "Creating a Modem Hardware Configuration" in Chapter 3. If you are using a gateway on your network, see "Creating a Node Hardware Configuration" also in Chapter 3.
- 5 Press Esc.
- 6 Choose a host mode from the Quick Connect Options menu.

Norton pcANYWHERE displays the current status of the connection while you wait for the online service to respond or to initiate a connection.

Using a DOS Command to Start the Host PC

You can bypass a number of the steps in the above procedures by starting the host PC from the DOS prompt. See Table 7-1.

Table 7-1 Starting the Host PC from the DOS Prompt

Action	Command
Display the Be A pcANYWHERE Host menu	AW /O:H
Start the host PC in waiting mode	AW /O:H /M:W
Start the host PC in incoming-call mode	AW /O:H /M:A
Initiate a session from the host	AW /O:H /M:D /N:phone_number
Change the current hardware configuration, then initiate a session from the host	AW [/O:H [/C:hdwe_config] [/N:phone_number]



Network

NETWORK USERS: If Norton pcANYWHERE has been installed to 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: `AW /I:userid /O:H`.

For other DOS commands and command-line options that affect remote control sessions, see “Using a DOS Command to Start the Remote PC,” “Ending the Session,” and “Transferring Files from the DOS Command Line,” later in this chapter.

Canceling the Host TSR

If you are in hotkey mode or when a session ends, you can cancel the host TSR.

To remove the host TSR from memory:

- Choose Cancel pcANYWHERE from the pcANYWHERE Host menu. This menu appears when your computer is in hotkey mode and you press the host hotkey, or after a session in which the remote user cannot reset the host mode.

Starting the Remote PC

You can begin remote operation:

- Using the menus.
You can initiate a connection (see “Initiating the Session from the Remote PC,” next) or leave the remote PC in waiting mode. When in waiting mode, the remote PC can do nothing except wait for a host user to attempt a connection. See “Waiting for a Host PC to Connect,” later in this chapter. When initiating a connection, you can start with voice communication (over the telephone) and switch to data communication (when the modems and the telephones share the same telephone line). See “Starting a Session with Voice Communication,” earlier in this chapter.
- Using a DOS command that bypasses one or more of the menus. You can type the command at the DOS prompt or put it in the AUTOEXEC.BAT or another batch file. See “Using a DOS Command to Start the Remote PC,” later in this chapter.
- Using automated procedures or scripts. These are commonly used for unattended sessions in which neither user is present. In fact, you can conduct a series of remote control sessions using a single procedure or script. See “Using Automated Procedures,” later in this chapter, and *Creating Norton pcANYWHERE Scripts*.

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 “Starting a Session with Voice Communication,” earlier in this chapter.

Upon connection, you are prompted for a password if the host PC requires one and no password is specified in the session configuration. The remote

PC displays Terminal mode, then the host screen appears and the remote control session begins.

To initiate a session with a host PC:

- 1 Confirm with the host user that the host PC is waiting for a connection.
- 2 Choose Call A pcANYWHERE Host... from the pcANYWHERE Main menu.

The Call A pcANYWHERE Host menu appears.

- 3 Choose Connect To A Host....

The Select Host For Connection menu appears.

NOTE: If you haven't already provided a name for your PC, you are prompted for one.

- 4 Choose the session configuration for the host PC that you want to connect to.

The Connect Options menu appears.

- 5 Choose Call.

- 6 Depending on what information is missing from the hardware and session configurations, you may have to type a telephone number, choose a gateway, or choose a host PC. See "Choosing a Host PC or Gateway on a LAN" next for additional information.

Norton pcANYWHERE displays the current status of the connection while waiting for the host PC to respond.

TIP: You can select the session configuration in step 4, then press F2 to call.

Choosing a Host PC or Gateway on a LAN

Norton pcANYWHERE displays a list of the available network connections for you to choose from when:

- You are on a LAN and your node hardware configuration requires a gateway but does not provide its name.
- Your session configuration does not provide the name of the host PC on the LAN.

Norton pcANYWHERE lists the computer name for each PC or gateway on the network along with the current operating mode (Host, Remote, or Gateway) and the status of the PC (Figure 7-4).

Figure 7-4 Choose a host PC or a gateway available on the network.

Known Network Connections		
▲ CRATNER	[Host]	Available
DAVE BRAUERMAN'S PC	[Host]	Available
DOS HP	[Host]	Available
ENG	[Host]	Available
G-EUR	[Host]	Available
G-1	[Host]	Available
G-2	[Host]	Available
G-3	[Host]	Available
GATE3	[Host]	Available
▼ GER	[Host]	Available

The status is one of the following:

- Available. You may connect to this PC.
- Suspended. This PC is available, but was suspended by another remote user who intends to return. If you are that remote user, you will not be asked for a password as you return.
- In Use. This PC is not available.
- Unknown. Norton pcANYWHERE does not know the status of this connection.

Waiting for a Host PC to Connect

Occasionally, the host user initiates the session from the host PC. To do so successfully, the remote PC must be in waiting mode. See “Initiating the Session from the Host PC,” earlier in this chapter.

To wait for a host PC:

- 1 Choose Call A pcANYWHERE Host... from the pcANYWHERE Main menu.

The Call A pcANYWHERE Host menu appears.

- 2 Choose Connect To A Host....

The Select Host For Connection menu appears.

NOTE: If you haven't already provided a name for your PC, you are prompted for one.

- 3 Choose the session configuration for the host PC that you want to connect to.

The Connect Options menu appears.

- 4 Choose Wait For A Call.

The message "Waiting for a connection... Press Esc to cancel." appears on the screen.

Using Quick Connect on the Remote PC

You can connect to a host PC without setting up either a hardware or session configuration. You provide the minimal information necessary and pcANYWHERE makes the connection. It is more convenient in the long run to create the configurations if:

- This is not the only host PC you call.
- You will be calling this particular host PC again.

To make a quick connection:

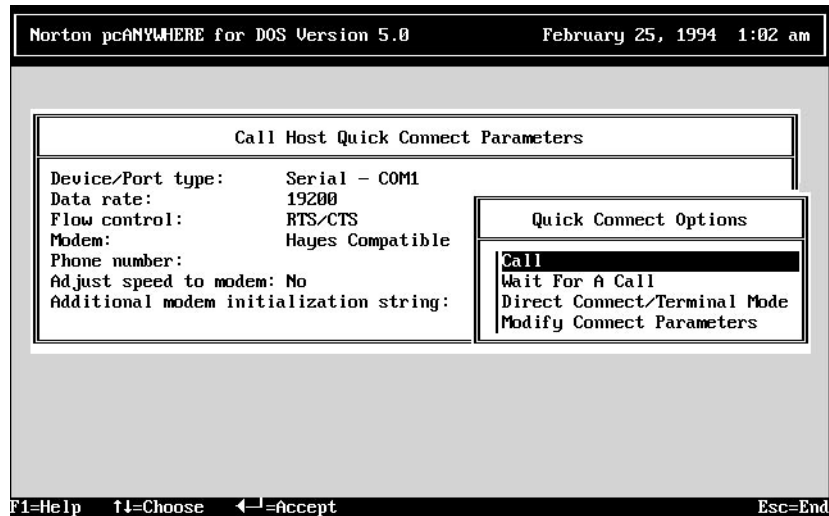
- 1 Choose Call A pcANYWHERE Host... from the pcANYWHERE Main menu.

The Call A pcANYWHERE Host menu appears.

- 2 Choose Quick Connect...

The Call Host Quick Connect Parameters form appears (Figure 7-5) along with the Quick Connect Options menu.

Figure 7-5 Quick Connect is a fast way to make a connection.



- 3 Choose Modify Connect Parameters from the Quick Connect Options menu.

The Call Host Quick Connect Parameters form becomes active.

- 4 All the parameters (except for Phone Number) are hardware configuration options. See Chapter 3, "Hardware Configurations," for more information. For example, if you will connect to the host PC using a modem attached to your PC, see "Creating a Modem Hardware Configuration" in Chapter 3. If you are using a gateway on your network, see "Creating a Node Hardware Configuration" also in Chapter 3.
- 5 Select Phone Number if you are going to initiate the connection. Type the phone number for the online service, including any prefix or suffix, then press Enter.
- 6 Press Esc.
- 7 Choose Call or Wait For A Call from the Quick Connect Options menu.

Norton pcANYWHERE displays the current status of the connection while you wait for the host PC to respond or to initiate a connection.

NOTE: You can choose Direct Connect/Terminal Mode and talk directly to your modem via a terminal window. See your modem's manual for details about the commands.

Using a DOS Command to Start the Remote PC

You can bypass a number of the steps in the above procedures by starting the remote PC from the DOS prompt. See Table 7-2.

Table 7-2 Starting the Remote PC from the DOS Prompt

Action	Command
Display the Call A pcANYWHERE Host menu	AW /O:R
Initiate a session from the remote	AW /O:R /M:D /N: <i>session_configuration_name</i>
Initiate a session with a script	AW /O:R /M:S /N: <i>script_name</i>
Initiate a session with an automated procedure	AW /O:R /M:P /N: <i>procedure_name</i>
Action	Command

If the name of the directory you specified for Norton pcANYWHERE during the installation (or the network path specified by your network administrator) is not in your PATH, precede AW with the correct pathname.



Network

NETWORK USERS: If Norton pcANYWHERE has been installed to 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: `AW /I:userid /O:R`.

For other DOS commands and command-line options that affect remote control sessions, see “Using a DOS Command to Start the Host PC,” earlier in this chapter, and “Transferring Files from the DOS Command Line” and “Ending the Session,” later in this chapter.

Managing the Remote Control Session

Normally, once the connection to the host PC is made, both the host and remote users can execute commands and run applications on the host PC. Both users also have access to a menu with session options—although not all the options are the same. They can both start a typed conversation using a dialogue window, change the destination for printed output, and end the session. These shared options are explained first.

To access the session menu:

- 1 Press the host or remote hotkey.

Depending on whether you are the host or remote user, the Host Session Options menu or the remote's Session Options menu appears (Figures 7-6 and 7-7).

Figure 7-6 The Host Session Options menu allows the host user to manage the session.

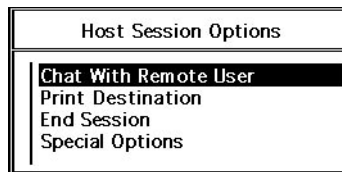
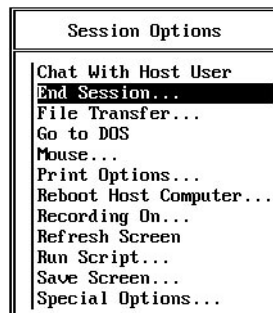


Figure 7-7 The Session Options menu allows the remote user to manage the session.



- 2 To choose an option, see the corresponding procedure in one of the next few sections.
- 3 Press Esc to return to the session.

Both menus cannot be active at the same time. The host hotkey does nothing while the remote user is busy. When the reverse is true, the remote user sees a message box explaining that the host user is busy. If the remote user presses the remote hotkey at that time, the only option available is End Session.

The changes you make from the Session Options menus are in effect for only the current session. The remote and host preferences you have set will be back in effect for your next session. The defaults you see for options on the Session Options menu are the settings from the remote and host preferences.

Chatting with the Other User

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

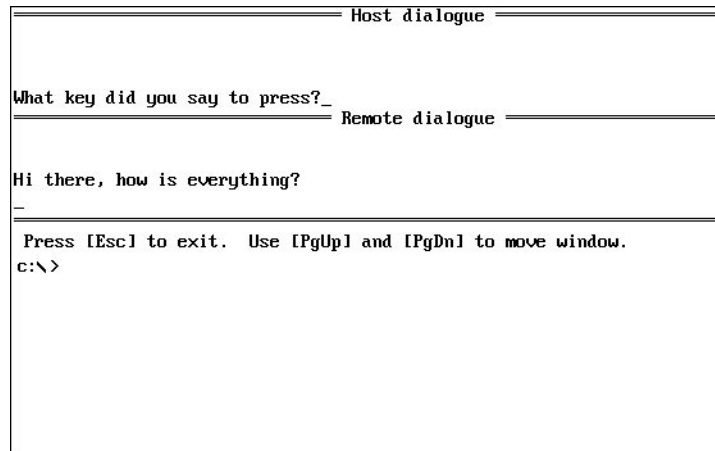
The host user's keystrokes automatically appear in the upper half of window, while the remote user's appear in the lower half. Both users can type simultaneously into their own half of the dialogue window. Either user can press PgDn or PgUp to move the windows to the bottom or top half of both screens.

To use the chat window:

- 1 Choose Chat With Host User or Chat With Remote User from either Session Options menu.

The dialogue window appears on both PCs (Figure 7-8).

Figure 7-8 Identical dialogue windows are displayed on the host and remote PCs.



- 2 Type your conversation.
- 3 Press Esc when the conversation is over.

Changing the Destination for Printed Output

Either the remote or host user can change the destination of any printed output during a session. The output can be printed on the active printer or saved in the active print file for the host, remote, or both PCs. It can also be discarded.

The destination of printed output can also be set as a remote preference. See “Remote Control Session Preferences” in Chapter 5, “Session Configurations and Remote Preferences.”

To change the destination for printed output:

- 1 Choose Print Options from the remote Session Options menu (Figure 7-7) or Print Destination from the host menu (Figure 7-6).
The Print Options menu appears on the remote PC or the Print Destination menu appears on the host PC. The menus have options with similar names.
- 2 Choose the appropriate option.

Ending the Session

Either the host or remote user can end the session.

To end the session:

- 1 Choose End Session from either Session Options menu.
If the remote user is ending the session and is allowed to change the host's mode, the Host Disconnect Options menu appears. If the host user is ending the session, the End Session menu appears. The menus have options with similar names.
- 2 Choose one of the following. The first option is on the menu the remote user sees; the second is on the menu the host user sees.
 - Host Waits For Another Call or Wait For Another Call.
 - The host PC goes into waiting mode.
 - Hotkey To Reactivate Host or Hotkey Reactivates.
 - The host PC goes into hotkey mode.
 - Host Accepts Calls At Any Time or Incoming Call Activates.
 - The host PC goes into incoming-call mode.
 - Cancel Host Operation or Cancel pcANYWHERE. This option removes the host TSR from memory and ends Norton pcANYWHERE on the host PC.

If you are a remote user on a network connected to a host PC on the same network, you choose from:
 - Disconnect.
 - Suspend And Connect To Another Host.

You can also end the session using the AWLOGOFF command (see Table 7-3). If you are the remote user, you must have permission from the host user to change the host mode or your use of the command-line options (/W, /H, /A, and /C) will be ignored.

Table 7-3 Ending the Session from the DOS Prompt

Action	Command
End the session leaving the host PC in waiting mode	AWLOGOFF /W

Table 7-3 Ending the Session from the DOS Prompt *(continued)*

Action	Command
End the session leaving the host PC in hotkey mode	AWLOGOFF /H
End the session leaving the host PC in on-call mode	AWLOGOFF /A
End the session and cancel pcANYWHERE on the host PC	AWLOGOFF /C

If the caller information used to start the session has a command for the Command To Execute option, `AWLOGOFF /W` must be used to end the session.

Special Options for the Host User

As the host user, you have two special options. You can enable or disable:

- The remote keyboard
- The transmission of video data about the host screen to the remote PC

NOTE: Neither of these options affects chat mode. You can still communicate with the remote user using the dialogue window.

To view or change the host's special options:

- 1 Choose Special Options... from the Host Session Options menu (Figure 7-6).
The Special Options form appears (Figure 7-9).
- 2 To choose an option, see the corresponding procedure in one of the next few sections.

Figure 7-9 The host PC has two special options during a session.

Special Options	
Remote screen	Enabled
Remote keyboard	Enabled

Controlling the Remote Keyboard from the Host

If the remote keyboard is disabled, the remote user can only observe the host screen.

To enable or disable the remote user's keyboard:

- Choose Remote Keyboard... from the Special Options form (Figure 7-9).

The setting for this option toggles from Enabled to Disabled, or vice versa.

Sending the Image of the Host Screen from the Host

If the remote PC is unattended and an automated procedure is running, you may want to stop transmitting video data from the host to the remote. Then no one can observe what is happening on the host. You can also stop transmitting video data as a way to disable an unauthorized user without ending the session. When you disable the remote screen, you simultaneously disable the remote keyboard.

To start or stop sending video data to the remote screen:

- Choose Remote Screen... from the Special Options form (Figure 7-9).

The setting for this option toggles from Enabled to Disabled or vice versa. When this option becomes disabled, the setting for Remote Keyboard is automatically Disabled. However, when this option becomes enabled, the setting for Remote Keyboard is not affected.

Session Options Available Only to the Remote PC

The next few sections describe options on the remote user's Session Options 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 permission.

Adjusting the Image of the Host Screen Displayed on the Remote

Most of the special options for the remote user affect how the host screen is displayed on the remote PC.

To view or change the remote's special options:

- 1 Choose Special Options... from the remote's Session Options menu (Figure 7-7).

The Special Options form appears (Figure 7-10).

- 2 To choose an option, see the corresponding procedure in one of the next few sections.

Figure 7-10 Most of the special options affect how the host screen is displayed on the remote PC.

Special Options	
Attribute translation:	Yes
Blink attribute:	Yes
Drive mapping:	Disabled
Full graphics:	Yes
Graphics translation favor:	Color
Hercules graphics page:	0
Host keyboard locked:	No
Host screen status:	Display
Scan frequency:	10
Special keyboard handler:	Disabled
Synchronized display:	No

All of the options, except for Hercules Graphics Page, Host Screen Status, and Scan Frequency, can be set as remote preferences. See Chapter 5, "Session Configurations and Remote Preferences."

Translating Video Attributes

Use the Attribute Translation preference when one PC has a monochrome display and the other has a color display.

To translate attributes:

- 1 Choose Attribute Translation from the Special Options form (Figure 7-10).

The Attribute Translation menu appears.

- 2 Choose No or Yes.

Control Blinking

The Blink Attribute option allows Norton pcANYWHERE to display blinking characters. Set this option to No only if you experience unexpected blinking during a session.

To display blinking characters:

- 1 Choose Blink Attribute from the Special Options form (Figure 7-10).

The Blink Attribute menu appears.

- 2 Choose No or Yes.

Using Full Graphics

Use the Full Graphics option when you want the most accurate representation of DOS graphics as possible. Disable the option to improve speed, when an approximation of graphics is acceptable.

To use full graphics:

- 1 Choose Full Graphics from the Special Options form (Figure 7-10).

The Full Graphics menu appears.

- 2 Choose No or Yes.

Choosing Between Color or Resolution

If the host and remote PCs have different color monitors, their resolutions and the number of colors they can display may be different. You can favor color or favor resolution while translating graphics.

To favor color or resolution when translating graphics:

- 1 Choose Graphics Translation Favor from the Special Options form (Figure 7-10).

The Graphics Translation Favors menu appears.

- 2 Choose Color or Resolution—whichever is most important to you.

Changing Hercules Pages

If you have a Hercules graphics adapter and the screen display is not correct, you can switch from one Hercules graphics page to another to see what looks best.

To change the Hercules graphics page:

- 1 Select Hercules Graphics Page from the Special Options form (Figure 7-10).
- 2 Type the digit for the graphics page you want to use, then press Enter. (The default is 0 which is the first page.)

Blanking the Host Screen

You can blank the host screen during the session to preserve your privacy. This option is often used when the host PC is unattended. The caller information on the host PC may not allow you to blank the host screen. The host screen may also be automatically blanked as a host security preference. See Chapter 6, “Caller Information and Host Preferences,” for more details.

To blank the host screen:

- 1 Choose Host Screen Status from the Special Options form (Figure 7-10).
The Host Screen Status menu appears.
- 2 Choose Blank or Display.

Deciding How Often to Update the Remote Display

Norton pcANYWHERE updates periodically the image of the host screen displayed on the remote PC. You can set the interval between scans (or updates) using the Scan Frequency option. Each unit represents 55 milliseconds. The default setting 10 is approximately half a second. Do not use this option unless screen display operation is not smooth. For example, increase the time between scans when screen updates contain pauses.

To set the interval between scans or updates of the image of the host screen on the remote PC:

- 1 Select Scan Frequency from the Special Options form (Figure 7-10).
- 2 Type a number from 0 to 999, then press Enter.

Synchronizing the Displays

The Synchronized Screen Display option slows the host application to the rate at which the remote can display screen activity. If this option is disabled, some lines of text may scroll off the screen before the remote can display them. If the speed of the application is more important than a complete display of all the characters, such as with a lengthy database indexing procedure, disable this option.

To synchronize the screen displays:

- 1 Choose Synchronized Display from the Special Options form (Figure 7-10).

The Synchronized Display menu appears.

- 2 Choose No or Yes.

Adjusting the Host Keyboard and the Keyboard Handlers

Two special options for the remote user affect the keystrokes that are sent to the host PC. You can:

- Disable the host keyboard to prevent interruptions. If the host keyboard is disabled, the host user can only observe the remote control session.
- Disable or change the level of the special keyboard handler used on the host PC by the remote user. The host user may not allow you to use a handler. See *keyboard hander* in the Glossary for more information.

To disable the host keyboard:

- 1 Choose Host Keyboard Locked from the Special Options form (Figure 7-10).

The Host Keyboard Locked menu appears.

- 2 Choose No or Yes.

To disable or change the level of the keyboard handler:

- 1 Choose Special Keyboard Handler from the Special Options form (Figure 7-10).

The Special Keyboard Handler menu appears.

- 2 Choose one of the following:

- Disabled.

- Level 1.
- Level 2.
- Level 3.

Changing Mouse Options

The mouse options affect the movement of the remote mouse cursor on the host screen. You must have permission from the host user to use the mouse on the host screen, but, if you have permission, you can enable or disable the mouse cursor and change both the acceleration rate and the double speed rate.

To specify mouse options:

- 1 Choose Mouse from the remote's Session Options menu (Figure 7-7). The Mouse Preferences form appears (Figure 7-11).

Figure 7-11 Use the Mouse Preferences form to control the use of the mouse.

Mouse Preferences	
Acceleration factor:	50 (1-100)
Double speed rate:	50 (1-100)
Remote mouse mode:	Enabled - track always

- 2 To change a mouse option, see the corresponding procedure in one of the next few sections.
- 3 Press Esc to exit the Mouse Preferences form.

Changing the Acceleration Factor

You can change the acceleration factor, which controls the movement of the mouse cursor in relationship to the movement of the mouse. The range is from 1 to 100 (1 is slowest and 100 is fastest).

To change the acceleration factor:

- 1 Select Acceleration Factor from the Mouse Preferences form (Figure 7-11).
- 2 Type in a number from 1 to 100.

Changing the Double Speed Rate

You can change the double speed rate, which determines how fast the mouse must move before the mouse cursor switches to *double speed* and moves across the screen faster. The range is from 1 to 100 (1 disables the use of double speed and 100 interprets any movement as double speed).

To change the double speed rate:

- 1 Select Double Speed Rate from the Mouse Preferences form (Figure 7-11).
- 2 Type in a number from 1 to 100.

Enabling or Disabling the Mouse Cursor

You can enable or disable the mouse cursor only for DOS applications because Windows handles the mouse differently than DOS.

To change the mouse cursor's movement (for DOS applications):

- 1 Choose Remote Mouse Mode from the Mouse Preferences form (Figure 7-11).
The Remote Mouse Option menu appears.
- 2 Choose one of the following:
 - Disabled. Moving the remote's mouse will have no effect on the host PC.
 - Enabled - Track Always. Two mouse cursors appears on the remote screen. When you move the remote mouse, you will see the host's mouse cursor catching up and eventually resting in the same location as the remote mouse cursor. This mode of operation is suitable for fast modem or network connections.
 - Enabled - Track Always, One Mouse. Only the host mouse cursor appears on the remote screen. This option can be difficult to use with slow connections because the mouse cursor moves much more slowly than the mouse. Its advantage is that you see only one mouse cursor.
 - Enabled - Track When Button Pressed. Two mouse cursors appear on the remote screen, but the host mouse cursor is updated only when a button is pressed on the remote mouse. This option works well with applications that react to the mouse's position only when a button is pressed. It is also suitable for

situations in which it is desirable to send the least amount of data, such as when you are using a modem that has a slow data rate.

You can experiment with each option to determine which is best for controlling the applications you are running on the host PC.

Accessing the Remote PC During a Session

As the remote user in a remote control session, you control the host PC. Your keystrokes and mouse movements take effect on the host PC—not your own PC. However, there are two ways to regain access to your files, applications, and so forth during the session:

- You can temporarily interrupt the session and return to your own DOS prompt. For example, you can check for electronic mail or look up something in a database and then return to the session. The host screen displays the message, “Remote user is busy. Please wait...”
- The remote PC’s drives can be mapped as additional drives on the host PC making them available during the session. For example, you can access your C drive as the host’s T drive.

To go from the session to the remote PC’s DOS prompt:

- Choose Go To DOS from the remote’s Session Options menu (Figure 7-7).

The DOS prompt appears.

To map remote drives to the host PC:

- 1 Choose Special Options... from the Session Options menu (Figure 7-7).

The Special Options form appears (Figure 7-10).

- 2 Choose Drive Mapping.

The Remote Drive Mapping menu appears.

- 3 Choose Enabled.

The Drive Mapping For Host Applications menu appears.

- 4 Choose the letter for a host drive. This is the letter that the remote drive will have on the host PC. Usually, you choose a letter currently unused by the host PC.

The Remote Drive menu appears showing all the drives available on the remote PC.

- 5 Choose the letter of the remote drive that will be accessed from the host PC.

NOTE: If you want your C drive to be the host's T drive, for example, you would choose T: in step 4 and C: in step 5.

- 6 Repeat steps 4 and 5 for each remote drive you want to map.

To disable drive mapping:

- 1 Choose Drive Mapping from the Special Options form (Figure 7-10). The Remote Drive Mapping menu appears.
- 2 Choose Disabled.

Refreshing the Screen

Sometimes the remote user will want to refresh the image of the host screen displayed on the remote PC. For example, some incorrect characters or "garbage" may appear on the screen.

To refresh the image of the host screen:

- Choose Refresh Screen from the remote's Session Options menu (Figure 7-7).
The host screen is repainted on the remote PC.

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 from data communication to voice:

- Choose Switch To Voice from the remote's Session Options menu. Follow the directions on the screen. Norton pcANYWHERE will assist you through the process of switching from voice communication to data communication and back.

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 PC only if allowed to by the caller information on the host PC. See “Allowing the User to Reboot the Host” in Chapter 6, “Caller Information and Host Preferences,” for details.

If the reboot does not restart pcANYWHERE automatically, the remote user cannot access the host PC. To load the host TSR automatically whenever the host PC reboots, put a DOS command that starts the host PC in the host's AUTOEXEC.BAT file. See “Using a DOS Command to Start the Host PC,” earlier in this chapter.

To reboot the host from the remote PC:

- 1 Choose Reboot Host Computer... from the remote's Session Options menu (Figure 7-7).

The Reboot Host Options menu appears.

- 2 Choose one of the following:
 - Cancel Reboot Request. This option returns you to the remote control session.
 - Cold Boot. This option cold boots the host PC. This is equivalent to turning the PC off and then back on.
 - Warm Boot. This option warm boots the host PC. This is equivalent to pressing Ctrl+Alt+Del or the reset button.

Transferring and Managing Files and Directories

You can transfer and manage files and directories on either the host PC or the remote PC by using the AWSEND program, which was installed in the directory with your pcANYWHERE program files.

You start the AWSEND program from the host's DOS prompt after the connection is made. You can select files from the file transfer window or transfer files from the DOS command line. The following sections describe both methods.

Using the File Transfer Program

This section explains how to transfer files between the host and remote PCs, and manage files and directories on either computer. You can initiate a file transfer from either PC.

Transferring files using AWSEND involves starting the program, selecting files, then beginning the transfer.

To transfer files using AWSEND:

- 1 Start the AWSEND program by typing the following at the DOS prompt:

```
[path]AWSEND
```

where *path* is the pathname to the directory where pcANYWHERE files reside. As the brackets [] indicate, the *path* is optional. When it is not specified, the current directory and directories in the computer's PATH statement are searched for AWSEND.

The file transfer window appears (Figure 7-12). The host's files appear on the right side of the window (labeled "HOST FILES") and the remote's files appear on the left side (labeled "YOUR FILES").

Figure 7-12 Use the file transfer window to transfer files.

YOUR FILES				HOST FILES			
D:\NU7				D:\NDW			
<DIR>				<DIR>			
..				..			
ADVISE.HLP	81131	11-03-93	7:00	AAPLAY.DLL	137232	11-15-93	3:00
ALIASES	9557	11-03-93	7:00	BATCHRUN.EXE	103504	11-15-93	3:00
APPNOTES.DOC	48485	11-03-93	7:00	CFGNDW.EXE	239760	11-15-93	3:00
BE.EXE	19001	11-03-93	7:00	CFGNDW.HLP	144832	11-15-93	3:00
CALIBBRAT.EXE	51343	11-03-93	7:00	DESKEDIT.EXE	230176	11-15-93	3:00
CALIBBRAT.HLP	14888	11-03-93	7:00	DESKEDIT.HLP	146574	11-15-93	3:00
CONFIG1.NPC	143	11-03-93	7:00	DLGEDIT.EXE	124672	11-15-93	3:00
CONFIG2.NPC	143	11-03-93	7:00	DLGEDIT.HLP	105209	11-15-93	3:00
CONFIG3.NPC	143	11-03-93	7:00	FASSIST.DOC	21515	11-15-93	3:00
DESCRIPT.ION	3158	11-03-93	7:00	FASSIST1.DLL	93600	11-15-93	3:00
DISKEDIT.EXE	132075	11-03-93	7:00	FINCALC.EXE	103856	11-15-93	3:00
DISKEDIT.HLP	85628	11-03-93	7:00	FINCALC.HLP	103669	11-15-93	3:00
▼ DISKMON.EXE	17000	11-03-93	7:00	▼ ICONEDIT.EXE	132848	11-15-93	3:00
201,752,576 bytes free				92,479,488 bytes free			
F1=Help F4+=Choose <space>=Mark/Unmark ←=Accept directory F2=Send Esc=Menu							

- 2 To send files from the host to the remote PC, tag files from the HOST FILES side of the window. To send files from the remote to the host PC, tag files from the YOUR FILES side of the window.
 - To switch between your files and the host's files, use RightArrow and LeftArrow.
 - To tag a file or directory of files, highlight it and press the Spacebar. See "Tagging and Untagging Files" next for details about other ways to tag files.
- 3 After selecting the files, switch sides and display the current contents of the destination directory.
- 4 Do one of the following:
 - Press F2 to send the files.
 - Press Esc to see a file transfer options menu. Then choose Begin Transfer....

NOTE: The two file transfer options menus, Options For Your Files menu (Figure 7-13) and Options For Host Files (Figure 7-14), can display the same options. However, depending on whether or not files and directories are tagged, not all the options are displayed. Figure 7-13 shows the menu as it appears when nothing has been tagged. Figure 7-14 shows the menu as it appears when one file and one directory have been tagged.

The status of the file transfer appears in the window once the transfer begins. An arrow at the top of the window indicates the direction of transfer.

Figure 7-13 The Options For Your Files menu.

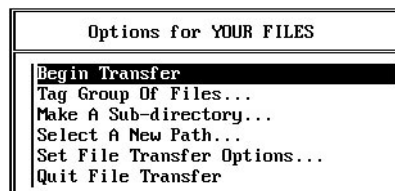
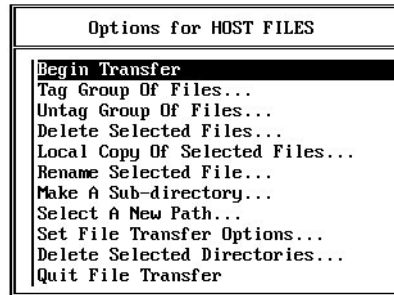


Figure 7-14 The Options For Host Files menu.

Tagging and Untagging Files

You can change drives and directories on either the host or remote side of the file transfer window to find the files you want to transfer. Once you have displayed the directories or files you want to tag, you can tag (or untag) them using either keystrokes or options from one of the file transfer options menus: the Options For Your Files menu (Figure 7-13) and the Options For Host Files menu (Figure 7-14). Table 7-4 lists the keystrokes and the procedures that follow explain how to use the menu options.

Table 7-4 Using the file transfer window

Action	Keystroke
Switch to and from HOST FILES and YOUR FILES	Right Arrow and LeftArrow.
Change drives	Choose <DIR> at the top of the window until you see a list of drives. Then choose the drive.
Change directories	Choose the name of a directory. If you want to move from a subdirectory to its parent directory, choose <DIR> at the top of the window.
Display the file transfer options menu for HOST FILES or YOUR FILES (whichever is currently selected)	Esc
Select a file or directory	UpArrow or DownArrow

Table 7-4 Using the file transfer window

Action	Keystroke
Tag or untag a file and directory	Select the file or directory then press Spacebar. When you tag a directory, you select all its files and subdirectories.
Start transferring tagged files	F2

To tag or untag a group of files:

- 1 Press RightArrow or LeftArrow to select the list of HOST FILES or YOUR FILES.
- 2 Press Esc.
A file transfer options menu appears.
- 3 Choose Select A New Path.
The New Path form appears.
- 4 Type the pathname to the files you want to display, then press Enter.
Make sure you have displayed the files or directories you want to tag or untag.
- 5 Press Esc.
A file transfer options menu appears.
- 6 Do one of the following:
 - To tag a group of files, choose Tag Group Of Files....
 - To untag a group of files, choose Untag Group Of Files....
 The Enter Pattern form appears.
- 7 Type a DOS filename with or without wildcards (* and ?) then press Enter.

Changing File Transfer Preferences

You can use the file transfer options menus to change the file transfer preferences.

To change the file transfer preferences:

- 1 Press Esc from the file transfer window.
A file transfer options menu appears.

2 Choose Set File Transfer Options....

The File Transfer Preferences form appears (Figure 7-15).

Figure 7-15 Use the File Transfer Preferences form to control a variety of options.

File Transfer Preferences	
Destination file:	Verify Before Overwriting
Allow deletion of directories:	No
Compression:	Enabled
Crash recovery:	On

3 You can do any of the following. For details, see the corresponding procedure later in this section.

- Change how duplicate files are handled during file transfer.
- Be asked for a file destination for every file that is transferred.
- Allow directories on the remote PC to be deleted.
- Enable or disable compression during transfers.
- Enable or disable crash recovery.

4 Press Esc to exit the File Transfer Preferences form.

The Save Changes menu appears.

5 Choose No or Yes.

6 Press Esc until you return to a menu you want to use.

To change how duplicate files are handled:

1 Choose Destination File from the File Transfer Preferences form (Figure 7-15).

The Destination File Options menu appears.

2 Choose one of the following:

- Verify Before Overwriting. During file transfer, you will be asked if a duplicate file is to be overwritten or renamed. You can also cancel the transfer of the duplicate file.
- Always Overwrite Duplicate Files. Duplicate files are automatically overwritten.
- Never Overwrite Duplicate Files. Duplicate files are not transferred to the destination directory.

- Always Ask For Destination Name. During file transfer, you are asked for the name of each transferred file. If you use a name that already exists in the destination directory, Norton pcANYWHERE asks you for verification before it overwrites the file.
- Overwrite Older Files Only. Duplicate files are transferred to the destination directory only if they have a more recent date than the file with that name in the destination directory.

To be asked for a file destination for every file:

- 1 Choose Destination File from the File Transfer Preferences form (Figure 7-15).

The Destination File Options menu appears.

- 2 Choose Always Ask For Destination Name.

To allow directories to be deleted:

- 1 Choose Allow Deletion of Directories from the File Transfer Preferences form (Figure 7-15).

The Allow Deletion of Directories menu appears.

- 2 Choose No or Yes.

To enable or disable compression:

- 1 Choose Compression from the File Transfer Preferences form (Figure 7-15).

The Compression menu appears.

- 2 Choose Disabled or Enabled.

To enable or disable crash recovery:

- 1 Choose Crash Recovery from the File Transfer Preferences form (Figure 7-15).

The Crash Recovery menu appears.

- 2 Choose Off or On.

Managing Files and Directories

AWSSEND gives you control over files and directories on both the host and remote PCs. For example, if you want to transfer one or more files from the host to the remote PC, you may need to create a new subdirectory in which to place these files. You can also delete files and directories, copy files locally, and rename files locally.

To create a new directory:

- 1 Select the directory from the YOUR FILES or HOST FILES list where the new directory will reside.
- 2 Press Esc.
A file transfer options menu appears.
- 3 Choose Make A Subdirectory....
The New Directory form appears.
- 4 Type the name of the new subdirectory, then press Enter.

To delete files:

- 1 Tag the file or files that you want to delete.
- 2 Press Esc.
A file transfer options menu appears.
- 3 Choose Delete Selected Files....
If you selected only one file to delete, you are asked to verify the deletion. If you selected more than one file, you are asked if you want to verify each deletion.
 - If you select No, all the files will be deleted.
 - If you select Yes, you are asked to verify the deletion of each file before it is deleted.

NOTE: If the host user has not given the remote user read/write access to a drive, the remote user cannot delete files and directories on that drive.

To delete directories:

- 1 Tag the directory or directories that you want to delete. See “Tagging and Untagging Files,” earlier in this chapter.
- 2 Press Esc.
A file transfer options menu appears.
- 3 Choose Delete Selected Directories....
If you selected only one directory to delete, you are asked to verify the deletion. If you selected more than one directory, you are asked if you want to verify each deletion.
 - If you select No, all the directories will be deleted.

- If you select Yes, you are asked to verify the deletion of each directory before it is deleted.

CAUTION: This option deletes all files and subdirectories within the tagged directory.

To copy files locally:

- 1 Tag the file or files that you want to copy.
- 2 Press Esc.
A file transfer options menu appears.
- 3 Choose Local Copy Of Selected Files....
The Destination form appears.
- 4 Type the destination pathname, then press Enter.
If you have tagged only one file to copy, you can include a new name for the copy of the file.

To rename a file locally:

- 1 Tag the file that you want to rename. (You must have only one file tagged.)
- 2 Press Esc.
A file transfer options menu appears.
- 3 Choose Rename Selected File....
The New Filename form appears.
- 4 Type the new file name then press Enter.

Exiting the File Transfer Program

When you have transferred all the files you want, you exit the file transfer program.

To exit the file transfer program:

- 1 Press Esc from the file transfer window.
A file transfer options menu appears.
- 2 Choose Quit File Transfer.
You are returned to the DOS prompt.

Background File Transfer

File transfers can be performed in the background, but this operation uses an additional 17K of host memory and must be allowed by the host user as a host features preferences. See “Allowing Background File Transfers” in Chapter 6, “Caller Information and Host Preferences.” The remote user can control the file transfer operation, and the host user can run an application undisturbed. The remote PC is dedicated to the file transfer and cannot issue commands to the host PC until the transfer operation is exited. The interface for the background file transfer is the same as that for the AWSEND program.

Use background file transfer when:

- You want to transfer files without the host user’s knowledge of what files are being exchanged.
- When file transfers must take place while the host user is in the middle of another application.
- When the AWSEND program is not available to the host PC, but background transfers are enabled.

Do *not* use background file transfer:

- When the host user, for possible security reasons, needs to know what actions are being taken by the remote user.
- When the additional host memory needed by background file transfer cannot be spared.
- When it is important to use the enhanced data compression available in the AWSEND program.

To invoke background file transfer:

- Choose File Transfer... from the remote’s Session Options menu (Figure 7-7).

Transferring Files from the DOS Command Line

This section explains how to transfer files from the DOS command line of the host or remote PC.

To transfer a file from the DOS command line:

- At the DOS prompt, type:

```
[path]AWSEND filename TO|FROM HOST|REMOTE [path]  
[option]
```

<i>path</i>	The pathname to the directory where your pcANYWHERE files, including AWSEND, are located.
<i>filename</i>	The name of the file or files to be transferred. You can use wildcards.
TO <i>or</i> FROM	Specifies which direction to transfer the file.
HOST <i>or</i> REMOTE	Specifies which PC is sending or receiving.
<i>path</i>	Specifies a drive or subdirectory for the transferred file. Otherwise, files will be stored in the current directory on the receiving PC.
<i>option</i>	One of the following command-line options specifying how destination files should be handled:
	Verifies before overwriting /O:V
	Always overwrites duplicate files /O:A
	Never overwrites duplicate files /O:N
	Overwrites only older files /O:O
	Ask for new destination name (rename) /O:R

For other DOS commands and command-line options that affect remote control sessions, see “Using a DOS Command to Start the Host PC,” “Using a DOS Command to Start the Remote PC,” and “Ending a Session,” earlier in this chapter.

AWSEND Error Level Values

AWSEND sets the ;DOS ERRORLEVEL variable according to the result of the last file transfer. This allows you to transfer files using DOS batch files that take appropriate action based on the success or failure reported in the ERRORLEVEL value. Refer to your DOS manual for a description of the use of ERRORLEVEL. The possible error levels returned from AWSEND are:

Operator cancel	1
Too many retries	2
Connection lost	3
Timeout	4

Disk read error	5
Remote computer canceled	6
Disk write error	7
File not found	8
File create error	9

Using Automated Procedures

As the remote user, you can create and execute an automated procedure that initiates one or more remote control sessions and performs a series of operations while connected to each host PC. The operations can vary from session to session. They can transfer files between the two PCs and/or execute DOS commands on the host and remote PCs. This feature is particularly useful for network administrators and others who want to automate repetitious activities and perform them at predefined times with no users present at either PC. The same operations file can be used for any number of remote control sessions or automated procedures.
online session;
remote control session;

If you design an automated procedure for unattended sessions, the session configurations you use must include all the information necessary to perform the remote control session. No one will be present to answer Norton pcANYWHERE prompts. Be sure to include the password, the host computer name, the host telephone number, and so forth. You should test the procedure before using it for unattended sessions.

The next few sections explain how to create and execute an automated procedure.

Creating and Modifying an Automated Procedure

Creating an automated procedure is really a matter of defining a remote control session or a series of remote control sessions. You specify the time of each session, the operations to perform, and so forth.

Before you create an automated procedure, think about what host PCs you will need to contact. Make sure you have a session configuration for each. Decide what operations you want to perform during the remote control session with each PC. When the operations are the same, you can assign the same operations file to the session definition for each PC.

To create or modify an automated procedure:

- 1 Choose Call A pcANYWHERE Host... from the pcANYWHERE Main menu.

The Call A pcANYWHERE Host menu appears.

- 2 Choose Automated Procedures....

The Automated Procedures menu appears. If this is your first automated procedure, the menu is empty.

- 3 Do one of the following:

- Press Insert to add a new procedure.
- The Procedure Name To Add form appears. Type the name of the procedure, then press Enter.

Or,

- Choose the name of an existing procedure to modify.

The AP Options menu for this procedure appears.

- 4 Choose View/Modify The Procedure.

The Hosts To Call menu for this procedure appears.

- 5 Do one of the following:

- Choose the session configuration you want to modify.

Or,

- Press Insert.

The Select Host For Connection menu appears from which you choose a session configuration.

The Session Options form for this configuration appears (Figure 7-16).

Figure 7-16 Use the Session Options form to define how and when a remote control session will take place.

Session Options for: Dave's SX via IPX	
Time to call:	01:30 (00:00 - 23:59)
Date to call:	02-25-1994
Retries:	3
Time between retries:	30 minutes
Host mode on disconnect:	Original Host Mode
Inactivity timeout:	30 minutes
If error occurs:	Quit This Session Only
File transfer overwrites:	Always Overwrite Duplicate Files
Operations file:	AW.OPR

- 6 To choose an option, see the corresponding procedure in one of the next few sections.
- 7 Press Esc to exit the Session Options form.
The Add New Host menu or Update Host menu appears (depending on whether you are adding or modifying an automated session).
- 8 Choose Yes, or all the information you have defined for the selected host session configuration will be lost.
- 9 Repeat steps 5 through 8 if you want to add an additional remote control session to this automated procedure.
- 10 Press Esc until you return to a menu you want to use.

TIP: The first time you create an automated procedure, you may want to specify times and dates that will allow you to test the procedure. This way you can be sure all the operations and sessions are correctly entered, and that the host and remote PCs are set up properly.

Specifying the Time and Date

You specify the time and the date for the connection to take place. If you leave this blank, Norton pcANYWHERE provides settings that allow the procedure to be run at any time and on any day.

To specify the time:

- 1 Select Time To Call.
- 2 Type the time of day you want this automated procedure to take place, then press Enter. Use the 24-hour clock and the format hh:mm.

The default is the current time. If you leave this option blank, Norton pcANYWHERE inserts NOW so the procedure can be executed any time.

To specify the date:

- 1 Select Date To Call.
- 2 Type the date of the year you want this automated procedure to take place, then press Enter. Use the format mm-dd-yyyy.

The default is the current date. If you leave this option blank, Norton pcANYWHERE inserts TODAY so the procedure can be executed any day.

Specifying the Number of Retries and the Time Between Them

You can specify the number of times the connection will be retried if it fails and the time interval between those attempts.

To specify the number of retries:

- 1 Select Retries.
- 2 Type the number of attempts (from 0 to 99) the procedure will make to connect to the specified host PC, then press Enter.

The default is 3.

To specify the time interval between retries:

- 1 Select Time Between Retries.
- 2 Type the number of minutes (from 0 to 99) the procedure will wait between connection attempts, then press Enter.

The default is 30.

Specifying the Host Mode After the Session

If the host user has given you permission to do so, you can set the mode in which the host PC is left after the session ends. See “Allowing the User to Change the Host Mode” in Chapter 6, “Caller Information and Host Preferences.”

To specify the mode the host PC will be left in after the session ends:

- 1 Choose Host Mode on Disconnect.
The Host Disconnect Options menu appears.
- 2 Choose the mode you want the host PC left in when the connection ends:
 - Host Waits For Another Call. The host PC will be left in waiting mode.
 - Hotkey To Reactivate Host. The host PC will be left in hotkey mode.
 - Host Accepts Calls At Any Time. The host PC will be left in incoming-call mode.
 - Original Host Mode (the default). This is the mode the host PC was in prior to this session.

- **Cancel Host Operation.** This removes the host TSR from memory and cancels pcANYWHERE.

Specifying the Length of the Inactivity Timeout

Inactivity is defined as the absence of keystrokes, mouse movements, and video data transfers. You specify a time limit after which an inactivity timeout occurs. This can be particularly useful when an unattended host PC crashes.

To specify the inactivity timeout:

- 1 Select Inactivity Timeout.
- 2 Type the number of minutes (from 0 to 999) the procedure will wait between connection attempts, then press Enter.

The default is 30. Zero means there is no inactivity timeout.

Determining What Action to Take After an Error

You decide what to do if an error occurs. Examples of errors include a failed file transfer or an expired inactivity timeout period.

To specify what to do if an error occurs:

- 1 Choose If Error Occurs.
The If Error Occurs menu appears.
- 2 Choose the action to take if an error occurs:
 - **Continue Session.** This continues the current remote control session despite the error.
 - **Quit This Session Only.** This ends the current remote control session and proceeds to the next one specified by the automated procedure.
 - **Quit Automated Process.** This ends the entire automated procedure.

Handling Transferred Files

You set file transfer preferences that determine how to handle files, particularly duplicate files, during a file transfer.

To specify how to handle files during a file transfer:

- 1 Choose File Transfer Overwrites.
The Destination File Options menu appears.

- 2 Choose the action to take when the name of a file being transferred has the same name as a file in the directory to which it is being transferred.
 - Always Overwrite Duplicate Files (the default). The file transfer always takes place.
 - Never Overwrite Duplicate Files. The file transfer is aborted for this file.
 - Overwrite Older Files Only. The file transfer takes place if the transferred file is the more recent of the two files.

Creating and Modifying an Operations File

The operations file determines what actions will be performed during the remote control session. It has the extension .OPR and the default file is AW.OPR. You fill it with DOS commands to be executed on either the host or remote PC, comments, and file-transfer commands.

You can assign the same operations file to more than one session defined for the same procedure or to sessions in other procedures. However, any time you modify an operations file, you change the outcome of every remote control session to which it is assigned.

To create or modify an operations file:

- 1 Choose Operations File.

The Select Path for Operations File form appears.

- 2 Type a new pathname or accept the default pathname, then press Enter. Do not type the filename at this step.

The Available Files menu appears.

- 3 Do one of the following:

- Choose the name of an existing operations file.

Or,

- Press Insert to create a new file.

The Enter File Name form appears. Type the name of the file, then press Enter.

The Operations menu for the selected host session appears (Figure 7-17).

Figure 7-17 You can send and receive files, as well as perform DOS commands on either PC.

Operations for: Dave's SX via IPX	
COMMENT:	Automated Procedure to maintain Host PC
HOST DOS:	CD\NNU8
HOST DOS:	NDD C: /C /R:C:\NDD.RPT
HOST SEND:	C:\NDD.RPT TO C:\REPORTS\SITE1.RPT
REMOTE SEND:	F:\ACCT\CUSTINFO.DB TO H:\ACCT\CUSTINFO.DB
REMOTE DOS:	COPY C:\REPORTS\SITE1.RPT LPT1:

- 4 You can add, delete, move, or modify an operation. For details, see the corresponding procedure in one of the next few sections.
- 5 Repeat step 4 until the file contains all the operations you want to perform on the host PC.
- 6 Press Esc to exit the Operations menu.
The Update Operations File menu appears.
- 7 Choose Yes, or your changes to the operations file will be lost.
- 8 Press Esc to exit the Session Options form.

Adding an Operation

For each DOS command you want to execute and each file transfer you want to perform during the remote control session, you add an operation to the operations file. In addition, you can add comments to explain the purpose of the operations. Figure 7-17 shows a short procedure using one of each of the possible operations.

To add an operation:

- 1 Position the cursor.
To add an operation to the end of the file, position the cursor on the last line. If the cursor is positioned anywhere else, the line for the operation will be inserted above the cursor.
- 2 Press Insert.
The Operation Type menu appears.
- 3 You can do any of the following:
 - Add a DOS command to be executed on the host PC.

- Add a DOS command to be executed on the remote PC.
- Add an operation that transfers files from the host to the remote PC.
- Add an operation that transfers files from the remote to the host PC.
- Add a comment or remark to the operations file. This is not executed. Use it to remind yourself about the purpose of the operation it follows or precedes.

For details, see the corresponding procedure in one of the next few sections.

- 4 Press Esc to exit the form.
The Add New Command menu appears.
- 5 Choose Yes, or your operation or comment will be lost.

NOTE: Remember that the pcANYWHERE programs will be in memory while the DOS commands you specify are executed. This limits the amount of memory available for running other programs (via a DOS command in the automated procedure) on the host and remote PC during an automatic procedure execution.

To add a DOS command:

- 1 Choose Execute DOS Command On Host or Execute DOS Command On Remote.
The Operation form appears.
- 2 Type the command, check it for accuracy, then press Enter.

To add an operation that transfers files:

- 1 Choose Send Files(s) From Host To Remote or Send Files(s) From Remote To Host.
The Operation form appears.
- 2 Type the complete pathname to the source files, check it for accuracy, then press Enter. You can use wildcards. (For example, C:\MYFILES*.*.)
- 3 Type the complete destination pathname, check it for accuracy, then press Enter. (For example, D:\NEWFILES.)
Do not place a backslash (\) after the last subdirectory name. If you used wildcards in the Source Name, the Destination Name must be a

subdirectory. When you send multiple files, the files will have the same name on both PCs. If you send just one file, you can rename it with the setting for Destination Name.

To add a comment to the operations file:

- 1 Choose Comment.
The Comment form appears.
- 2 Type the comment then press Enter.

Deleting an Operation

You can delete any operation or comment.

To delete an operation:

- 1 Position the cursor on the operation you want to delete.
- 2 Press Delete.
The Delete menu appears.
- 3 Choose Yes (the default).

Moving an Operation

You can move any operation or comment.

To move an operation:

- 1 Position the cursor on the operation you want to move.
- 2 Press Delete.
The Delete menu appears.
- 3 Choose Yes (the default).
- 4 Position the cursor below the line where you want to insert the deleted operation.
- 5 Press Insert.
The Insert Deleted Entry menu appears.
- 6 Choose Yes (the default).

Modifying an Operation

You can modify any operation or comment.

To modify an operation:

- 1 Position the cursor on the operation you want to modify.
- 2 Press Enter.
The Operation or Comment form displays the current version of your operation or comment.
- 3 Change the DOS command, comment, source pathname, or destination pathname as appropriate. Then press Enter.

NOTE: If you are modifying a file-transfer operation, you press Esc to exit the form.

The Modify Command menu appears.

- 4 Choose Yes (the default).

Executing an Automated Procedure

When you execute an automated procedure, Norton pcANYWHERE prompts you for any missing information and waits for an answer—even if no one is there. If the automated procedure is intended to be used for unattended sessions, you need to be sure that all the session configurations and so forth are complete. You also need to be sure that each host PC is waiting for a connection at the appropriate time.

You have two choices for setting up a host to be called:

- Put the host in waiting mode (using Wait For a Connection or a DOS command). The caller information for the remote user (running the automated procedure) must have the Command To Execute option set to AWSEND. (You don't have to run AWLOGOFF for this use of the Command To Execute option. Norton pcANYWHERE does it for you automatically.)
- Leave the host in any mode that will accept an incoming call with background file transfer capability enabled. In this case, however, your procedure cannot contain any DOS commands to be executed on the host PC. They will be treated as errors.

To execute an automated procedure:

- 1 Choose Call A pcANYWHERE Host... from the pcANYWHERE Main menu.

The Call A pcANYWHERE Host menu appears.

- 2 Choose Automated Procedures....

The Automated Procedures menu appears.

- 3 Choose the procedure you want to execute.

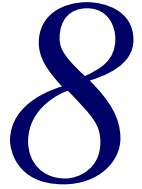
The AP Options menu for this procedure appears.

- 4 Choose Execute The Procedure.

The procedure starts.

NOTE: If the procedure has defined any remote control sessions that were to have taken place prior to the current time, a warning message and the Execute Options menu appears. Choose Execute All Sessions (which updates the inappropriate times to the current time), Execute Future Sessions (which ignores sessions it is too late to perform), or Quit Procedure.

Online Sessions



This chapter explains how to start a Norton pcANYWHERE online session. An online service is a service such as CompuServe, Dow Jones, MCI Mail, or an electronic bulletin board (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 for DOS 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, session configuration, and online preferences set on your PC. Be sure to complete the necessary installation and configuration procedures described in the preceding chapters before beginning. 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.

Norton pcANYWHERE supports only services that have full-duplex transmission.

This chapter covers:

- Initiating an online session or waiting for an online service to connect to your PC
- Controlling an online session
- Transferring files during a session

Initiating the Session or Waiting to Connect

This section explains how to initiate an online session or wait for the online service to connect to you. Usually, as the remote user, you initiate the online session. Occasionally, the service initiates the online session. For the service to do so successfully, your PC must be in waiting mode.

You can initiate the session:

- Using the menus provided by Norton pcANYWHERE.

- Using a DOS command that bypasses one or more of the menus. You can type the command at the DOS prompt or put it in the AUTOEXEC.BAT or another batch file. See “Using a DOS Command to Start the Remote Program,” next.
- Using a script. You can initiate an online session or conduct part or all of the session using a script. See the reference guide, *Creating Norton pcANYWHERE Scripts*, for more information.

Upon connection, your PC displays Terminal mode and the online session begins. You log in and operate the service as it was designed to be used.

To initiate an online session:

- 1 Choose Call An Online Service... from the pcANYWHERE Main menu.

The Call An Online Service menu appears.

- 2 Choose Connect To An Online Service....

The Select Online Service menu appears.

NOTE: If you haven't already provided a name for your PC, you are prompted for one.

- 3 Choose the session configuration for the online service that you want to connect to.

The Connect Options menu appears.

- 4 Do one of the following:

- To initiate the session, choose Call.

Depending on what information is missing from the hardware and session configurations, you may have to type a telephone number or choose a gateway from a list of those on the LAN.

Norton pcANYWHERE displays the current status of the connection while waiting for the online service to respond.

Or,

- To wait for an online service to connect, choose Wait For a Call.

Norton pcANYWHERE displays the current status of the connection while you wait. While your PC is waiting for a connection, it cannot be used.

Using a DOS Command to Start the Remote Program

You can bypass a number of the steps in the above procedures by activating the remote program from the DOS prompt. See Table 8-1.

Table 8-1 Starting the Program from the DOS Prompt

Action	Command
Start Norton pcANYWHERE with the Call An Online Service menu.	AW /O:S
Initiate an online session.	AW /O:S /M:D /N: <i>session_configuration_name</i>
Initiate an online session with a script.	AW /O:S /M:S /N: <i>script_name</i>

If the name of the directory you specified for Norton pcANYWHERE during the installation (or the network path specified by your network administrator) is not in your PATH, precede AW with the correct pathname.



Network

NETWORK USERS: If Norton pcANYWHERE has been installed to a network, be sure to include the `/I:userid` command-line option in conjunction with the normal command line. Replace *userid* with the same ID you used to start the network installation of Norton pcANYWHERE. For example:

```
AW /I:userid /O:S.
```

Using Quick Connect

You can connect to an online service without setting up either a hardware or session configuration. You provide the minimal information necessary and pcANYWHERE makes the connection. However, it is more convenient in the long run to create the configurations (which save all your settings) in the following situations:

- This is not the only service you call.
- You will be calling this particular service again.

To make a quick connection:

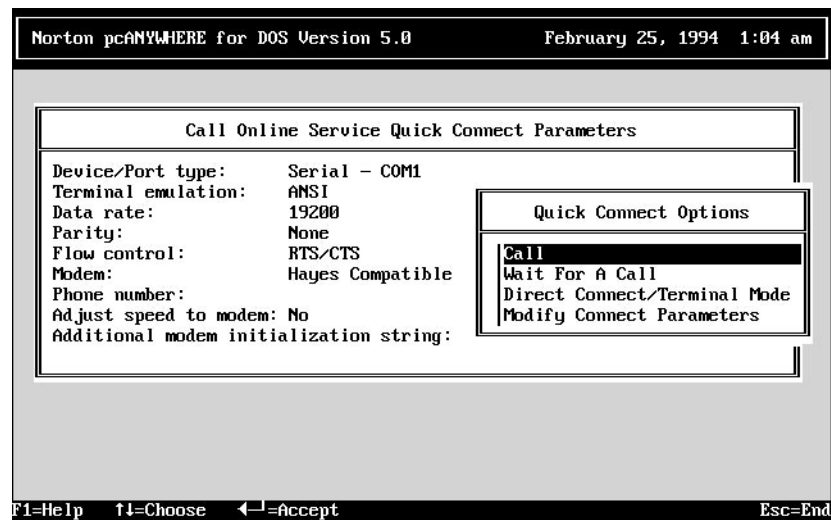
- 1 Choose Call An Online Service... from the pcANYWHERE Main menu.

The Call An Online Service menu appears.

- 2 Choose Quick Connect....

The Call Online Service Quick Connect Parameters form appears (Figure 8-1) along with the Quick Connect Options menu.

Figure 8-1 Quick Connect is a fast way to make a connection.



- 3 Choose Modify Connect Parameters from the Quick Connect Options menu.

The Call Online Service Quick Connect Parameters form becomes active.

- 4 All of the parameters (except for Terminal Emulation and Phone number) are hardware configuration options. See Chapter 3, "Hardware Configurations," for more information about setting these. For example, if you will connect to the online service using a modem attached to your PC, see "Creating a Modem Hardware Configuration" in Chapter 3. If you are using a gateway on your network, see "Creating a Node Hardware Configuration" also in Chapter 3.

- 5 Choose Terminal Emulation.

The Terminal Emulation menu appears.

- 6 Choose the emulation expected by the online service.
- 7 Select Phone Number if you are going to initiate the connection.
Type the phone number for the online service, including any prefix or suffix, then press Enter.
- 8 Press Esc.
- 9 Choose Call or Wait For A Call from the Quick Connect Options menu.
Norton pcANYWHERE displays the current status of the connection while you wait for the online service to respond or to initiate a connection.

NOTE: You can choose Direct Connect/Terminal Mode and talk directly to your modem via a terminal window. See your modem's manual for details about the commands.

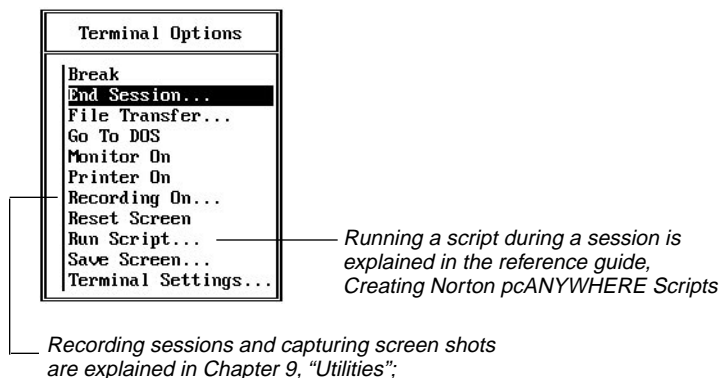
Managing the Online Session

Once the connection to the online service is made, Norton pcANYWHERE provides a menu that allows you to manage the online session.

To access the Terminal Options menu:

- 1 Press the remote hotkey.
The Terminal Options menu appears (Figure 8-2).

Figure 8-2 Use the Terminal Options menu to manage the session.



- 2 See the corresponding procedure in one of the next few sections.
- 3 Press Esc to return to the online session.

Sending a Break Signal

You can send a break signal to the online service if your connection is a serial connection. The effect of this signal depends on the service and the activity you are performing. For example, some mainframes use the break signal to interrupt the current activity. Send a break signal only if you understand the effect it will have on the service and want that effect. (You specify the length of the break signal as part of the hardware configuration.)

NOTE: Do not confuse a break signal with the Ctrl+Break key on a PC. The break signal is a hardware function and has nothing to do with a keystroke.

To send a break signal:

- Choose Break from the Terminal Options menu.

Ending the Session

Before you end the online session, you should log off or follow whatever ending procedure is expected by the service.

To end the session:

- 1 Choose End Session... from the Terminal Options menu.
The Disconnect menu appears.
- 2 Choose No or Yes (the default).
The Call An Online Service menu reappears.

Accessing Your PC During a Session

To access your PC's files, applications, and so forth during an online session, use the Go To DOS option.

To access your own files and applications:

- Choose Go To DOS from the Terminal Options menu.
The DOS prompt appears.

To return to the online session:

- Type `exit` at the DOS prompt. Then press Enter.

Monitoring Control Codes

You can display on your screen all received control codes (that is, non-displayable data such as carriage returns) using the equivalent IBM graphic character set. This allows you to analyze received data on the screen. The codes do not have their usual effect. For example, a received carriage return is displayed as a musical note, and the cursor does not move to the next line. Monitoring control codes is an advanced feature used for troubleshooting.

To monitor control codes:

- Choose Monitor On from the Terminal Options menu.

After you choose the Monitor On command, the terminal status line displays MON, monitoring begins, and the command toggles to Monitor Off. To stop monitoring control codes, choose Monitor Off from the Terminal Options menu.

Printing

You can turn printing on and off from the Terminal Options menu. You can also change the destination for printed output on your PC.

To turn printing on:

- 1 Choose Printer On from the Terminal Options menu.
The Remote Print Device menu appears.
- 2 Choose a new print device: LPT1, LPT2, LPT3, PRN, or Spool File.
If you choose Spool File, the default spool file AW.SPL is used.

To change the spool file:

- 1 Choose Printer On from the Terminal Options menu.
The Remote Print Device menu appears.
- 2 Choose Select Spool File....
The Select Path For Spool File form appears.
- 3 Use the default directory (where the pcANYWHERE files are installed) or type in a new one. Then press Enter.

Do not type the filename at this step.

The Available Files menu appears. The default file is AW.SPL.

4 Do one of the following:

- Choose the .SPL file to use as a spool file.
- Press Insert to create a new spool file.

The Enter File Name form appears. Type the name of the file then press Enter.

The Remote Print Device menu reappears with Spool File already selected.

5 Press Esc to return to the Terminal Options menu.

To turn printing off:

- Choose Printer Off from the Terminal Options menu.

Clearing the Screen

To clear the screen and place the cursor in its upper-left corner, you use the Reset Screen option.

To clear the screen:

- 1** Choose Reset Screen from the Terminal Options menu.
The Reset menu appears.
- 2** Choose No or Yes (the default).

Changing Terminal Settings

Terminal settings allow you to adjust some of the options from your hardware and session configurations. For example, you may need to change the type of terminal emulation, the data rate, or the parity.

These options were originally set in either the session configuration or hardware configuration. If you need to change them for this session, you may want to modify them in the configurations later. See Chapter 4, “Hardware Configurations,” and Chapter 6, “Session Configurations and Remote Preferences.”

- 1** Choose Terminal Settings from the Terminal Options menu.
The Current Terminal Settings form appears (Figure 8-3).

Figure 8-3 The terminal settings affect how you interact with the online service.

Current Terminal Settings	
Terminal emulation:	ANSI
Data rate:	9600
Parity:	Even
Flow control:	RTS/CTS
Break length:	5 (10ths/sec)
Line wrap:	No
Screen wrap:	No
<BS> key:	Non-Destructive
Received <CR>:	CR
Macro keys:	AW, MK6
Translation table:	Disabled

- 2 To change a terminal setting, see the corresponding procedure in one of the next few sections.
- 3 Press Esc to return to the Terminal Options menu.
- 4 Press Esc to return to the online session.

Changing the Terminal Emulation

You can change the terminal emulation during the session. (This is set originally in the session configuration.)

To change the terminal emulation:

- 1 Choose Terminal Emulation.
The Terminal Emulation menu appears.
- 2 Choose the correct emulation type.

Changing the Data Rate

You can change the data rate during the session. (This is set originally in the hardware configuration.)

To change the data rate:

- 1 Choose Data Rate.
The Data Rate menu appears.
- 2 Choose a rate.
See Appendix A, “Technical Information,” for an explanation of rates.

Changing the Parity

You can change the parity during the session. (This is set originally in the hardware configuration.)

To change the parity:

- 1 Choose Parity.
The Parity menu appears.
- 2 Choose None, Odd, Even, Mark, or Space.
See Appendix A, “Technical Information,” for an explanation of parity.

Changing the Flow Control

You can change the flow control during the session. (This is set originally in the hardware configuration.)

To change the flow control:

- 1 Choose Flow Control.
The Flow Control menu appears.
- 2 Choose None, X-ON/X-OFF, RTS/CTS, or Both.
See Appendix A, “Technical Information,” for an explanation of flow control.

Changing the Break Length

You can change the break length during the session. (This is set originally in the hardware configuration.)

To change the break length:

- 1 Select Break Length.
- 2 Type a number of tenths of seconds from 0 to 99. Then press Enter.

Changing the Line Wrapping

You can change how lines are wrapped during the session. (This is set originally as one of the emulation preferences in the session configuration.)

To change line wrapping:

- 1 Choose Line Wrap.
The Line Wrap menu appears.

- 2 Choose No if you want the line to end with the last character position in the line.
Or,
Choose Yes if you want lines to wrap to the next line when the number of characters exceeds the length of the line.

Changing the Screen Wrapping

You can change how lines wrap from the beginning to the end of the screen during the session. (This is set originally as one of the emulation preferences in the session configuration.)

To change screen wrapping (which works only when Line Wrap is On):

- 1 Choose Screen Wrap.
The Screen Wrap menu appears.
- 2 Choose No if you want the screen to end with the last character position in its line.
Or,
Choose Yes if you want lines to wrap from the bottom of the screen to the top when the number of characters in the last line exceeds the length of the screen.

Changing the Backspace Key

You can change the functionality of the backspace key during the session. (This is set originally as one of the emulation preferences in the session configuration.)

To change the use of the backspace key:

- 1 Choose BS Key.
The BS Key menu appears.
- 2 Choose Non-Destructive if you want pressing the backspace key to simply move the cursor backward *without* deleting any characters.
Or,
Choose Destructive if you want pressing the backspace key to delete the characters to the left of the cursor as the cursor moves backward.

Changing Received Carriage Returns

You can change the way carriage returns received from the online service are interpreted during the session. (This is set originally as one of the emulation preferences in the session configuration.)

To change the carriage returns received from the online service:

- 1 Choose Received CR.
The Received CR menu appears.
- 2 Choose CR if you want each carriage return to be interpreted as a carriage return only.
Or,
Choose CR/LF if you want each carriage return to be interpreted as a carriage return/linefeed.

Changing the Macro Keys

The macro keys can be specified as part of the session configuration or during the session. You assign string expressions to the keys Alt+0 through Alt+9 and store them in a file with the extension .MK6. The string expressions can include control characters, such as ^M for a carriage return or ^J for a linefeed. For example, you may want to use macro keys for an online service account name and password.

You can have several .MK6 files, and you can assign the same .MK6 file to more than one session configuration.

NOTE: If you are using macro keys with a direct connection, you need to use a data rate of 19,200 or lower.

To specify or modify a set of macro keys:

- 1 Choose Macro Keys.
The Macro Keys menu appears.
- 2 Choose Enabled.
The Select Path For Macro Key File form appears.
- 3 You can accept the default directory (where Norton pcANYWHERE is installed) or type the path to a new directory. Then press Enter.
Do not type the filename at this step.
The Available Files menu appears. The default file is AW.MK6.

- 4 Do one of the following:
 - Choose the .MK6 file which contains the macro keys you want to use.
 - Press Insert to create a new file for macro keys.
The Enter File Name form appears. Type the name of the file then press Enter.
The Macro Keys form displays the macro keys from the selected file. The macro keys are Alt+0 through Alt+9.
- 5 If you want to make additions or modifications:
 - a Select a key.
 - b Type the characters you want to send to the service when the selected key is pressed. Then press Enter.
- 6 Repeat step 5 for any other keys you want to add or modify.
- 7 Press Esc to exit the Macro Keys form.

To disable the use of macro keys:

- 1 Choose Macro Keys.
The Macro Keys menu appears.
- 2 Choose Disabled.

Changing the Translation Table

The use of translation tables is an advanced feature that is part of the session configuration. They are used to 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 session configuration. See Appendix B, "Terminal Emulation," for more information.

To change which translation table is being used:

- 1 Choose Translation Table.
- 2 Choose Enabled.
The Select Path For Translation Table form appears.
- 3 You can accept the default directory (where Norton pcANYWHERE is installed) or type the path to a new directory. Then press Enter.
Do not type the filename at this step.
The Available Files menu appears. The default file is AW.TRN.

- 4 Choose the name of the .TRN file that contains the translation table you want to use.

To create or modify a translation table:

- 1 Do steps 1 through 3 in the above procedure, “To change which translation table is being used.”
- 2 Do one of the following:
 - Choose the name of the .TRN file that contains the translation table you want to modify.
 - Press Insert to create a new file for a translation table.
The Enter File Name form appears. Type the name of the file then press Enter.

The Translation Table menu appears. Each translation table has two parts: one for received characters and one for transmitted characters.

- 3 Choose Receive or Transmit, depending on which part of the table you want to specify or modify.

The Receive Translation Table form or the Transmit Translation Table form appears.

The form displays the hex codes for the 256 characters (00 to FF) in the extended ASCII set (see Appendix B, “Terminal Emulation”). The form has 16 rows and 16 columns; the rows represent the first digits of the hex codes (0 to F) and the columns represent the second digits. As you select a code, the character it represents appears in the upper-right corner of the form. For example, 41 is “A” and 61 is “a.” If you change the hex code 41 to 61 in the Receive Translation Table, “a” will be displayed for every “A” that is received.

- 4 Select the hex code for a character you want to change, then type in the hex code for its translation.
- 5 Repeat step 4 for any characters you want to modify.
- 6 Repeat steps 3 through 5 for the other translation table form.
- 7 Press Esc twice to exit.

To disable the use of the translation table:

- 1 Choose Translation Table.
The Translation Table menu appears.
- 2 Choose Disabled.

Transferring Files

You can receive files from or send files to an online service. To do so, you must follow the procedures required by the online service and by Norton pcANYWHERE for receiving or sending files.

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, you use the Terminal Options menu.

If the protocol is ASCII or ZMODEM, you need to set a number of preferences for the protocol. You may have done this when you set online preferences. See “Setting Protocol Preferences for Online Sessions” in Chapter 5, “Session Configurations and Remote Preferences.”

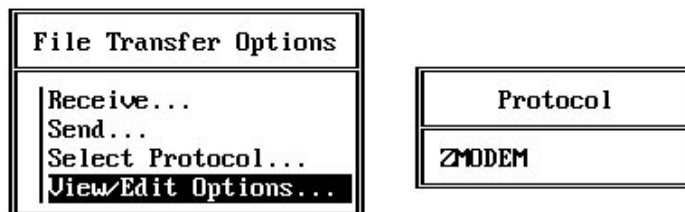
For example, you let the online service know what files you want to receive and then use pcANYWHERE's Terminal Options menu to receive the files; or you can prepare the service to receive files and the Terminal Options menu to send them.

To receive (download) files from the service:

- 1 Do what the service requires to send files.
- 2 If the protocol allows autodoing, Norton pcANYWHERE automatically starts to download the files.

Otherwise, the File Transfer Options menu appears along with a status box indicating the current protocol for transferring files (Figure 8-4).

Figure 8-4 Use the File Transfer Options menu to change the protocol (if necessary) and then upload or download files.



- a Choose Receive.

The Select Path For Received Files form appears.

- b Type the name of the directory where you want to store the downloaded files. Then press Enter.

The Receiving form displays the name of the file being transferred, its size, percentage transferred, and so forth.

To send (upload) files to the service:

- 1 Do what the service requires to receive files.
- 2 Choose File Transfer... from the Terminal Options menu.
The File Transfer Options menu appears along with a status box indicating the current protocol for transferring files (Figure 8-4).
- 3 Choose Send.
The Select Files to Send form appears.
- 4 Type the pathname to the file or files you want to upload. You can use wildcards (* and ?). Then press Enter.

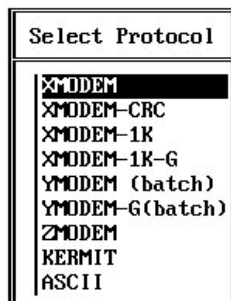
NOTE: If you type a pathname to a directory in the Select Files to Send form, the Available Files menu appears when you press Enter, and you can select one file to upload.

The Sending form displays information about the transfer.

To change the protocol used by Norton pcANYWHERE:

- 1 Choose File Transfer... from the Terminal Options menu.
The File Transfer Options menu appears along with a status box indicating the current protocol for transferring files (Figure 8-4).
- 2 Choose Select Protocol...
The Select Protocol menu appears (Figure 8-5).

Figure 8-5 Norton pcANYWHERE offers a variety of file transfer protocols.



- 3 Choose a protocol acceptable to the online service.
Your choice appears in the Protocol status box.

NOTE: If you choose the ZMODEM or ASCII protocols, you can also set options for the protocol by choosing View/Edit Options... from the Terminal Options menu. See “Setting Preferences for Online Sessions” in Chapter 5, “Session Configurations and Remote Settings,” for an explanation of these options.

This chapter explains the utilities that come with Norton pcANYWHERE for DOS:

- **Hardware Diagnostics.** This utility tests your communications ports, keyboard, and video display. It also lets you review your hardware, environment, and AUTOEXEC.BAT and CONFIG.SYS files.
- **Playback Sessions/Screens.** This utility plays back recorded remote control and online sessions or specific screens you have saved from these sessions. How you, as the remote user, record the sessions and capture the screen shots is also explained.
- **Activity Log Processing.** This utility manages the data about sessions that is logged on the host or remote PC. Log files 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.
- **Preprocess Scripts.** This utility preprocesses (compiles) a script file. For more information see *Creating Norton pcANYWHERE Scripts*, which accompanies this user's guide.

Checking Your Hardware

Using Hardware Diagnostics, you can determine:

- The number of parallel ports and serial ports that you have.
- The type of your keyboard: 84-Key AT or 101/102-Key Enhanced.
- The amount of memory (RAM) on your primary and/or secondary video adapter and its type: Monochrome Display Adapter, Hercules Monochrome (HGC), Color Graphics Adapter (CGA), Enhanced Graphics Adapter (EGA), Multi-Color Graphics Array (MCGA), or Video Graphics Array (VGA).
- The type of your monitor: Monochrome, Color, Digital Color, Analog Monochrome, or Analog Color.

To check what hardware you have:

- 1 Choose Utilities... from the pcANYWHERE Main menu.
The Utilities menu appears.

- 2 Choose Hardware Diagnostics....
The Diagnostics Main menu appears.
- 3 Choose Overview....
The Overview Options menu appears.
- 4 Choose Hardware....
The Hardware form displays information about your communications hardware (Figure 9-1).

Figure 9-1 Check the number of ports and the type of your keyboard, adapters, and monitor.

Hardware	
Parallel ports :	1
Serial ports :	2
Keyboard :	Enhanced
Primary video adapter :	UGA w/256K or more RAM
Secondary video adapter :	NONE
Monitor :	Color

Reviewing the DOS Environment

You can review your PATH and the settings for other DOS environment variables.

To read the current DOS environment settings:

- 1 Choose Utilities... from the pcANYWHERE Main menu.
The Utilities menu appears.
- 2 Choose Hardware Diagnostics....
The Diagnostics Main menu appears.
- 3 Choose Overview....
The Overview Options menu appears.
- 4 Choose Environment....
The Environment... form displays each variable and its setting.

Reviewing Configuration Files

You can review your AUTOEXEC.BAT and CONFIG.SYS files.

To read either your AUTOEXEC.BAT or CONFIG.SYS file:

- 1 Choose Utilities... from the pcANYWHERE Main menu.
The Utilities menu appears.
- 2 Choose Hardware Diagnostics....
The Diagnostics Main menu appears.
- 3 Choose Overview....
The Overview Options menu appears.
- 4 Choose AUTOEXEC.BAT... or CONFIG.SYS....
You are asked to enter the name of your boot drive.
- 5 Type the drive letter for the drive where the file resides, then press Enter.
The AUTOEXEC.BAT or CONFIG.SYS form displays the contents of the file you chose.
- 6 Press Esc to return to a menu you want to use.

Testing Your Hardware Configurations

You can test each of your hardware configurations. See Chapter 3, “Hardware Configurations,” for more details.

For a serial hardware configuration, you can:

- Check the port.
- Check the status of signals: Clear To Send (CTS), Data Set Ready (DSR), Ring Indicator (RI), Carrier Detect (DCD).
- Test the modem by initializing it in auto-answer mode. (This test is available only when a modem is specified in the configuration.)

For a network hardware configuration, you can:

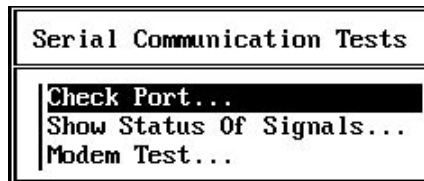
- Check the network driver.
- Test network communications.

To test any hardware configuration:

- 1 Choose Utilities... from the pcANYWHERE Main menu.
The Utilities menu appears.
- 2 Choose Hardware Diagnostics....
The Diagnostics Main menu appears.

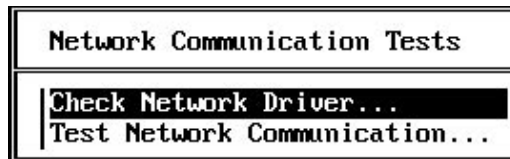
- 3 Choose Communications Tests....
An overview of the tests appears.
- 4 Read the overview, then press Enter.
The Hardware Configurations menu appears.
- 5 Choose the configuration you want to test.
The Configuration form displays the hardware configuration you chose. You can modify the configuration as explained in Chapter 3, "Hardware Configurations," if you need to.
- 6 Press Esc to continue.
If you chose a serial hardware configuration, the Serial Communication Tests menu appears (Figure 9-2).

Figure 9-2 Check a serial hardware configuration.



If you chose a network hardware configuration, the Network Communication Tests menu appears (Figure 9-3).

Figure 9-3 Check a network hardware configuration.



- 7 Choose the test you want to perform. Read the information on the screen and press Esc or Enter as appropriate.
After each test, the menu reappears so you can choose another test.
- 8 Press Esc to exit the Serial Communication Tests or Network Communication Tests menu.
The Hardware Configurations menu reappears
- 9 Repeat steps 5 through 8 if you want to test another configuration.
- 10 Press Esc to return to a menu you want to use.

Testing Your Video Adapter

You can test your primary video adapter for:

- Snow (if the adapter is CGA).
- Horizontal and vertical synchronization.
- Graphics detection (if the adapter is a CGA or a Hercules adapter).
- Ability to display types of cursors. You are asked to check these visually. For example, you are asked if the cursor is blinking or not.
- Video memory (RAM) conflicts.
- Ability to display various video modes (such as 40-column monochrome and 80-column color modes). You are asked to check these visually.
- Ability to display various colors. You are asked to check these visually.

To test a video adapter:

- 1 Choose Utilities... from the pcANYWHERE Main menu.
The Utilities menu appears.
- 2 Choose Hardware Diagnostics....
The Diagnostics Main menu appears.
- 3 Choose Video Tests....
An overview of the tests appears.
- 4 Read the overview, then press Enter.
The Video Tests menu appears.
- 5 Choose the test you want to perform. Read the information on the screen and press Esc, Enter, Y, or N as appropriate.
After each test, the menu reappears so you can choose another test.
- 6 Press Esc to exit the Video Tests menu.
The Results of Video Tests form appears (Figure 9-4) giving the status of each test: N/A, untested, passed, or failed.

Figure 9-4 The results of the video tests for one PC.

Results Of Video Tests	
Adaptor Causes Snow:	N/A
Horizontal/Vertical Synch Test:	PASSED
Graphics Detection Test:	N/A
Cursor Tests:	PASSED
RAM Conflict:	PASSED
Graphics Modes Test:	PASSED
Color Bar Test:	PASSED
Press <Esc> to continue...	

- 7 Press Esc to return to a menu you want to use.

Testing Your Keyboard

You can test your keyboard for:

- Support of function keys.
- Support of the RightShift, LeftShift, Alt, and Ctrl keys. You are asked to press them and see the results.
- Keyboard lights. You are asked to check these visually.
- Scan codes. You are asked to press keys and see the results.
- Whether or not an application controls the keyboard. When the result of this test is APP, a remote user using this PC as a host PC may need a special keyboard handler to perform remote control. (If you run this test while the host TSR is loaded, you will always be informed that an application is running the keyboard. This will not be an indication that a keyboard handler is needed.)

To test your keyboard:

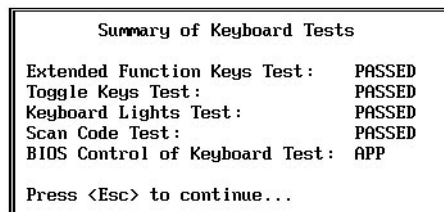
- 1 Choose Utilities... from the pcANYWHERE Main menu.
The Utilities menu appears.
- 2 Choose Hardware Diagnostics....
The Diagnostics Main menu appears.
- 3 Choose Keyboard Tests....
The Keyboard Tests form appears.
- 4 Choose the test you want to perform. Read the information on the screen and press keys as appropriate.

After each test, the Keyboard Tests menu reappears so you can choose another test.

- 5 Press Esc to exit the Keyboard Tests menu.

The Summary of Keyboard Tests form appears (Figure 9-5) giving the status of each test: N/A, untested, passed, or failed. The APP status for the BIOS Control of Keyboard Test indicates that an application controls the keyboard; the BIOS status indicates that the BIOS controls the keyboard.

Figure 9-5 The results of the keyboard tests for one PC.



- 6 Press Esc to return to a menu you want to use.

Recording Sessions

It is often helpful to have a record 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 can play back the recording to review the exact steps demonstrated.

You can record a session manually or automatically in one or more .RCD files. Recording a session manually is much like operating a VCR or audio tape recorder. You turn recording on and off when you want to. Each start and stop define the beginning and ending of a recorded session. In the recorded file, sessions are numbered starting 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 session manually:

- 1 Begin a remote control or online session.
- 2 Press the remote hotkey.

Depending on the type of session, the Session Options or Terminal Options menu appears.

3 Choose Recording On....

The Select Path for Recording File form appears.

4 Type a new pathname or accept the default pathname, then press Enter. Do not type the filename at this step.

The Available Files menu appears.

5 Do one of the following:

- Choose the name of the .RCD file to append the recording to.
- Press Insert to create a new file for this recording.

The Enter File Name form appears. Type the name of the file, then press Enter.

A message informs you that the recording has started.

6 Press Esc to return to the session.

NOTE: After you choose the Recording On command, recording begins and the menu command toggles to Recording Off.

To stop recording a session:

1 Press the remote hotkey.

Depending on the type of session, the Session Options or Terminal Options menu appears.

2 Choose Recording Off.

A message informs you that the recording has stopped.

3 Press Esc to return to the session.

NOTE: Recording automatically stops when you end a session.

To enable automatic session recording:

1 Choose either Call A pcANYWHERE Host... or Call An Online Service... from the pcANYWHERE Main menu.

The Call A pcANYWHERE Host or the Call An Online Service menu appears, respectively.

2 Choose View/Modify List Of Hosts... or View/Modify List Of Services....

The Select Host For Connection or the Select Online Service menu appears, respectively.

- 3 Choose a session configuration.

The form for that session configuration appears.

- 4 Choose Data Recording for a remote control session configuration or Recording for an online session configuration.

The Recording Options menu appears.

- 5 Choose Select Recording File... to specify a recording file for all sessions using this session configuration.

The Select Path for Recording File form appears.

- 6 Type a new pathname or accept the default pathname, then press Enter. Do not type the filename at this step.

The Available Files menu appears.

- 7 Do one of the following.

- a Choose the name of the .RCD file to append the recording to.

- b Press Insert to create a new file.

The Enter File Name form appears. Type the name of the file, then press Enter.

- 8 When the Recording Options menu reappears, choose Initially On to start recording the session from the time of connection.

NOTE: When you begin a session, pcANYWHERE automatically begins recording and saves the session to the specified file. You can stop the recording manually when you want to. Otherwise, the recording automatically stops when the session ends.

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 are numbered in the order of their occurrence.

While you replay a session, you can do any of the following:

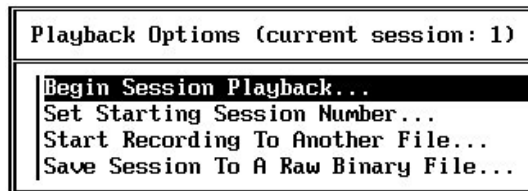
- Copy a session or a partial session to a new file.
- Save a recorded session as a raw binary file so you can process the text data in an application that requires binary files.

- Save the currently displayed screen from a recorded session as a screen shot.

To play back recorded sessions:

- 1 Choose Utilities... from the pcANYWHERE Main menu.
The Utilities menu appears.
- 2 Choose Playback Sessions/Screens....
The Playback Options menu appears.
- 3 Choose Play Back Recorded Sessions....
The Select Path Containing Recording Files form appears.
- 4 Type a new pathname or accept the default pathname, then press Enter. Do not type the filename at this step.
The Available Files menu appears.
- 5 Choose the .RCD file you want to review.
A new Playback Options menu appears (Figure 9-6) along with a message telling you what keystrokes can be used during the playback and the number of recorded sessions in the file you have chosen. From now on, the number of the current session appears in the title of the Playback Options menu.

Figure 9-6 You can play back one or more sessions.



- 6 To bypass earlier sessions also in the .RCD file:
 - a Choose Set Starting Session Number....
The range of sessions, for example, 1-7, appears.
 - b Type the number of the session you want to replay, then press Enter.
- 7 Choose Begin Session Playback... from the Playback Options menu.
The recorded session plays immediately.

NOTE: Use UpArrow or DownArrow to increase or decrease the playback speed. Press a number from 0 to 9 to select a speed (0 is the fastest). Press the spacebar to stop the replay until the next key is pressed. Press Esc to display the Playback Options menu.

- 8 When the session replay completes, do one of the following:
 - Press Esc to return to the Playback Options menu.
 - Press Enter to see the next session.

To copy one or more recorded sessions to another file:

- 1 Follow steps 1-5 in the previous procedure to get to the Playback Options menu.
- 2 To indicate the session you want to copy:
 - a Choose Set Starting Session Number... from the Playback Options menu.

The range for the sessions, for example, 1-7, appears.
 - b Type the number of the session you want to copy, then press Enter.
- 3 Choose Start Recording To Another File... from the Playback Options menu.

The Start Recording menu appears.
- 4 Choose Yes.

The Select Path For Recording File appears.
- 5 Type a new pathname or accept the default pathname, then press Enter. Do not type the filename at this step.

The Available Files menu appears.
- 6 Do one of the following:
 - Choose the .RCD file to append the session to.
 - Press Insert to create a new file for this session.

The Enter File Name form appears. Type the name of the file, then press Enter.
- 7 When the Playback Options menu reappears, choose Begin Session Playback....

The session to be copied plays immediately.
- 8 Do one of the following:
 - Copy a partial session. Press Esc to stop the recording before it completes playing. This copies a partial session, and the Playback

Options menu reappears. Choose Stop Recording, then Yes. The rest of the session replays. When it is complete, press Esc to return to the Playback Options menu.

- Copy an entire session. When the recording completes, press Esc to return to the Playback Options menu.
 - Copy successive sessions. When the recording completes, press Enter to copy the next session as well. Press Esc to return to the Playback Options menu when you have all the successive sessions you want to copy.
- 9 Repeat steps 2 through 8 if you want to copy additional sessions.
 - 10 Choose Quit.

To save a recorded session to a raw binary file:

- 1 Follow steps 1-5 in the “To play back recorded sessions” procedure to get to the Playback Options menu.
- 2 Choose Save Session to a Raw Binary File....
The range of sessions, for example, 1-7, appears.
- 3 Type a number, then press Enter.
The Select Path for Raw Binary Recording File form appears.
- 4 Type a new pathname or accept the default pathname, then press Enter. Do not type the filename at this step.
The Available Files menu appears.
- 5 Do one of the following:
 - Choose the .RAW file to append the data to.
 - Press Insert to create a new file for the data.
The Enter File Name form appears. Type the name of the file, then press Enter.
The session is converted to raw binary data and the Playback Options menu reappears.
- 6 Press Esc to return to a menu you want to use.

To save a screen from a recorded session:

- 1 Begin playing a recorded session.
- 2 Press Esc when the screen you want to save appears on the screen.
- 3 Choose Save Screen... from the Playback Options menu.
The Select Path For Save Screen File form appears.

- 4 Type a new pathname or accept the default pathname, then press Enter. Do not type the filename at this step.

The Available Files menu appears.

- 5 Do one of the following:
 - Choose the name of the .SCN file to append the screen to.
 - Press Insert to create a new file.

The Enter File Name form appears. Type the name of the file, then press Enter.

A message informs you that the screen has been saved.

- 6 Press Esc to continue replaying the recorded session.
- 7 Repeat steps 2 through 6 if you want to save more screens from this session.
- 8 Press Esc to return to a menu you want to use.

Saving Screen Shots

When making a recording of the session will capture a great deal of unnecessary extra information, you can save a screen shot or a series of screen shots that are representative of the session. Capturing the contents of the screen during a session is like taking a snapshot with a camera. Norton pcANYWHERE for DOS stores them in a file with an .SCN extension. In the recorded file, screen shots are stored in the order they were taken and numbered starting with 1.

To save a screen shot from a recorded session, see “Playing Back Recorded Sessions,” the previous section.

To save a screen shot:

- 1 Begin a remote control or online session.
- 2 Press the remote hotkey.

Depending on the type of session, the Session Options or Terminal Options menu appears.
- 3 Choose Save Screen....

The Select Path For Save Screen File form appears.
- 4 Type a new pathname or accept the default pathname, then press Enter. Do not type the filename at this step.

The Available Files menu appears.

- 5 Do one of the following:
 - Choose the name of the .SCN file to append the screen shot to.
 - Press Insert to create a new file.
The Enter File Name form appears. Type the name of the file, then press Enter.
A message informs you that the screen shot has been saved.
- 6 Press Esc to return to the session.
- 7 Repeat steps 2 through 5 if you want to save an additional screen shot.

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 are numbered in the order in which they were 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 Utilities... from the pcANYWHERE Main menu.
The Utilities menu appears.
- 2 Choose Playback Sessions/Screens....
The Playback Options menu appears.
- 3 Choose Play Back Saved Screens....
The Select Path Containing Screen Files form appears.
- 4 Type a new pathname or accept the default pathname, then press Enter. Do not type the filename at this step.
The Available Files menu appears.
- 5 Choose the name of the .SCN file that you want to review.
A new Playback Options menu appears along with a message telling you what keystrokes can be used during the playback and the number of screen shots in the file you have chosen. From now on, the number

of the current screen shot appears in the title of the Playback Options menu.

- 6 To bypass earlier screen shots also in the .SCN file:
 - a Choose Set Starting Screen Number... from the Playback Options menu.
The range of screen shots, for example, 1-4, appears.
 - b Type the number of the screen shot you want to replay, then press Enter.
- 7 Choose Begin Screen Playback... from the Playback Options menu.
The screen shot appears.

NOTE: Use UpArrow and DownArrow to review previous or subsequent screen shots in the file.

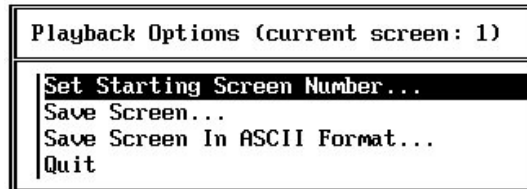
- 8 Press Esc to return to the Playback Options menu.

To copy a screen shot to an .SCN or .TXT file:

- 1 Follow steps 1-7 in the previous procedure to display the screen shot you want to copy.
- 2 Press Esc.

The Playback Options menu appears (Figure 9-7).

Figure 9-7 This Playback Options menu allows you to copy a screen shot or save it as ASCII text.



- 3 Choose Save Screen... or Save Screen in ASCII Format...
The Select Path For Save Screen File form or the Select Path for ASCII Screen File form appears.
- 4 Type a new pathname or accept the default pathname, then press Enter. Do not type the filename at this step.
The Available Files menu appears.

- 5 Do one of the following:
 - Choose the name of the .SCN or .TXT file to append the screen shot to.
 - Press Insert to create a new file for this recording.
The Enter File Name form appears. Type the name of the file, then press Enter.
A message informs you that the screen shot has been saved.
- 6 Press Esc to return to a menu you want to use.

Logging Remote Control and Online Sessions

You can log information about remote control and online sessions for curiosity, historical, billing, or security purposes. For example, you may want to know just how often you call a particular host PC or online service.

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 *AW.RL6* (or *AWuserid.RL6* on a network). It is in the directory where Norton pcANYWHERE is installed.

Similarly, the caller information on the host PC determines whether or not the session is logged on the host. The host log file is *AW.HL6* (or *AWuserid.HL6* on a network).

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 information is preserved in case you need to reference it at a later date. You can also delete log information without archiving it. The remote log history file is *AW.RH6* or *AWuserid.RH6*, which stores data archived from the remote log file, and the host log history file is *AW.HH6* or *AWuserid.HH6*, which stores data archived from the host log file.

To log sessions on the remote PC:

- 1 Choose either Call A pcANYWHERE Host... or Call An Online Service... from the pcANYWHERE Main menu.
The Call A pcANYWHERE Host menu or the Call An Online Service menu appears, depending on your choice.
- 2 Choose View/Modify List of Hosts... or View/Modify List of Services....

The Select Host for Connection menu or the Select Online Service menu appears, respectively.

- 3 Choose a session configuration.
The form for that configuration appears.
- 4 Choose Log Session.
The Log Session menu appears.
- 5 Choose Yes.
- 6 Press Esc to return to the Select Host for Connection menu or the Select Online Service menu.
- 7 Repeat steps 3 through 6 for any other session entries about which you want to log information.
- 8 Press Esc until you return to a menu you want to use.

To log sessions with specific remote users on the host PC:

- 1 Choose Be A Host... from the pcANYWHERE Main menu.
The Be A pcANYWHERE Host menu appears.
- 2 Choose Caller Information....
The Caller Names menu appears.
- 3 Choose a caller.
The Caller Information form appears.
- 4 Choose Log Calls From This Caller.
The Log Calls From This Caller menu appears.
- 5 Choose Yes.
- 6 Press Esc to return to the Caller Names menu.
- 7 Repeat steps 3 through 6 for any other callers you want to log information about.
- 8 Press Esc until you return to a menu you want to use.

To log all sessions on the host PC using the default caller information form:

- 1 Choose Be A Host... or from the pcANYWHERE Main menu.
The Be A Host menu appears.
- 2 Choose Host Preferences....
The Host Preferences menu appears.

- 3 Choose Security....
The Host Security Preference form appears.
- 4 Choose Default Caller Entry.
The default caller information form appears.
- 5 Choose Log Calls From This Caller.
The Log Calls From This Caller menu appears.
- 6 Choose Yes.
- 7 Press Esc until you return to a menu you want to use.

To log unsuccessful connection attempts on the host PC:

- 1 Choose Be A Host... or from the pcANYWHERE Main menu.
The Be A Host menu appears.
- 2 Choose Host Preferences....
The Host Preferences menu appears.
- 3 Choose Security....
The Host Security Preference form appears.
- 4 Choose Log Failed Connections.
The Log Failed Connection Attempts appears.
- 5 Choose Yes.
- 6 Press Esc until you return to a menu you want to use.

Creating Log Reports

From the information stored in log files, you can create any of the following reports. The reports can be displayed on screen or written to a text file. You can print the text file later.

- Activity log report. This is a chronological listing of connections. Each record in the log becomes a line in the report. Each field in the record becomes a column in the report. The columns are:
 - Date. The date of the session (shown in mm-dd-yy format).
 - Time On. The time the session started (shown in a 24-hour clock format).
 - Time Off. The time the session ended.
 - Time Online. The length of the session in hours and minutes.
 - Comment. The user is prompted for a comment at the end of the session.

- 3 Choose Activity Log..., Billing Detail..., or Billing Summary...
The parameters form appears for the type of report you chose (Figure 9-11).

Figure 9-11 The parameters determine what data appears in the report.

Parameters For Activity Report	
Log file to process:	Host Log File
Start date:	EARLIEST
End date:	02-27-1994
Report destination:	Screen
Report format option:	Formatted Report Output

- 4 To set each parameter, see the corresponding procedure in one of the next few sections.
- 5 Press Esc to exit the parameters form.
The Process Report/Action menu appears.
- 6 Choose Yes (the default).
The report is displayed on your screen, written to a file, or printed.
- 7 Press Esc to return to a menu you want to use.

Choosing the Log File

You can create reports for any of your log files.

To choose a log file:

- 1 Choose Log File To Process.
The Log File To Process menu appears.
- 2 Choose one of the following:
 - Host Log File (the default)
 - Remote Log File
 - Host Log History File
 - Remote Log History File

Choosing the Date Range

You choose the date range for the records to be used in the report. For example, you may want to see all the records for the month of July.

To change the date range:

- 1 Select Start Date.
- 2 Type a date, then press Enter.

Use the format `mm-dd-yy`. To separate the parts of the date, use a hyphen (-), slash (/), backslash (\), or period (.). If the number representing the month or day is under 10, you can enter a single digit—no leading 0 is necessary. If you leave the setting blank, Norton pcANYWHERE resets it to EARLIEST, the earliest date in the specified log file and the default setting for this parameter.

- 3 Select End Date.
- 4 Type a date, then press Enter.
The default is the current date.

Displaying or Printing the Report

You specify a destination for the report. It can be displayed on the screen, stored in a text file, or printed with 80 or 132 columns.

To specify a destination:

- 1 Choose Report Destination.

The Destination For Output menu appears.

- 2 Choose one of the following:

- Screen. The report output appears on your screen. You can use UpArrow and DownArrow keys to scroll.
- Disk File. The report output is an ASCII text file.

The names of the files are AW.ACT for activity reports, AW.DET for billing detail reports, and AW.SUM for billing summary reports.

CAUTION: Existing files with the same name in the current directory will be overwritten and lost when you generate this report.

- Printer (80-column). Report output is formatted for a printer that prints 80 characters on a line. The 80-column report does not include the Project and Comment columns.
- Printer (132-column). Report output is formatted for a printer that prints 132 characters on a line. The report includes the Project and Comment columns.

Choosing a Report Format

The format you choose determines how the report looks in your disk file or printout. When you view a report on the screen, it is always formatted with headings and columns.

To choose a format:

- 1 Choose Report Format Option.
The Format For Output menu appears.
- 2 Choose one of the following:
 - Formatted Report Output. This format resembles the screen reports shown in Figures 9-8 and 9-9. The only differences are that page numbers are included and that the columns are adjusted for the printer (if you specified a printer as a destination).
 - Export Log Data With Delimiters. This option formats the data for use in a database application or other program that requires delimiters between fields. No headings, titles, or lines are included. Each item is enclosed in double quotation marks (") and separated from the next item by a comma (.). Month, date, and year are separated by slashes (/). Each record is followed by a carriage return. No spaces are used, except within the text items. The Comment field is never included in this report. Here is a brief example showing an activity report record without a project name:
 - "5/15/90", "15:08", "15:28", "00:20", "John Doe"
 - Export Log Data In Fixed Format. This option formats the data in columns, using no title, column headings, or lines. You can edit the data using almost any word processor. When this report is printed in 80 columns, the Comment field is included.

Deleting and Archiving Logged Information

When a log file becomes large, you may want to delete or archive some of the older data in it.

To delete data from a log file:

- 1 Choose Utilities... from the pcANYWHERE Main menu.
The Utilities menu appears.
- 2 Choose Activity Log Processing...
The Log Processing Options menu appears.

- 3 Choose Delete Old Log Data...
The Parameters For Deleting Old Log Data form appears.
- 4 You can do either or both of the following:
 - Choose the log file to be used in the report.
 - Change the date range for the records to be used in the report.
For example, you may want to delete all the records for the month of July.For details, see the corresponding procedures in “Creating Log Reports,” the previous section.
- 5 Press Esc to exit the Parameters For Deleting Old Log Data form.
The Process Report/Action menu appears.
- 6 Choose Yes (the default).
The specified data is deleted from the log file.
- 7 Press Esc to return to a menu you want to use.

To archive data from a log file:

- 1 Choose Utilities... from the pcANYWHERE Main menu.
The Utilities menu appears.
- 2 Choose Activity Log Processing...
The Log Processing Options menu appears.
- 3 Choose Move Old Data To History File...
The Parameters For Moving Old Data To History File form appears.
- 4 You can specify either or both of the following:
 - Choose the log file to be used in the report.
 - Change the date range for the records to be used in the report.
For example, you may want to archive all the records for the month of July.For details, see the corresponding procedures in “Creating Log Reports,” the previous section.
- 5 Press Esc to exit the parameters form.
The Process Report/Action menu appears.
- 6 Choose Yes (the default).
The report is displayed on your screen, written to a file, or printed.
- 7 Press Esc to return to a menu you want to use.

Technical Information



This appendix covers technical information about serial port connections, one of the ways you can connect your PC to another computer. Its purpose is to help you understand the options in a serial hardware configuration and select their settings. It discusses:

- 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

The Role of the PC

Your PC relies on an electronic component known as the CPU, or *central processing unit*, to control all of 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 prior to 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. The problem with this

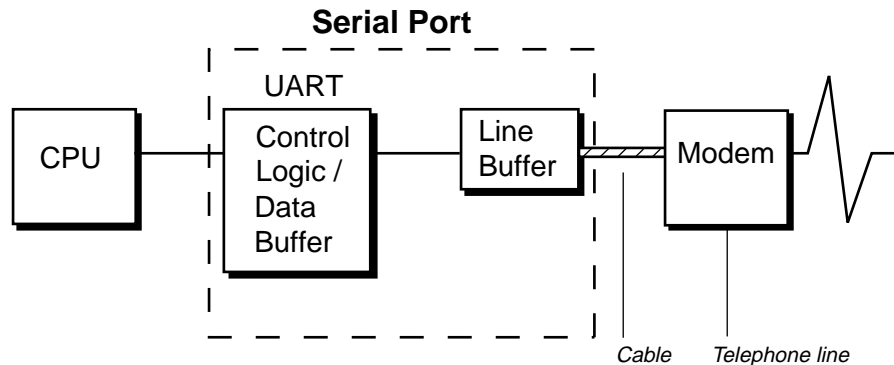
arrangement is that *two ports sharing one IRQ line cannot be active at the same time*. If both ports send an interrupt request to the CPU at the same time, the resulting confusion can force you to reboot your computer. For example, if your mouse is on COM1 and your modem is on COM3, moving your mouse can interfere with your modem.

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 can transfer data at a maximum speed of 9600 bps (bits per second). It was the standard UART in the original IBM XT, but some IBM-compatible ATs contain 8250 UARTs. It can store one character in its buffer.

The 16450 UART can transfer data at a maximum speed of 38,400 bps. It also stores one character at a time and is a standard on most 286 (AT), 386 and 486 PCs.

The 16550A UART can transfer data at a maximum speed of 115,200 bps. It can store 16 characters in its data buffer. Norton pcANYWHERE automatically detects and enables the buffering capabilities of this UART.

The Role of the Modem

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*.

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), while 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*.

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 2400 and 9600 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 it is sent. 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 MNP/5 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 product line. Additional commands and enhancements are usually 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. Do not worry if your modem does not have switches for all of 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
FUNCTION	SWITCH SETTING

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 will 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, via 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, a cable that tricks two computers into thinking that they are connected via modems by crossing two or more of the serial lines, often transfers data at rates of 19,200 bps or greater, depending on the speed of the PCs and the capabilities of the serial port. 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

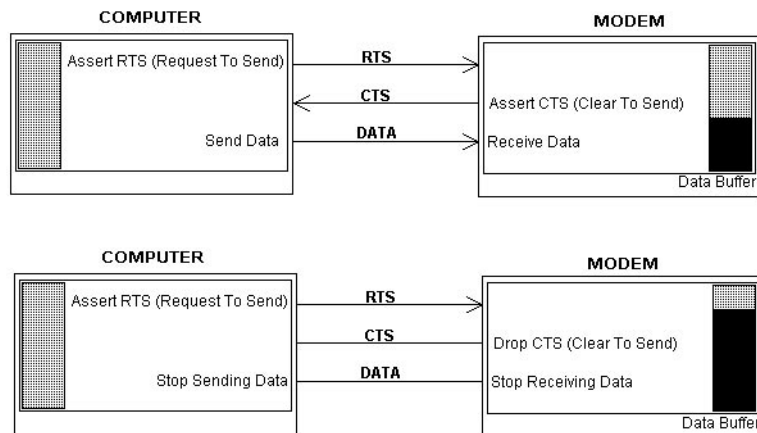
To avoid losing any data, *flow control* starts and stops data transmission. The modem and CPU signal each other by sending signals over the RTS and CTS lines of the RS-232 serial interface or special characters embedded in the data stream. For example, the modem may want to halt data transmission because 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.

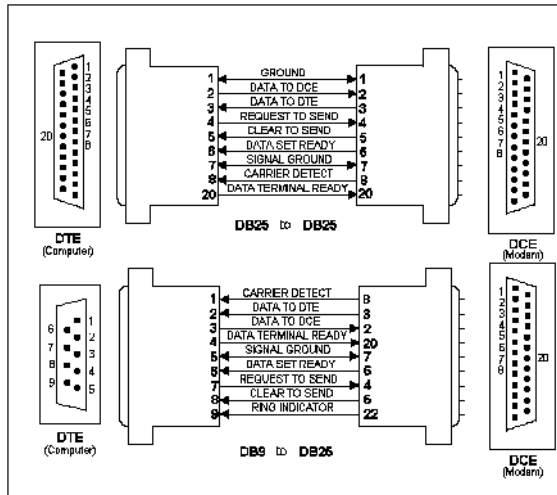
Figure A-2 Hardware flow control stops data flow to avoid overflowing the data buffer.



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 was written to cover a lot more than just modem connections, a “compatible” cable may not always implement all of 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.

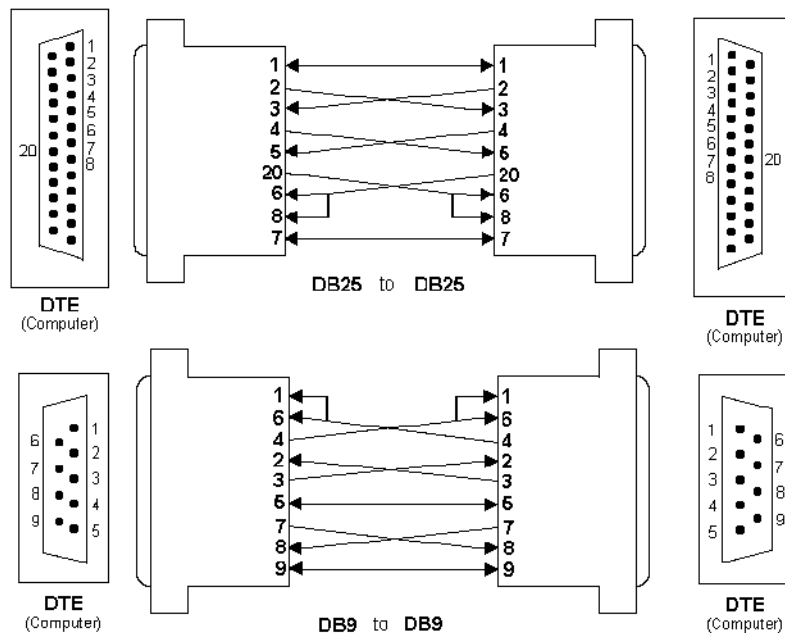
CAUTION: Often you may find yourself with a 25-pin cable, but your computer has only a 9-pin port. Adapters are available for 25-to-9 pin and 9-to-25 pin and will pass the correct signals.

Null Modem Cable

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

takes the place of 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 own 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 have 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:

Method #1: Modems with Automatic Leased Line Mode

If both modems have the capability of performing an automatic leased line connection (check the &L parameter in the modem’s documentation), then placing the modems in this mode results in them going offhook as soon as they are turned on. Once offhook, they will 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

Table A-3 Method #1 Hardware Configurations (*continued*)

	Host PC	Remote PC
Flow Control:	RTS/CTS	RTS/CTS
Connection Started By:	Receive 2 <CR>'s	Always Connected
Connection Ended By:	Always Connected or DCD Host PC	Always Connected or DCD Remote PC
Device:	(the port attached to the modem.)	(the port attached to the modem.)
Modem:	None	None

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 method one (described above) must be used.

Testing Leased Lines:

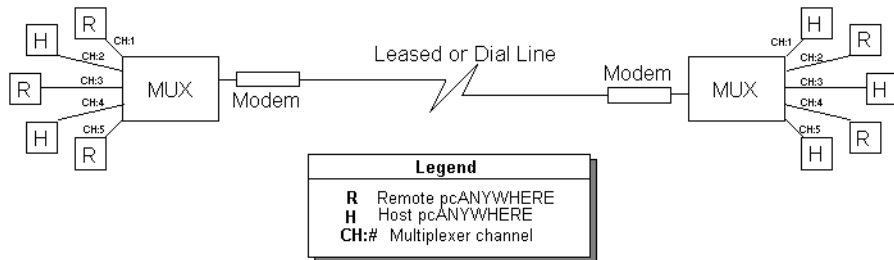
To make sure that your leased line is operating properly, replace the modems with normal telephones. Have a person on each end pick up the telephone and attempt a conversation. If both people can communicate, the modem connection should work correctly.

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 of 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 demultiplexes 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 it were 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.

The remote-to-remote test can be used to determine if data can flow across the channel correctly. To perform a remote-to-remote test over a serial device, each user creates a hardware configuration, chooses Quick Connect from the Call A pcANYWHERE Host menu, chooses Direct Connect/Terminal Mode, and types characters. If each can see characters typed at the other PC, the configurations and so forth are working. Another way to perform a remote-to-remote test is to have each user select Connect To An Online Service... from the Call An Online Service menu on each PC. One calls and the other waits for a call.

The options in Table A-4 depend on the Multiplexer used.

Table A-4 Norton pcANYWHERE Configurations:

	Remote PC	Host PC
Modem:	None	None
*Date rate:	(set to speed of MUX)	(set to speed of MUX)
*Parity:	None	None
*Flow control:	RTS/CTS	RTS/CTS

Table A-4 Norton pcANYWHERE Configurations: *(continued)*

	Remote PC	Host PC
Conn. started by:	Carrier Detect (DCD)	Receive 2 CR's
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.

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 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 which 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

Options in 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, remote control session always use “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 will 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.

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 options not explained in this section.

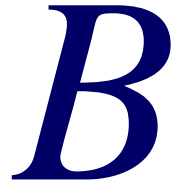
Miscellaneous Options

The remaining hardware configuration options for modems:

- Indicate the types of signal your system will use 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 also find them in the Glossary.

- Allow you to control hardware settings for serial communications. DTR State and RTS State refer to the Data Terminal Ready signal (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). These options are automatically set by Norton pcANYWHERE 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.)

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

PC KEY	ADM3A KEY
Down	Down
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

PC KEY	DG KEY
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
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

PC KEY	DG KEY
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
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

PC KEY	DG KEY
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	HAZ KEY
Home	Home Cursor
Up	Up
Left	Left
Right	Right
Down	Down
Gray-Home	Home Cursor
Gray-Up	Up
Gray-Left	Left
Gray-Right	Right
Gray-Down	Down

IBM 3101

PC KEY	IBM3101 KEY
F1	F1
F2	F2
F3	F3
F4	F4
F5	F5
F6	F6
F7	F7
F8	F8
Home	Home Cursor
Up	Up

PC KEY	IBM3101 KEY
Left	Left
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

Teletype 912/920

PC KEY	TVI912/920 KEY
Alt+F n	Funct+n
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
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

PC KEY	TVI912/920 KEY
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
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
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

PC KEY	TVI925 KEY
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
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
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)

PC KEY	VT100/220 KEY
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
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

PC KEY	VT100/220 KEY
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

PC KEY	VT52KEY
Pad 1	Pad 1
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
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

PC KEY	WYSE50 KEY
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
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

PC KEY	WYSE50 KEY
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

PC KEY	3270 Key
Shift+F5	PF15
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

PC KEY	3270 Key
Pad *	PF23
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 multiuser 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 8, "Online Sessions." 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 these extended ASCII character set. Microsoft refers to the 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	±	225	β
2	⊗	34	"	66	B	98	b	130	é	162	ó	194	⌈	226	Γ
3	♥	35	#	67	C	99	c	131	â	163	ú	195	⌋	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	â	166	œ	198	‡	230	μ
7	•	39	'	71	G	103	g	135	ç	167	œ	199		231	τ
8	□	40	(72	H	104	h	136	ê	168	¿	200	⌌	232	̄
9	○	41)	73	I	105	i	137	ë	169	ƒ	201	⌍	233	θ
10	⊠	42	*	74	J	106	j	138	è	170	ƒ	202	⌎	234	Ω
11	♂	43	+	75	K	107	k	139	ï	171	½	203	⌏	235	δ
12	♀	44	,	76	L	108	l	140	î	172	¾	204	⌐	236	ω
13	ℙ	45	-	77	M	109	m	141	ì	173	¡	205	=	237	ø
14	ℚ	46	.	78	N	110	n	142	ñ	174	«	206	⌑	238	€
15	⊛	47	/	79	O	111	o	143	ñ	175	»	207	±	239	π
16	▶	48	0	80	P	112	p	144	é	176	≡	208	⌒	240	≡
17	◀	49	1	81	Q	113	q	145	æ	177	≡	209	⌓	241	±
18	‡	50	2	82	R	114	r	146	ff	178	≡	210	⌔	242	≥
19	‡	51	3	83	S	115	s	147	ô	179		211	⌕	243	≤
20	¶	52	4	84	T	116	t	148	ö	180	†	212	⌖	244	ƒ
21	§	53	5	85	U	117	u	149	ð	181	‡	213	⌗	245	J
22	≠	54	6	86	V	118	v	150	û	182		214	⌘	246	÷
23	±	55	7	87	W	119	w	151	ù	183	⌐	215	⌙	247	∞
24	↑	56	8	88	X	120	x	152	ÿ	184	‡	216	⌚	248	o
25	↓	57	9	89	Y	121	y	153	ö	185		217	⌛	249	·
26	→	58	:	90	Z	122	z	154	Û	186		218	⌜	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	⌟	221	■	253	z
30	▲	62	>	94	^	126	~	158	℞	190	⌠	222	■	254	■
31	▼	63	?	95	_	127	△	159	ƒ	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 chapter can help you troubleshoot your remote control sessions. It covers:

- Error messages and their explanations
- Common problems and their possible solutions

Error Messages

Table C-1 lists alphabetically the messages Norton pcANYWHERE displays to alert you to a problem or condition. Each message is followed by one or more solutions or explanations. Italics are used to indicate words or values that vary according to the names and settings in your copy of Norton pcANYWHERE.

NOTE: Please check the README.TXT file for any additions or corrections to the messages.

Table C-1 Common Error Messages

Error Message	Explanation
Access denied	Because of drive security settings on the host PC, this drive is not accessible to the remote user.
Access violation opening <i>filename</i>	Either DOS or your network operating system has reported that you cannot read a file you have attempted to transfer. This can happen if the file is in use by someone else or if you do not have the necessary network privileges to open the file.
An incompatible version of pcANYWHERE is already active.	Cancel the operation of the older version, then try again.
An incompatible version of the gateway software is already active.	Deactivate the older version of the software, then restart the correct version of Norton pcANYWHERE and reactivate the gateway.

Table C-1 Common Error Messages *(continued)*

Error Message	Explanation
AWSEND could not disable Host	The file transfer program, AWSEND, was started, but the session was lost before the directory information could be exchanged.
AWSEND could not enable Host	A file transfer session with AWSEND was finishing up, but the session was lost before AWSEND was done.
Busy	The telephone number of the other system is busy. If your session configuration specifies redial attempts, Norton pcANYWHERE will try again. For more information about redialing, see Chapter 3, "Hardware Configurations."
Cannot create HOST file	There may not be enough space on the host disk for the file you want to transfer.
Cannot create REMOTE file	There may not be enough room on the remote disk for the file you want to transfer to it.
Cannot make new directory.	The directory may already exist, or there may be a file with the same name as the requested directory name. Use a different directory name.
Cannot open HOST file	DOS or the network operating system cannot open the file. You may not have the right to access it or the file may be in use.
Cannot open REMOTE file	DOS or the network operating system cannot open the file. You may not have the right to access it or the file may be in use.
Cannot read the file C:\COMMAND.COM. Insert correct disk and strike any key.	You probably do not have access to the fixed drive where COMMAND.COM resides. The host PC can deny access to drives. Check the Drive Security settings. See "Host Features Preferences" in Chapter 6, "Caller Information and Host Preferences." You must have at least read-only rights to COMMAND.COM. This is an error reported by DOS.

Table C-1 Common Error Messages (*continued*)

Error Message	Explanation
Cannot remove directory.	There are probably files in the directory you are attempting to remove.
Cannot use RTS/CTS flow control when connection detection set to CTS.	When the Connection Started By option in the hardware configuration is set to CTS, you cannot also set the Flow Control option to RTS/CTS.
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.
CRC error on <i>drive name</i> .	DOS has detected a serious disk error, called a CRC error, on a file on the specified drive. It usually indicates defective disk media.
Disk full.	You cannot write the file to the specified disk drive, because it is full. Exit to DOS and make room on the disk before retrying the operation.
Disk I/O error.	The disk does not seem to be working properly. Make sure the correct drive name is specified.
DOS is busy, try again later.	An attempt to cancel Norton pcANYWHERE host operation was aborted because DOS was busy doing something else. Try the operation later.
DOS is currently busy on the host PC. Only the master password can be accepted at this time.	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. If this happens, the host TSR cannot read the caller information files and, therefore, cannot give you access to the host. If you don't have the master password, try the host again later.
Error: Ambiguous file names are not allowed.	You may not use wildcards (* and ?) in a filename.

Table C-1 Common Error Messages (*continued*)

Error Message	Explanation
Error: Cannot load configuration.	Your configuration file may have been erased or physically damaged. Contact your network administrator, if you have one. You may have to restart Norton pcANYWHERE and re-enter the configuration information.
Error: Cannot save graphics screens to ASCII data files.	Only nongraphics recorded sessions and screens can be saved as ASCII files.
Error in message file.	This error indicates a serious problem with the message database file.
Error in modem script.	This generally indicates a failure in the message file.
Error - not enough memory to execute the function.	A function you have requested, such as file transfer, cannot be executed because there is not enough available memory. Make sure you are not running software that is taking up RAM memory needed by Norton pcANYWHERE. You may recover some memory by exiting to DOS and restarting AW.
Error reading configuration or program file.	The host PC cannot read a configuration or program file. This problem may be due to a physical problem on the disk. See "Error reading the configuration file" below.
Error reading HOST file.	The host file may be on a defective portion of the disk.
Error reading the configuration file	Your configuration file for this operation may have been erased, or moved to a directory other than the directory specified during installation. Contact your network administrator, if Norton pcANYWHERE is installed on your network. Otherwise, move your configuration files to the location where Norton pcANYWHERE expects to find them, or reenter the configuration information.

Table C-1 Common Error Messages (*continued*)

Error Message	Explanation
Error: Source file not found.	Exit to DOS, if necessary, and check the source file name and location.
File already exists.	You have specified the name of an existing file. Use a different filename or path.
File not found.	This file does not exist on the specified path.
General failure on <i>drive name</i> .	The drive is not turned on or is not functional. It is also possible that the disk is not formatted. This is an error reported by DOS.
General failure reading <i>drive name</i> .	You probably do not have access to the specified floppy drive. The host PC can deny access to drives. Check the Drive Security settings. See "Host Features Preferences," in Chapter 6, "Caller Information and Host Preferences." This is an error reported by DOS.
General network error.	This message may be caused by a variety of different problems that can occur on the network you are using. Contact your network administrator. This error is reported to Norton pcANYWHERE by DOS and your network software.
Host user is busy.	The host user is performing some activity such as file transfer or directing print output using the Host Session Options menu. You cannot use the host PC until this activity is complete.
Inactivity timeout expired.	The session was ended because the amount of time specified for an inactivity timeout has passed with no activity over the telephone line or direct cable.
Incompatible version already running.	An older version of pcANYWHERE is already running. Cancel it and try again.
Incorrect date format.	Valid date entry formats use one or two digits for month, day, and year, separated by slashes (/), hyphens (-), or dots (.).

Table C-1 Common Error Messages *(continued)*

Error Message	Explanation
Incorrect MSG file...	You do not have the correct .MSG file. Try reinstalling Norton pcANYWHERE. If that doesn't work, contact your network administrator or the dealer who sold you Norton pcANYWHERE.
Incorrect password	You have not entered the correct master password. You need the master password to perform the operation you have selected. If you have made a typographical error, press Esc and try the operation again. Otherwise, contact your network administrator or the licensee of this copy of Norton pcANYWHERE.
In order to run pcANYWHERE in a DESQview window you need DESQview 2.26 or later.	You must use a later version of DESQview.
Internal communication error.	A serious software error was detected. You may want to write down the circumstances that led up to the problem.
Internal error.	A serious software error was detected. You may want to write down the circumstances that led up to the problem.
Internal window error.	A serious software error was detected. You may want to write down the circumstances that led up to the problem.
Invalid filename.	Enter a correct DOS filename, using letters and numbers. DOS does not accept the following characters as part of filenames: ! @ # \$ % ^ & * ()
Invalid file name. Do not include an extension.	For your current operation, Norton pcANYWHERE adds the extension for you. Use a DOS filename of up to eight characters only.

Table C-1 Common Error Messages *(continued)*

Error Message	Explanation
Invalid password. Please try again.	<p>You have entered the wrong password for this host, but you are permitted at least one more try. You must enter either the password that the host user has designated for access to the host PC or the host master password.</p> <p>If you typed in the password, you may have made a typing error. Try again.</p> <p>If the password was stored in the session configuration for this host, try typing the correct password in manually. If that doesn't work, the host does not have a caller information configuration with the password you are entering. If you don't know the right password, press the hotkey (initially Ctrl+RightShift) to end the session and check with the host user or network administrator, if necessary.</p>
Invalid serial number.	<p>Contact the dealer where you bought Norton pcANYWHERE, or see your network administrator.</p>
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, or Norton pcANYWHERE has entered it for you via the session configuration. The host is not allowing you another password attempt.</p> <p>If you think you have made a typographical error, press the hotkey (initially Ctrl+RightShift) to end the session then try again.</p> <p>The password in the session configuration for this host may be incorrect. Check with the host user or network administrator, if necessary, to correct the password.</p>

Table C-1 Common Error Messages (*continued*)

Error Message	Explanation
Month, day and/or year out of range.	The numbers entered for month, day, and year do not represent a valid date.
Name already in use.	This configuration is already defined. Type in a different name.
Network driver not found.	If your connection specifies NetWare IPX, you must have the NetWare network drivers loaded before Norton pcANYWHERE can be used for a session. If your configuration specifies NetBIOS, the network software must be loaded first. Contact your network administrator if you need help.
The following network driver must be loaded in order to use the selected device type: <i>driver name</i>	If your connection specifies NetWare IPX, you must have the NetWare network drivers loaded before Norton pcANYWHERE can be used for a session. If your configuration specifies NetBIOS, the network software must be loaded first. Contact your network administrator if you need help.
Network error.	The network specified in the hardware configuration is not working properly. Contact the network administrator.
Network request not accepted.	The host PC was issued a DOS request at a time that it could not process it. This error may be generated when you are using drive mapping.
No connection.	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.
No dial tone.	Norton pcANYWHERE attempted to use the telephone line, but there was no dial tone. The telephone line may be disconnected from the jack or otherwise cut off.
No log data found within the given date range.	Make sure that the type of log and dates you entered are correct, or check if the log data you seek has been moved to a history file.

Table C-1 Common Error Messages (*continued*)

Error Message	Explanation
No modem response.	<p>Your modem is not responding 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 use. <p>Appendix A, “Technical Information,” gives information on modems or cabling. For other problems, see your modem or system manual, or contact your network administrator.</p>
No paper.	The printer reports that there is no paper in it.
No record files found in the current directory.	Try accessing another directory.
No screen files found in the current directory.	Try accessing another directory.
Not available: <i>computer name</i> .	This PC is already in use or not ready to start a session.
Not ready <i>drive or device name</i> .	The drive you specified has no disk in it, or the drive door is not closed, or the drive is not turned on.
Operator abort.	This message may be followed by “Please wait” and “Press any key to continue.” The remote control session was ended before both parties were online for the session, probably because you pressed Esc. To try the session again, you must restart Norton pcANYWHERE.

Table C-1 Common Error Messages (*continued*)

Error Message	Explanation
Procedure name already in use.	Two procedures cannot have the same name. Enter a new name, or rename the other procedure.
Program not installed correctly. Please reinstall or contact your dealer.	Try reinstalling first. If any files are missing from your installation of Norton pcANYWHERE, the installation program will tell you.
Read fault on <i>drive name</i> .	A physical defect on the disk drive makes it unreadable. This error was reported to Norton pcANYWHERE by DOS.
Remote machine not listening.	The host PC issued a drive mapping request to the remote PC and did not receive a response.
Remote print data will be discarded.	You or the host user has specified that printed data should be discarded. Use the Session Options menu to change that setting.
Remote user is busy.	The remote user is using the Session Options menu to perform some activity such as file transfer or directing print output. You cannot use your host PC until this activity is complete.
Remote user logged off.	The remote user ended the session.
Sector not found on <i>drive name</i>	The drive you have specified appears to have a physical defect. This is an error reported by DOS.
Security violation in caller information file (<i>AWuserid.CI6</i>).	The caller information file for your user ID is corrupted, or it was created by some other user and renamed. All users must create their own caller information files.
Security violation in session configuration file (<i>AWuserid.PC6</i>).	The session configuration file for your user ID is corrupted, or it was created by some other user and renamed. All users must create their own session configuration files.

Table C-1 Common Error Messages (*continued*)

Error Message	Explanation
Seek error on <i>drive name</i> .	Norton pcANYWHERE cannot search the specified drive, because of a hardware problem with that drive. This is an error reported by DOS.
The caller information file could not be found. Logging off...	The host's caller information files could not be found, so the host PC cannot accept connects. These files must be located in the directory that was specified during installation. Check with the network administrator or host user.
The caller information file is invalid. Logging off...	The caller information file is most likely physically damaged. The filename is <i>AWuserid.CI6</i> . The host user may have to reenter the caller information.
The gateway operator has terminated gateway operation.	The session has ended because the person whose PC is set up as the gateway has deactivated that gateway, breaking your connection. Contact the gateway operator or your network administrator or try a blank Gateway Computer Name in the hardware configuration for the LAN connection; then the user making the LAN connection can select an active gateway from a list that Norton pcANYWHERE displays.
The host operator is busy. You may end the session now or wait for the host operator to resume normal operation.	The host user may be performing a Norton pcANYWHERE online activity.
The host PC is in a graphics mode that your terminal does not support.	The host PC is running a software application that uses bitmapped graphics, and your PC does not support bitmapped graphics. It may be possible to run the application in text mode. Have the host user check the manual for the software.

Table C-1 Common Error Messages (*continued*)

Error Message	Explanation
The incoming and outgoing configurations may not be the same.	You cannot use the same device and port for the incoming and the outgoing gateway configurations, because only one operation can take place at a time on the same hardware device.
The password already exists in another entry. Please use another password.	The password the host user specified for a remote user (or group of users) is already being used. Enter a different password for each caller information configuration.
The previous session was interrupted. 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 master password. The host user can safeguard against this problem by setting the host preference Allow Any Password On Reconnect to Yes.
There are no hosts currently available.	No network host is ready and waiting for a call.
The selected comm port is not available or not responding. The selected comm port is: <i>comm port</i> . Please verify....	The port specified in the hardware configuration is not correct. See Chapter 4, "Hardware Configurations," for more information.
The selected host is not available.	The host may not be running Norton pcANYWHERE, or may already be connected to another remote user.
The terminal configuration file cannot be accessed at this time. If your terminal type is <i>terminal type</i> , press Enter to continue.	The host's AW.TRM file could not be read now. It may be corrupted, missing, or the host's access rights do not permit it to be opened. You can connect to this host only if your terminal type matches that of the previous remote user.
This function may not be executed when your keyboard is disabled.	The operation (such as host rebooting) chosen from the Session Options menu is disabled because your remote keyboard is not active in the current session.

Table C-1 Common Error Messages *(continued)*

Error Message	Explanation
Time allowed online has expired.	The session is ended, because the host user has specified a limit on the amount of time you can spend in a session, and that time period has expired. In a few moments, you'll be prompted to leave the session.
Too many files open.	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.
Transfer failed - connection lost.	The file transfer has been halted by a break in the connection between the host and remote PCs. The break may have been caused by: hanging up the telephone, turning off or rebooting the PC, turning off the modem, or unhooking the cable.
Transfer failed - disk read error.	The file transfer cannot be performed because Norton pcANYWHERE cannot read one of the disks. The cause may be: a defect in the disk, a non-existent disk, or a disk of the wrong format.
Transfer failed - disk write error.	Norton pcANYWHERE cannot perform the file transfer because it cannot copy the files to the receiving disk. The causes may be: a defect in the disk, a write-protected removable disk, or a non-existent disk.
Transfer failed - file create error.	The file transfer failed because Norton pcANYWHERE could not copy the file to the receiving PC. This is a message generated by DOS, and may be caused by insufficient disk space.
Transfer failed - operator canceled.	The person who initiated the file transfer canceled it.

Table C-1 Common Error Messages (*continued*)

Error Message	Explanation
Transfer failed - other side canceled.	The other user canceled the file transfer.
Transfer failed - timed out.	One side of the remote session was not responding, so the transfer could not be performed. There is a problem on the other PC.
Transfer failed - too many retries.	The program kept trying to send blocks but they were not received.
Unable to access remote print device. Remote print data will be discarded.	Any attempt by the host to send print data to the remote print device will be ignored. Check that you specified the remote print device correctly in the Remote Preferences (see Chapter 8, "Session Configurations and Remote Preferences") and that the printer is turned on.
Unable to access the file.	Check whether the file is already in use or does not exist. Also check your network access rights to the file.
Unable to activate background file transfer on the host, because DOS is busy....	Try again. File transfer requires various DOS operations and DOS is currently busy on the host. An application may be writing information to the disk, or another DOS operation may be taking place.
Unable to begin operation. Operation must be canceled before restarting with a new device type. Please cancel the operation and try again.	If you have changed your port or device (specified in the hardware configuration), you will have to cancel host operation and restart with the new configuration.
Unable to connect to: <i>computer name</i> .	The named PC is unavailable. It is already in use or not ready to start a session.

Table C-1 Common Error Messages (*continued*)

Error Message	Explanation
Unable to connect to the gateway.	The gateway connection cannot be made because the gateway PC is not prepared. The gateway may not be active, the PC may be turned off, or there may be some problem with the gateway configurations. For more information about gateway operation, see Chapter 5, "Gateways."
Unable to create the file.	Check whether: the disk is full, the filename already exists, or the disk is write-protected.
Unable to delete the configuration. It is a default configuration of the Gateway.	The selected hardware configuration is specified as the incoming or outgoing gateway configuration. You cannot delete it until the user at the gateway PC specifies another configuration for the gateway.
Unable to delete the configuration. It is used by host directory entry: <i>session configuration name</i> .	Before you can delete a hardware configuration, it must be removed from any session configurations that use it. Make sure you don't delete a configuration that someone else needs.
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.
Unable to find COMMAND.COM.	The operation you have requested requires that the COMMAND.COM program, normally on your boot disk, be located. Check your environment (using the Overview option from Norton pcANYWHERE's Hardware Diagnostics) to verify that the pathname following "COMSPEC=" specifies the location of COMMAND.COM.
Unable to initialize communications.	Check with your network administrator to make sure that the network or communications server is functioning properly.

Table C-1 Common Error Messages *(continued)*

Error Message	Explanation
Unable to initialize communications device.	This message generally indicates a network or hardware problem. Contact your network administrator.
Unable to initialize modem.	Your modem is not responding to Norton pcANYWHERE. See "No modem response" earlier for suggested causes.
Unable to release allocated memory.	You attempted to remove Norton pcANYWHERE from memory, but that cannot be done at this time. Other software used by this host PC has probably utilized memory in a way that prevents Norton pcANYWHERE from being removed from memory.
Unable to release system resources.	You attempted to remove Norton pcANYWHERE from memory, but it cannot be done at this time. Releasing another TSR (if the TSR has such an option) may let Norton pcANYWHERE release itself.
Unable to remove from memory.	If you have attempted to cancel the host TSR while the host has other memory-resident software loaded, you may have to cancel that software before Norton pcANYWHERE can be removed from memory.
Unable to respond to the hotkey now because the host is busy. You may end the session now, or continue the session and press the hotkey again later.	The host PC cannot handle the interruption caused by pressing the hotkey sequence at this time. Usually you can try this again and it will work.
Unable to save changes because the entry was updated by another user.	The operation you have attempted cannot be completed because some other user has changed the information. Cause this entry to be re-read from the appropriate file (for example, reselect this item from a menu list) and try the operation again.

Table C-1 Common Error Messages (*continued*)

Error Message	Explanation
Unable to save new settings to disk.	There may not be room on your disk for the new settings, or there is some other problem with your disk. Exit to DOS and check.
Unable to save the screen.	You may not have enough space on your disk to save this screen. You can exit to DOS and make some room.
Unable to transmit. Host not responding.	The host PC is not operating correctly for Norton pcANYWHERE.
Unable to write to the recording file.	You may not have enough space to add to the recording file. You can exit to DOS and make some room.
Unexpected network error.	The host PC received a bad packet sequence number in a response from the remote PC. This error may be generated when you are using drive mapping.
Unknown media on <i>drive name</i> .	Make sure you have specified an IBM-compatible floppy or hard disk drive. The disk may not be formatted.
Unknown modem response.	Check that the modem name in your hardware configuration is correct. If that is not the problem, consult your modem's manual, and Chapter 3, "Hardware Configurations." You may have to enter an additional modem initialization string. Alternatively, with modem manual in hand, you can attempt a connection by typing commands directly to your modem. (Use Direct Connect/Terminal Mode from the Quick Connect Options menu.)
Volume in <i>drive name</i> has no label.	You probably do not have access to the specified fixed drive. The host PC can deny access to drives. Check the Drive Security settings. See "Host Features Preferences," in Chapter 6, "Caller Information and Host Preferences." This is an error reported by DOS.

Table C-1 Common Error Messages (*continued*)

Error Message	Explanation
Warning: Parity is being changed to NONE, which is required for the Norton pcANYWHERE terminal type.	When the session is a remote control session, the parity must be set to NONE. Norton pcANYWHERE will set this automatically.
Warning: The selected directory is not empty. All files and subdirectories will be deleted.	From the file transfer window, if you attempt to delete a directory that contains files and subdirectories, you see this warning message. It gives you an opportunity to change your mind. Otherwise, all files and subdirectories in the chosen directory will be erased.
Warning: The gateway is currently in use. You may cancel the session but this will immediately break the connection to both the primary and secondary computers.	You are attempting to deactivate a gateway while a remote computing session is using that gateway. If you cancel, the host and remote PCs will be disconnected, and the users will be informed that the session is over.
Warning. There are no callers defined and the preferences specify that the caller table is to be used. You may choose to use the default caller parameters or cancel the operation.	The host preferences require the use of caller information configurations to screen incoming connections. However, no caller information configurations are defined. You can change your preference to use the default caller information form or define some caller information configurations.
Warning. There are suspended host sessions...	Before ending the session, you should terminate any suspended remote computing sessions. Otherwise, these host PCs are accessible only with your password or the master password.
Write fault on <i>drive name</i> .	A physical defect on the disk drive that makes it impossible to save data to it. This error was reported to Norton pcANYWHERE by DOS.
Write protect on: <i>drive name</i> .	You cannot write to this drive because it is write-protected.

Problem Solving

This section lists some common remote computing problems and possible solutions for them. They are divided into the following categories:

- Serial communications
- Keyboard
- Graphics
- Other problems
- Tips for remote control of Windows

Incorrect cabling and modem switch settings are also common problems. If you are using a serial configuration, be sure to review Appendix A, “Technical Information,” too.

Serial Communications

Incorrect modem settings and conflicts with hardware interrupts (IRQs) cause a number of serial communications problems.

I can't seem to transfer files with my IBM-compatible computer.

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.

I get an "Unable to initialize communications" message.

There may be a piece of hardware, such as a network card, tape backup card, or other equipment, that is conflicting with the IRQ (interrupt request) 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.

I am accessing a host via modem and my modem is dialing the host, but I can't make a connection.

If you are using a modem to reach a host (or if the host is calling you) and nothing seems to happen after the dial, 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 adjusted. Some telephone systems may require from 45 to 120 seconds after dialing to complete the connection.

I can't seem to run IBM BASIC and BASICA programs on the host PC.

Make sure that the programs you are running remotely do not attempt to use the same port that your hardware configuration specifies.

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.

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.

My modem isn't on pcANYWHERE's list, and it won't initialize.

If your modem is supposed to be Hayes-compatible, use the Hayes modem setting that most closely matches the data rate of your own. If that doesn't work, use 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.

If Norton pcANYWHERE issues the message "Unknown modem response" or another message indicating that it can't start your modem, include commands for carrier-detect (DCD) to follow a normal carrier, DTR on, and a ring number to answer on in the Additional Modem Initialization String.

My modem isn't on pcANYWHERE's list and I get strange characters when I try to start a session.

See the item above.

pcANYWHERE thinks there is a connection when there is none.

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 only goes on 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.

Sometimes there is a break in the connection when I try to access the host PC as it is running an application, or when I try to run certain software on the host PC.

Check the software on the host PC. If the application is expecting to find the mouse or a printer on the same port that the host is using for the remote control session, you may have to reinstall the application or change its settings.

The host PC sometimes drops the connection during a session.

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.

When the host user calls the remote PC, there's no response.

If there is a problem when the host user calls the remote PC, it may be caused by a setting on the remote modem. Make sure that the carrier detect signal (DCD) is set to follow a normal carrier.

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.

My remote screen looks fine, but the keyboard doesn't seem to work correctly.

You may need to try Norton pcANYWHERE's special keyboard handler. Use Special Options from the Remote Sessions Options menu, and try Level 1 of the special keyboard handler first. Then try the other levels if this doesn't

work. (The host's caller entry must allow use of the special keyboard handler.)

Some of the special (function, cursor) keys don't work during the session.

You may need to enable the special keyboard handler. Press the host hotkey and select *Special Options*. This is a host-controlled function, so your caller information entry on the host PC must enable the use of the special keyboard handler.

The hotkey isn't working.

This problem may be caused by memory-resident programs that are running on your PC, programs like mouse drivers, print spoolers, or pop-up software. Remove all memory-resident programs. Then you can try loading them again, one at a time, to pinpoint which one is causing the problem.

Graphics

Both the host and remote PCs have preferences that can improve the display of graphics on the remote screen.

My remote screen repaints frequently on my monochrome monitor when I run host programs that are in color.

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. You can also change the Attribute Translation option to No, using Special Options from the Remote Session Options hotkey menu.

Both the remote and host PCs have graphics adapters that are compatible with pcANYWHERE, but graphics images do not appear on the remote screen.

The host user may need to make a change to host preferences. Try setting Advanced Graphics Mode Detection to Yes.

Other Problems

This section contains miscellaneous problems and their possible solutions.

I want to use pcANYWHERE to do customer support.

Set up the host PC so that Norton pcANYWHERE is activated by an incoming call. Use the Begin Host Operation or Exit, Allow Incoming Calls option. If you are communicating via modem and want the customer to bear most of the telephone costs, set the caller information on the host PC to include your telephone number as the Callback Phone Number. (It can also be included as the Default Phone Number in Host preferences.) See Chapter 7, "Remote Control Sessions," for the command-line options that launch the host PC from the host user's AUTOEXEC.BAT file.

I want to run DESQview on the host PC.

To run DESQview remotely, first invoke Norton pcANYWHERE on the host PC. Then, press Alt to view the DESQview menu after the remote PC is in session.

pcANYWHERE seems to freeze up when I use it to access Novell NetWare services.

Make sure you run the NetWare shell program *before* you run Norton pcANYWHERE.

I have some problems running pcANYWHERE on my 20-MHZ 80386 computer.

You may have to slow down your processor speed to 12 or 16 Mhz. If your serial port or modem is not fully compatible with your high-speed computer, hardware problems may occur. These problems are not caused by Norton pcANYWHERE.

Tips for Remote Control of Windows

The memory and graphics requirements of the Windows environment can pose unique problems to memory-resident software (TSRs). To avoid any conflicts between Windows and Norton pcANYWHERE, use the following guidelines when installing and using Norton pcANYWHERE.

General Information

Make certain that you load the Norton pcANYWHERE/Host *before* running WINDOWS.

Both the host and remote PC must have EGA or VGA graphics capability.

Windows Information

Avoid using complex wallpapers when in the WINDOWS operating environment. Complicated graphics patterns drastically decrease the performance of Norton pcANYWHERE. Repetitive patterns, including cubes and pyramids are acceptable.

In addition, the Windows logo displays relatively slowly. You can bypass the logo and initiate Windows by using the following command:

WIN :

If you cannot run Microsoft Windows remotely with Norton pcANYWHERE, check the following items. (The examples use a standard VGA adapter, keyboard, and a Microsoft mouse.)

- SYSTEM.INI file:

In the [boot] section of your SYSTEM.INI file, changes are made to the following lines to use pcANYWHERE drivers:

```
display.drv=
keyboard.drv=
mouse.drv=
```

In the [386Enh] section, the TimerCriticalSection statement, the NetHeapSize statement, and the following device= statements are modified as follows:

```
TimerCriticalSection=500
NetHeapSize=24
device=vpcaw.386
device=aw_vcd.386
```

- Make sure PCAW.INI file exists and is correct. The contents of this file should be similar to the following. It will contain the drivers formerly in your SYSTEM.INI file. You can compare this with the backup of your SYSTEM.INI (SYSTEM.01) to see what the original drivers were.

```
[pcANYWHERE ]
mouse=aworgmse.drv
keyboard=keyboard.drv
display=vga.drv
```

If the original mouse driver in the SYSTEM.INI file was "mouse.drv", then the line should be "mouse=aworgmse.drv". If it was not mouse.drv, then the filename after "mouse=" should be the original driver from the SYSTEM.INI file.

- The following pcANYWHERE files must be located in the same directory as the Windows System drivers:

```
aw_vga.drv
aw_vgabw.drv
aw_ega.drv
aw_mouse.drv
aw_kbd.drv
aw_kbdhp.drv
aw_kbdol.drv
aw_vcd.386
ega.3gr
egacolor.2gr
vag.3gr
vagcolor.2gr
```

aworgmse.drv (This file will only be added if the original mouse driver line in your SYSTEM.INI file was "mouse=mouse.drv".)

NOTE: If you are using a network installation of Windows, the Windows System drivers are in a shared directory on the network, and the SYSTEM.INI files are personal. The above files must be in the shared directory on the network.

- Make sure Windows can run alone on the host PC before trying to run it remotely.
- Make sure the mouse driver is loaded on the remote PC.

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 ending 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.
- automated procedure** A Norton pcANYWHERE automated procedure allows the remote user to set up predefined remote control sessions that can take place in the absence of an operator. This is very convenient for performing certain activities—routine, repeated file backups, for example—during non-business hours.
- 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 (300×1) 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 (300×4) 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 device 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. The host user can also blank the remote screen during a session.
- 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. *Compare* baud rate.
- break length** *See* 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). *See* *bit*.
- 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. *See* also null modem cable.
- call** Making a connection between computers by dialing a computer via a modem or making a connection between computers in general.
- Telephone numbers for calls appear in session configurations on the remote PC. On the host PC, the default telephone number used to initiate a session is set as a host general preference. The host PC can perform a callback. *See* callback.

- 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 Attempted 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 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. *See* 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 /O:R, /O:R</code> is a command-line option that starts pcANYWHERE on a remote PC.
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. <i>See</i> flow control, protocol.
communications system	The combination of hardware, software, and data-transfer links that makes communications possible.
compression	<i>See</i> data compression.
computer name	The name you assign to your PC for Norton pcANYWHERE sessions.

- configuration** *See* hardware configuration, session configuration, caller information, and gateway configuration.
- connection** The point at which devices establish a communications link.
- connection detection** Whether you are using a modem or a direct connection, you must specify some method by which your system determines that a physical connection has been made or ended. (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 preferences that can be set for the AWSSEND program 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 setting for the Modem option in serial hardware configurations. When your modem and no reasonable alternative is in the list of supported modems, you can choose 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	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	Usually refers to the screen or monitor. The following display preferences affect the speed of display of the host screen on the remote PC and how graphics or characters are displayed: Maximize Display Speed, Synchronized Screen Display, Full Graphics, Advanced Graphics Mode Detection, Graphics Translation Favor, Attribute Translation, and Blink Attribute Support (also called Blink Attribute).
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). To do so, you enable the mapping on the host PC using the Remote Drive Mapping option, a host features preferences. From the remote PC, you enable the mapping and also use the Drive Mapping option in the session configuration to define what drive letters will be used on the host PC to access the remote 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. *See* 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. *See* 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. *See* 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 *modems* 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. *See* 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 AWSEND and background file programs. For AWSEND, the remote user sets file transfer preferences; the host user must allow background transfers.

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, X-ON/X-OFF. 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** The PC or computer to which the remote user is connected.
- host PC** The PC controlled by the remote user during a remote control session.
- host mode** The host mode is the state of pcANYWHERE on the host PC. These modes are waiting, incoming-call, and hotkey modes. The host user controls the host mode or allows the remote user to do so. The mode can be set using menus or command-line options with either AW or AWLOGOFF.
- host password** The password a remote user uses to access a specific host PC. The password is often listed as part of a session configuration.
- 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 menu during a session. The host hotkey is initially Alt+RightShift. The remote hotkey is initially Ctrl+RightShift. Either can be changed.

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. Use the Inactivity Timeout option, which is in the Host Security Preferences form, to set the number of minutes for the timeout. Whether or not the timeout is enforced depends on the setting of the Caller Subject to Inactivity Timeout option, which is in the caller information configurations and the default caller information form.

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 option in the Host Security Preferences determines what passwords are valid in this case.

An option, which is in the caller information configurations and the default caller information form, that determines whether or not the inactivity timeout is enforced for a particular remote user.

A gateway preference can also specify an inactivity timeout. It applies only to idle sessions that take 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 a 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 a 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

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 the caller information) to specify whether or not a keyboard handler is used by the remote user and the Special Keyboard Handler Type option (a host features preference) 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** Describing 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 for remote control sessions.
- 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 transfer files using the DOS COPY command instead of AWSEND. *See* drive mapping.
- 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 and then back to digital (demodulates) at the other end. Modems can transmit at different speeds or data-transfer rates. *See* baud rate, bps.
- Modem** An option in serial hardware configurations that specifies the type of modem to be used during a connection.
- 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 using 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.

parameter

In Norton pcANYWHERE, an option or preference on a form. In the script language, information supplied to a command that follows the command name.

parity

In communications, parity refers to 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 can be computed in any of the following ways:

- even Adding the data bits and the parity bit yields an even number. If a character with an even number of bits arrives with the parity bit set (to 1), an error must have occurred during transmission.
- odd Adding the data bits and the parity bit yields an odd number. If a character with an odd number of bits arrives with the parity bit set (to 1), an error must have occurred during transmission.
- none There is no parity bit.
- space Sometimes a parity bit is used, but it is always set to 0. If a character is received with a parity bit set to 1, an error may have occurred during transmission. Space can also be used to transmit 7-bit characters to a device which is expecting 8-bit characters. Also referred to as *bit trimming*.
- mark Works the same way as Space, except that the parity bit is always set to 1. Also referred to as *bit forcing*.

- parity bit** In modem-to-modem communications, the sending computer adds an extra bit, called a parity bit, to the data bits that represent a character. 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.
- 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** In Norton pcANYWHERE, a term used to describe 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** *See* 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. *See* 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. *See* 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 (X-ON/X-OFF). *See* RTS, CTS, X-ON/X-OFF, 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. *See* 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* *Creating Norton pcANYWHERE Scripts*, 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.
snow	Some color displays cause snow (just like the static on a TV set) on the remote or host screen. Norton pcANYWHERE can eliminate snow when it does occur.
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. *Compare* 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. *Contrast* asynchronous transmission.
- Telebit ACS** 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.
- terminal** 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). *See* terminal emulation.
- terminal emulation** 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.
- terminal mode** The pcANYWHERE mode that mimics a terminal when connecting to an online service for an online session. Terminal mode can also be used by advanced users who wish to type commands directly to their modems.

timeout	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.
tone dialing	Sounds of particular frequencies can be heard when dialing, as opposed to pulse dialing where clicks can be heard.
translation table	A table that specifies a conversion of specific data bytes from one code to another.
unidirectional gateway	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.
upload	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.
Use Gateway	An option in network hardware configurations. Set this to Yes if you want to use a gateway. <i>See</i> gateway.
voice-first connection	A connection via modem for a remote control session, in which you talk first, then switch to a 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.

X-ON/X-OFF

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 X-ON/X-OFF as the setting for flow control in a hardware configuration. *See* flow control and RTS/CTS.

Index

A

access

drives, 30

ACS, 65

contrasted with a gateway, 77

definition of, 20, 311

driver, 68

hardware configuration, 68, 69

Telebit ACS, 71

Activity Log Processing utility, 215, 230

activity log report, 232, 235

adding

operation to operations file, 191

options to menu, 51

Additional Modem Initialization String

option, 311

address, 239

ADDS Viewpoint terminal emulation, 258

ADM 3A terminal emulation, 258

advanced

network installation, 39, 41, 42

Allow Caller To Blank Host Screen option,
122

Allow Caller To Change Host Mode option,
123

Allow Caller To Reboot Host option, 122

Allow Deletion of Directories option, 180

Allow Drive Security option, 131

Allow Pop-Up File Transfer option, 130

Allow Remote Drive Mapping option, 130

Allow Remote Mouse from the Host option,
130

Allow Scanning While Host Busy option,
129

Allow Special Keyboard Handler option,
123

Allow Use of Ctrl+Break option, 122

Alt keys, 325

American National Standards Institute, 311

American Standard Code for Information
Interchange. *See* ASCII

analog communication., 242

ANSI, 311

ANSI terminal emulation, 260, 311

applications

launching automatically, 124

archiving

log file data, 230, 238

ASCII, 212

carriage returns, 113

character set, 280

character translation table, 95

control characters, 281

definition of, 280

extended character set, 210

file-transfer protocol, 112, 280, 320

linefeeds, 114

OEM character set, 282

asynchronous communications server. *See*
ACS

asynchronous transmission, definition of, 312

attribute, definition of, 312

AUTOEXEC.BAT

changing, 45

reviewing, 22, 216

automated procedure, 154, 185

definition of, 312

execution of, 194

testing, 187

automating

connection, 90, 186

downloading of files, 116

execution of DOS commands on host PC,
22, 124

file transfers, 124, 192

limitations of, 22

- automating (*continued*)
 - procedures, 187
 - recording of communications session, 222
 - remote control operations, 22, 185
 - remote control sessions, 312
 - using script files, 22
 - AW environment variable, 41, 43
 - adding to AUTOEXEC file, 45
 - AW.BIN, 77
 - AW.EXE, 30
 - AW.HH6, 230
 - AW.MK6, 94
 - AW.OPR, 190
 - AW.RL6, 230
 - AW.SPL, 102
 - AW.SWP, 111
 - AW.TRN, 96
 - AWHOST.EXE, 30
 - AWLOGOFF, 163
 - AWREMOTE.EXE, 30
 - AWSSEND.EXE, 103, 124, 175, 180, 194
 - error level values, 184
 - exiting, 182
 - file-transfer protocol for, 320
 - AWSWAP environment variable, 111
- B**
- background file transfers, 130, 183, 202
 - when to use, 183
 - backspace key
 - changing functionality, 207
 - destructive, 93, 207
 - non-destructive, 93, 207
 - Banyan VINES, 66
 - support for, 18
 - Banyan Vines, 312
 - baud rate
 - definition of, 242, 312
 - BBS. *See* bulletin board
 - Be A pcANYWHERE Gateway menu, 79
 - Be A pcANYWHERE Host menu, 145
 - bidirectional gateway, 29, 77, 79
 - definition of, 312
 - specifying, 82
 - billing
 - detail report, 233, 235
 - summary report, 234, 235
 - bit, 242, 313
 - definition of, 313
 - start, 332
 - stop, 333
 - bit forcing, 252, 328
 - bit trimming, 252, 328
 - blanking host screen, 122, 139, 146, 168
 - blinking characters, 109, 167, 313
 - board
 - add-on, 73
 - bps, 242
 - contrasted to baud rate, 242
 - definition of, 313
 - break length, 206, 313
 - break signal, 202
 - definition of, 313
 - buffer
 - explanation of, 245
 - specifying size, 115
 - bulletin board, 19, 197
 - definition of, 312
 - byte, 242
 - definition of, 313
- C**
- cable
 - RS-232 standard, 246
 - cables, 246
 - definition of, 313
 - selection of, 247
 - call
 - definition of, 313
 - inbound, 77
 - incoming, 79
 - outbound, 77
 - outgoing, 79
 - waiting for, 150, 157

- Call A pcANYWHERE Host menu, 86, 155
- Call Remote User option, 151
- callback
 - definition of, 314
 - waiting before, 134
- Callback Phone Number, 126
- Callback Remote User, 126
- caller information, 117
 - configuration
 - creating, 120
 - creating reports for billing purposes, 233
 - specifying, 136
 - default, 126
 - definition of, 314
 - logging, 231
 - what it does, 21
- calling card number, 333
- Cancel And Remove From Memory option, 151
- canceling
 - gateway operation, 83
 - host TSR, 153
 - remote control session, 163
- carriage returns, 93, 113, 208
 - definition of, 314
- carrier detect, 316
 - definition of, 314
- carrier, definition of, 314
- case-sensitivity, 137
 - definition of, 314
- changing
 - AUTOEXEC.BAT file, 45
 - automated procedure, 186
 - break length, 206
 - caller information, 120
 - colors of menus, 56
 - cursor, 107
 - data rate, 205
 - file transfer preferences, 178
 - file type, 43
 - file-transfer protocol, 94, 212
 - flow control, 206
 - changing (*continued*)
 - gateway, 83
 - hardware configuration, 75, 89
 - host mode, 146, 150
 - hotkey, 102, 133
 - menu options, 51
 - modes, 150
 - mouse preferences, 106, 170
 - online session configuration, 88, 204
 - operations file, 190, 193, 194
 - parity, 206
 - password, 54
 - path, 43
 - personal files to shared files, 41, 43
 - print device, 102, 162, 203
 - received carriage returns, 208
 - session configuration, 87, 88
 - telephone number, 90
 - terminal emulation, 92, 205
 - translation table, 209
 - channel, 314
 - character mode, 257
 - chat mode, 161
 - definition of, 315
 - choosing
 - forms options, 50
 - log file, 235
 - menu options, 50
 - prefix/suffix, 133
 - print device, 203
 - versus selecting, 47, 50
 - class
 - definition of, 315
 - gateway, 82
 - clear screen, 204
 - Clear To Send, 316, 317
 - definition of, 315
 - cold boot, 136
 - color
 - checking ability to display, 219
 - display, 108, 166
 - graphics, 109, 167

- colors
 - of menus, 56
- comm port. *See also* serial port
- comm port. *See* communications port
- command
 - automatic execution of, 124
- command mode
 - modem, 243
- command-line options, 30, 153, 159, 184, 199
 - definition of, 315
- command-line options. *See also* DOS,
 - commands
- commands
 - modem, 243
- comment, adding to operations file, 193
- communication
 - analog, 242
 - definition of, 315
 - digital, 242
 - voice, 242
- communications channel, 314
- communications device
 - selecting, 67
 - sharing, 77
 - using more than one, 151
- communications link, 315
- communications port, 239, 332
 - ACS, 70
 - address, 239
 - checking number of, 215
 - custom, 73, 74
 - definition of, 315
 - Interrupt 14, 64
 - modem, 61
 - non-standard address, 73
 - null modem cable, 63
 - selecting, 61, 64
 - serial, 63
 - Telebit ACS, 71
- communications session
 - automated, 124
 - configuration of, 86
 - ended by inactivity timeout, 81
 - communications session (*continued*)
 - ending from menu, 163
 - hardware configuration, 89
 - logging, 221
 - logging of, 21
 - play back of, 223
 - recording, 21, 22, 221
 - reports of disconnects, 233
 - starting from host, 147
 - starting remote PC, 154
 - switching from data to voice, 173
 - switching from voice to data, 148
 - time limit for, 124
 - timing out, 123
 - unattended, 143, 154, 194
 - using Quick Connect feature, 151, 157, 199
 - voice first, 148
- communications system, 315
- Communications Tests... option, 218
- compiling scripts, 215
- compression, 105, 180, 243, 315
 - setting, 254
- CompuServe, 19, 197
 - parity, 68
- computer
 - naming, 20
- CONFIG.SYS
 - reviewing, 22, 216
- configuration, 316
 - caller information, 120
 - specifying, 136
 - gateway, 79, 321
 - hardware, 59, 321
 - host PC, 127
 - host security preferences, 135
 - network hardware configurations, 65
 - overview of, 20
 - remote control session, 86
 - remote PC, 85
 - stand-alone PC hardware configurations, 60
 - testing, 217

- configuration files
 - for caller information, 120
 - for network installation, 40
 - connection
 - automating, 90, 186
 - break in, 314
 - carrier detect, 316
 - definition of, 316
 - detection of, 316
 - direct, 62
 - ended by inactivity timeout, 322
 - failed
 - logging, 232
 - logging attempts, 231, 232
 - lost, 322
 - network, 65
 - node-to-node, 67
 - online service, 85
 - PC to network, 65
 - prompt host about, 140
 - report of activity log, 232
 - serial, 60
 - time/date of, 187
 - unsuccessful
 - logging, 231, 232
 - using Quick Connect feature, 151, 157, 199
 - voice first, 148, 334
 - without session configuration, 86
 - Connection Ended By option, 316
 - Connection Started By option, 316
 - control codes, 203
 - converting 4.5 files to 5.0, 30
 - copying
 - files, 182
 - installation disk, 37
 - recorded sessions, 225
 - screen snapshot to a file, 229
 - CPU
 - port addresses, 239
 - CPU usage
 - gateway, 81
 - CR. *See* carriage returns
 - crash recovery, 103, 106, 115, 180
 - definition of, 316
 - creating
 - ACS hardware configuration, 69
 - automated procedure, 186
 - caller information configuration, 120
 - directory, 181
 - gateway, 79
 - hardware configuration, 75
 - modem hardware configuration, 60
 - network hardware configuration, 65
 - network node hardware configuration, 66
 - online session configuration, 86
 - operations file, 190
 - remote control session configuration, 86
 - reports from log files, 234
 - serial hardware configurations, 60
 - Telebit ACS hardware configuration, 71
 - telephone prefix/suffix, 55
 - translation table, 210
 - credit card number, adding to telephone number, 55
 - Ctrl+Break, 122, 202
 - CTS
 - definition of, 315, 317
 - cursor
 - changing movement, 107, 171
 - display test, 219
 - custom modem, 29
 - customizing
 - modem commands, 74
 - modem connection, 317
 - port address, 73, 74
- ## D
- data bits, definition of, 317
 - data compression, 105, 243
 - definition of, 317
 - data encryption, 30, 140
 - data mode
 - modem, 243

- data rate, 245, 254
 - changing
 - on-line, 205
 - definition of, 317
 - modem data transfer, 242
 - null modem cable, 63, 245
 - selecting, 63
 - with macros, 208
- Data Rate option, 317
- Data Set Ready, 316, 317, 319
- Data Terminal Ready, 255, 319
- data transfer, 317
- data transmission, 317
- data window
 - size of, 115
- database
 - exporting log files to, 237
- date range for reports, 235
- DB25 connectors, 247
- DB9 connectors, 247
- DCD. *See* carrier detect
- deactivating
 - gateway, 84
- default
 - caller information, 126
 - hardware configurations, 60
 - hotkey, 133
 - telephone number, 133
- Delay Before Callback Attempted option, 134
- deleting
 - data from log file, 237
 - directory, 180
 - host and remote, 181
 - directory on remote PC, 105
 - files
 - host and remote PCs, 181
 - hardware configuration, 76
 - operation from operations file, 193
 - options from menu, 51
- destination
 - definition of, 318
 - for log report, 236
- Destination File option, 104, 179
- device
 - printer, 102
 - selecting correct type for network, 67
 - sharing, 77
- Device/Port option, 318
- DG 100/200 terminal emulation, 260
- diagnostic tests, 22, 215
- dial, definition of, 318
- dialing instructions, 90
- dial-up telephone connection, 333
- digital communication, 242
- direct connection
 - definition of, 318
- direct connection. *See also* null modem cable
- direct connection/tsee null modem cable, 254
- direct serial hardware configuration, 62
- directory
 - creation, 181
 - deletion
 - on host/remote PCs, 181
 - on remote PC, 105, 180
 - management, 181
 - selecting, 52
- disconnect from host on network, 163
- DISKCOPY, 37
- display
 - definition of, 318
- display. *See also* screen
- displaying
 - received control codes, 203
 - reports, 236
- DOS
 - accessing during online session, 202
 - accessing during remote control session, 172
 - available memory needed, 192
 - commands
 - adding to operations file, 192
 - automatic execution of, 22
 - starting remote with, 159
 - using to log off remote control session, 163
 - using to start host, 153

DOS (continued)

- environment, 22
 - settings, 216
 - ERRORLEVEL, 184
 - exiting, 203
 - launching host TSR from, 153
 - launching online session from, 199
 - starting remote PC from, 159
 - transferring files from, 183
 - version required to run Norton
 - pcANYWHERE, 17
- Dow Jones, 19, 197
- downloading
- definition of, 318
 - files
 - automating, 116
 - from online service, 211
 - timing out, 113
- drive
- restricting access to, 125, 131
 - security for, 125, 131, 319
- drive access, 30
- drive mapping, 18, 91, 92, 130, 172, 173
- definition of, 319
 - what it does, 29
- drive security, 30
- driver
- ACS, 68
- DSR, 317, 319
- DTE (Data Terminal Equipment), 247
- DTR, 319
- DTR State option, 319
- duplicate files, 103, 104, 179

E

- emulation. *See* terminal emulation
- encryption, 30, 140
- End Session option, 163, 202
- error
- action to take upon occurrence of, 189
 - AWSSEND, 184
 - detection of, 252
 - during remote control session, 189

error (continued)

- message boxes, 49
- error checking, 114, 319
- error correction, 319
- ERRORLEVEL, 184
- escape sequences, 311
- even parity, 252
- executing command
 - automatically, 124
- exit
 - DOS session, 203
 - file transfer program, 182
 - gateway, 84
 - menu, 51
 - online session, 202
 - remote control session, 163
- Exit, Allow Incoming Calls option, 146, 150
- exporting
 - log files to database, 237
- extended ASCII character set, 210
- external modem, 240
 - definition of, 319
- external modem. *See also* modem

F

- favor color or resolution, 109, 167
- file
- selecting, 52
- file attributes, 312
- file compression, 103, 105, 180
- file transfer window, 175
- File Transfer... option, adding to remote's menu, 130
- file transfers, 211
- allow pop-up, 130
 - automating, 22, 124, 192
 - background operation of, 130, 183
 - between host and remote PCs, 174
 - between online service and PC, 211
 - definition of, 320
 - from DOS prompt, 183
 - modem speed, 242
 - preferences, 103, 178, 189

- file transfers (*continued*)
 - protocol
 - changing, 94
 - definition of, 320
 - setting for, 112, 114
 - speed of, 245
 - using ASCII protocol, 112
 - using KERMIT, 212
 - using null modem cable, 62
 - using XMODEM, 212
 - using YMODEM, 212
 - using ZMODEM protocol, 114
 - file type
 - changing, 43
 - files
 - automatic download of, 116
 - compression of, 105, 180
 - copying, 182
 - deletion of
 - host and remote PCs, 181
 - downloading, 116, 211
 - duplicate, 103, 104, 179
 - log report, 236
 - macro keys, 95
 - management of, 181
 - overwriting, 104, 179
 - recorded sessions, 223
 - renaming, 182
 - sharing
 - configuration, 80, 86
 - tagging, 177, 178
 - transferring. *See* file transfers
 - uploading, 212
 - flow control, 254
 - changing
 - on-line, 206
 - definition of, 320
 - explanation of, 245
 - hardware, 331
 - null modem cable, 63
 - selecting, 63
 - setting, 254
 - software, 331, 335
 - Formatted Report Output option, 237
 - forms, 47
 - choosing options on, 50
 - selecting options from, 50
 - full graphics, 109, 167
- ## G
- garbage characters, 173
 - gateway
 - activating, 83
 - benefits of using, 77
 - bidirectional, 29, 77, 79
 - definition of, 312
 - specifying, 82
 - canceling operation, 83
 - changing, 83
 - choosing, on a LAN, 156
 - class, 82
 - definition of, 315
 - contrasted with ACS, 77
 - creating, 79
 - deactivating, 84
 - definition of, 20, 320
 - exiting, 84
 - frequency of CPU access, 81
 - hardware configuration, 60, 78, 80
 - inactivity timeout, 81
 - inbound, 78, 323
 - modifying, 83
 - options, 67
 - outbound, 78, 327
 - parity, 68
 - preferences, 80
 - reactivating
 - after cancelation, 83
 - after reboot, 83
 - setting up, 79
 - specifying at installation, 42
 - starting, 83
 - status box, 79
 - TSR, 77, 78
 - unidirectional, 77, 78, 79, 327
 - definition of, 334

gateway (*continued*)
 unidirectional (*continued*)
 specifying, 82
 what it does, 77
 gateway configuration, 321
 Gateway... option, 79
 general preferences, 102, 127, 132
 General... option, 100, 101
 Go to DOS option, 172, 202
 graphics
 color, 109, 167
 full, 109, 167
 non-standard, 129
 resolution, 109, 167

H

handler, 110, 123, 131, 169
 definition of, 324
 handshaking, 320, 321
 hard carriage return, 314
 hardware configuration
 ACS, 68, 69
 changing, 89
 session options only, 204
 creating, 75
 multiple, 59
 current, 145
 default, 60
 definition of, 59, 321
 deleting, 76
 diagnostics, 22
 dial type, 318
 difference between network and stand-alone, 65
 direct connection, 62
 DTR state, 319
 explanation of, 20
 gateway, 78, 80
 Interrupt 14, 64
 modem initialization, 311
 modem options, 253
 modifying, 75

hardware configuration (*continued*)
 multiple, 65
 network, 65
 NASI/NCSI, 69
 network, 65
 testing, 217
 node, 66
 null modem cable, 62
 off-LAN connections, 65
 online service, 254
 redial attempts, 330
 renaming, 75
 selecting
 correct type, 59
 for communications session, 89
 serial, 60
 testing, 217
 shared file, 80
 specifying custom port, 73
 Telebit ACS, 71
 types of, 59
 Hardware Configurations menu, 60
 Hardware Diagnostics utility, 215
 hardware flow control (RTS/CTS), 245, 331
 hardware handshake, 320, 321
 hardware interrupt, 240, 323
 hardware requirements, 17
 hardware, testing, 215
 Hayes AT Command Set, 243
 Hayes Compatible setting, 253
 Hayes Smartmodem 2400 setting, 253
 Hazeltine 1500 terminal emulation, 264
 help system, 49
 Hercules graphics page, 168
 hex codes, 96, 210
 high memory, loading host TSR, 133
 history. *See* log files
 host
 definition of, 321
 host mode
 definition of. *See also* host PC, modes
 Host Name To Add. *See* creating, remote control session configuration

Host Names menu, 86

host PC

- allow rebooting of, 122
- caller information, 21
- canceling TSR, 153
- changing mode, 146
 - by remote user, 123
 - using hotkey, 150
- choosing, on a LAN, 156
- connecting without session configuration, 86
- contrasted to online service, 19
- contrasted to remote PC, 18
- definition of, 18, 321
- directory deletion on, 181
- entering name for, 91
- hotkey, 133, 322
- hotkey mode, 144
- incoming-call mode, 144
- installation
 - with Windows installed, 37
- launching, 144
- list of, 86
- loading TSR into high memory, 133
- log file, 230
- log history file, 230
- mapping drives to, 91, 172
- mode to be in after disconnect, 188
- mode, types of, 144
- preferences, 127
 - table of, 117
- rebooting, 122, 174
 - automatically, 136
- recording sessions with, 221
- screen updates, 129
- security preferences, 135
- setting time limit for use, 124
- starting, 144
- starting remote control session from, 146
- waiting mode, 144

Host Preferences... option, 128, 132

host TSR

- activating, 150

host TSR (*continued*)

- launching, 144
 - from DOS, 153
- status of, 145, 148

host user

- definition of, 18
- special options, 164

hotkey, 102

- changing, 133
- default, 133
- default key combination for, 322
- defining, 102
- definition of, 322
- host, 322
- remote, 322
- using to change host modes, 150

hotkey mode, 144, 150, 321

I

IBM terminal emulation, 264

inactivity timeout

- definition of, 322
- ending remote session, 123
- session ended by, 81
- specifying, 81, 189
- specifying time for, 138

inbound gateway, 78, 323

incoming calls, 77, 79

incoming-call mode, 144, 150, 321

information boxes, 48

initialization string, 254

- what it does, 243

initialize, definition of, 323

Initially On, 223

initiating remote control session

- from host PC, 146
- from remote PC, 154

installation

- on a diskless workstation, 37
- on a network, 39
 - default options, 41
- on a PC, 36
 - with Windows installed, 37

installation (*continued*)
 single-user, 36
 uninstalling, 44
 internal modem, 73, 240
 definition of, 323
 Interrupt 14 hardware configuration, 64, 323
 interrupt. *See* IRQ
 IRQ, 73
 definition of, 323
 explanation of, 240
 hardware interrupt, 73
 explanation of, 240
 interrupt request, 73
 non-standard, 73

K

KERMIT file-transfer protocol, 212
 keyboard
 activating, 139
 definition of, 323
 diagnostics, 22, 220
 disabling, 139, 165
 locking, 139
 mapping for terminal emulation, 257
 keyboard handler, 110, 123, 131, 169
 definition of, 324
 keys
 backspace, 93, 207
 macro, 94, 208

L

LAN. *See* local area network (LAN)
 leased line, 62
 definition of, 324
 using modems with, 249
 LF. *See* linefeeds
 Line Wrap option, 92, 206
 linefeeds, 93, 113, 114
 definition of, 325
 List of Hosts, 77, 86
 List of Hosts. *See also* remote control session

local
 definition of, 325
 local area network
 choosing gateway for remote session, 156
 choosing host PC for remote session, 156
 definition of, 324
 local area network (LAN), 20
 hardware configuration, 65
 installation, 39
 off-LAN connections, 65, 77
 locking host keyboard, 139
 log
 connections attempted, 231, 232
 connections made, 21
 definition of, 325
 log files
 archiving, 238
 choosing, 235
 creating reports from, 235
 deleting data from, 237
 displaying on screen, 236
 exporting
 to column format, 237
 to database, 237
 history, 230
 host PC, 230
 printing, 236
 remote PC, 230
 report format, 237
 storing reports on disk, 236
 what they do, 215
 log reports
 types of, 232
 Log Session option, 231
 logging off, 163
 logging off. *See also* AWLOGOFF
 login
 definition of, 325
 logoff, 325
 LPT1, 325, 327

M

macro keys, 94, 208
 definition of, 325

macro, definition of, 325

mainframe. *See* terminal emulation

map drives. *See* drive mapping

mapping keys. *See* keyboard,mapping

mark parity, 252

master password, 326

Maximize Display Speed option, 129

memory
 amount available for DOS commands, 192
 video, 215

memory-resident software, 307

menus
 adding options to, 51
 choosing options from, 50
 customizing colors, 56
 deleting options from, 51
 exiting, 51
 navigation within, 50
 renaming options on, 52
 Yes/No, 49

message boxes
 error, 49
 informational, 48

mode
 after disconnect, 188
 changing, 146, 150
 types of, 321

modem, 242
 cable selection, 247
 command mode, 243
 commands, 243
 connect speed, 311
 custom, 29
 custom setup, 254, 317
 data compression, 243, 254
 data mode, 243
 definition of, 19, 326
 external, 240
 definition of, 319
 hardware configuration, 60, 253

modem (*continued*)
 Hayes-compatible command mode, 243
 how it works, 242
 initialization, 311
 initialization string, 254
 internal, 73, 240
 definition of, 323
 leased-line compatible, 249
 manual setting, 254
 pool, 20
 recommended settings for, 244
 replacer. *See also* null modem cable
 selecting parameters for, 62, 65
 setting physical switches on, 243
 sharing, 77, 79
 speed, 242
 use of data compression, 243

modify. *See* changing

modular connection, 319

monitor
 types, checking, 215

monitoring control codes, 203

monochrome display, 108, 166

mouse
 definition of, 326
 preferences, 106, 170
 remote, 170

multiplexers, 249, 250

MUX, 250

N

NACS, 65
 definition of, 326

naming
 computer, 20
 your PC, 20, 53

NASI, 326

NASI/NCSI
 definition of, 326
 hardware configuration, 69
 selecting device, 69

NetBIOS, 66
 definition of, 327

- NetBIOS (*continued*)
 - support for, 18
 - NetWare IPX, 66, 67
 - definition of, 327
 - network
 - asynchronous communications server, 326
 - caller information, 126
 - choosing
 - gateway, 156
 - host PC, 156
 - configuration files, 40
 - connection
 - definition of, 20
 - default installation options, 41
 - definition of, 327
 - hardware configuration, 65
 - difference from serial hardware configuration, 65
 - multiple, 65
 - testing, 217
 - installation, 39
 - node
 - definition of, 327
 - hardware configuration, 66
 - node-to-node connections, 67
 - restricting access using unidirectional gateway, 79
 - use of command-line options, 153, 159, 199
 - network asynchronous communications server, 333
 - node, 66
 - definition of, 327
 - device drivers, 66
 - hardware configuration, 60, 66
 - node-to-node connections, 67
 - Norton pcANYWHERE for DOS
 - difference between stand-alone and network installation, 65
 - file-transfer protocols, 212
 - hardware requirements, 17
 - installation, 36, 37
 - Norton pcANYWHERE for DOS (*continued*)
 - navigation and selection, 46
 - new features, 29
 - what it does, 17
 - Novell Asynchronous Communications Server. *See* NACS
 - Novell Asynchronous Services Interface. *See* NASI/NCSI
 - Novell NetWare, 20
 - support for, 18
 - null modem cable, 62
 - data-transfer speed, 245
 - definition of, 20, 327
 - explanation of, 247
 - hardware configuration for, 62
 - pin configuration for, 248
 - number of retries, 188
 - number, telephone. *See* telephone, number
- ## O
- odd parity, 252
 - OEM character set, 282
 - off-LAN connections, 65, 77
 - online service
 - configuration of session, 86
 - connecting to, 85
 - difficulty with, 254
 - definition of, 19, 197, 327
 - file transfers, 211
 - preferences, 97
 - quick connection, 199
 - recording sessions with, 221
 - terminal emulation, 92
 - transferring files to/from, 211
 - online session
 - access DOS prompt during, 202
 - background operation of, 202
 - changing configuration, 88
 - configuration of, 21, 86
 - ending, 202
 - file-transfer protocol, 94, 320
 - initiating, 197
 - Quick Connect, 199

online session (*continued*)
 recording, 221
 starting, 197
 from DOS prompt, 199
 terminal options, 201
 waiting to connect, 198

operations file
 adding operation to, 191
 changing, 190
 creating, 190
 what it does, 190

options
 adding to menu, 51
 choosing from menu, 50
 deleting from menu, 51
 gateway, 67
 renaming on menu, 52
 selecting from forms, 50

outbound gateway, 78, 327

outgoing calls, 77, 79

output, 103

overwriting
 duplicate files, 104, 179

P

pace character, 112, 113

parallel port, 327

parameters
 definition of, 328
 for reports, 235

parity, 254
 changing
 on-line, 206
 definition of, 328
 even, 252
 mark, 252
 null modem cable, 63
 odd, 252
 setting
 gateway, 68
 space, 252

parity-checking error detection, 252

password, 90, 321
 case-sensitivity, 137
 changing, 54
 definition of, 329
 limiting attempts to enter, 137, 138
 management of, 137
 setting, 54, 121
 timeout, 137, 138
 when required for access, 54

path, 45
 changing default, 43
 checking, 216

PATH statement, 45

pathname
 selecting, 52
 selecting from form, 52

PC
 comparison of host and remote, 18
 connecting to a gateway, 60
 connecting to another PC, 60
 gateway setup, 79
 keyboard mapping, 257
 naming a, 20, 53
 set up as remote, 85

PC. *See also* host PC, remote PC
 pcANYWHERE. *See* Norton pcANYWHERE for
 DOS

PCAW.INI, 37

personal files
 changing to shared, 41, 43

phone. *See* telephone

pin configurations for cables, 247, 248

Play Back Saved Screens... option, 228

playback options, 22

Playback Sessions/Screen utility, 224

Playback Sessions/Screens utility, 215

port
 ACS, 70
 addressing, 239
 custom, 74
 definition of, 329
 selecting, 64
 Teletbit ACS, 71

port (*continued*)

- serial, 61, 63, 239
 - definition of, 332
 - Interrupt 14, 64

preferences

- changing for current session, 160
- Eliminate Snow, 55
- file transfer, 103
 - changing, 178
- file-transfer protocol, 112, 114
- gateway, 80
- general, 102
- host PC, 127
- mouse, 106, 170
- remote PC, 108
- security, 134
- setting, 22
 - for online service, 97
 - for remote PC, 97
- table of
 - host PC, 117
 - online sessions, 97
 - remote sessions, 97
- terminal emulation, 92
- video attributes, 108, 166, 167

prefix

- choosing, 90, 133
- definition of, 54, 329

Preprocess Scripts utility, 215

print device, 102

- changing, 162
- choosing, 203
- defining, 102

print spooler, 102

printer, 329

- defining, 102
- selecting, 102, 203

printing

- destination, 103, 162
 - changing, 162, 203
 - for log report, 236
- host only, 162
- log files, 236

printing (*continued*)

- options, 162
- remote only, 162
- reports, 236
- turning on/off, 203

PRN, 329

procedure. *See also* automated procedure

- Program Colors menu, 57
- Prompt on Connection option, 140
- Prompt Timeout option, 140

protocols

- ASCII, 112, 212, 320
- changing, 94, 212
- definition of, 315, 329
- KERMIT, 212
- NetBIOS, 327
- NetWare IPX, 327
- selecting, 212
- selecting preferences, 111
- XMODEM, 212
- X-ON/X-OFF, 335
- YMODEM, 212
- ZMODEM, 114, 212, 320

pulse dialing, 318, 329

Q

Quick Connect, 21, 151, 157, 199

- when to use, 199

quick start, 23

- over a LAN, 26
- via modems, 23

R

RAM

- checking for conflicts, 219
- requirement to run Norton
 - pcANYWHERE, 17
 - video, 215

reactivating

- gateway
 - after cancelation, 83
 - after reboot, 83

- reboot
 - host PC, 122, 136, 174
- Receive 2 CR's option, 329
- receiving files, 211
- Record file, 22
- recording
 - communications session, 22, 221
 - definition of, 330
 - turning on and off, 221
- redial
 - seconds to wait before, 331
- Redial Attempts option, 330
- refresh screen, 173
- Remote control
 - Windows, 307
- remote control
 - benefits of, 18
 - definition of, 18, 330
- remote control session, 160
 - automating, 185
 - chat mode, 161
 - configuration of, 21, 86
 - defining, 185
 - definition of, 143
 - ending, 163
 - with AWLOGOFF, 163
 - error
 - specifying action to take upon occurrence of, 189
 - file-transfer protocol, 320
 - host preferences, 128
 - inactivity timeout, 189
 - logging, 230
 - operations file, 190
 - starting from host PC, 146
 - starting from remote PC, 154
 - starting host PC, 144
 - starting remote PC, 154
 - suspending to return to DOS, 172
 - unattended, 143, 154, 194
 - voice first, 148
 - voice/data switch, 173
- remote control sessions
 - automating, 312
- Remote General Preferences, 102
- remote mouse, 170
- remote PC
 - accessing during session, 172
 - configuration of, 85
 - connect to host PC, 85
 - connect to online service, 85
 - contrasted to host PC, 18
 - default telephone number, 133
 - definition of, 18, 330
 - directory deletion on, 105, 180, 181
 - disabling screen display of, 165
 - file compression on, 105, 180
 - hotkey, 102, 322
 - log file, 230
 - log history file, 230
 - preferences, 97, 108, 160, 166, 170, 178
 - session options, 166
 - starting session, 154
- remote printing, 162
- remote user
 - change host mode, 123, 146
 - control specifications for host PC, 120
 - definition of, 18
 - password for, 121
 - session options, 166
- renaming
 - files, 182
 - hardware configuration, 75
 - options on menu, 52
- replay recorded communications sessions, 223
- reports
 - creating, 234
 - displaying, 236
 - format options for, 237
 - log file, 232
 - printing, 236
- request to send, 255, 330
- requirements
 - to run Norton pcANYWHERE, 17

resolution
 of graphics, 109, 167
 Retries option, 188
 Ring Indicator (RI) option, 316, 330
 rings, number of, 330
 rotary-style dialing, 329
 RS-232 standard
 cable, 246
 RS-232-C standards, 331
 definition of, 330
 RTS, 330
 RTS State option, 331
 RTS/CTS, 64, 245
 definition of, 331

S

saving
 recorded communications session, 226
 screen, 227
 from recorded communications
 session, 226
 scan interval, 134, 168
 scan, definition of, 331
 screen
 blanking, 122, 139, 146, 168
 capturing, 228
 checking video adapter type, 215
 clearing, 204
 copying to a file, 229
 disabling on remote, 165
 display of on remote PC, 166
 maximizing speed of updates, 129
 playback of, 228
 recording, 22
 refreshing, 173
 reviewing captured, 228
 saving, 226, 227
 snapshot of, 22, 228
 speed of updates, 38
 synchronization of displays of remote and
 host, 110, 111, 169
 translation of monochrome/color, 108,
 166, 167

screen (*continued*)
 updating image, 129, 134
 Screen file, 22
 Screen Wrap option, 93, 207
 script
 compilation of, 215
 definition of, 331
 use of to automate tasks, 22
 script language, 22
 script. *See also* automated procedure
 Seconds Between Redials option, 331
 Seconds to Wait after Dial option, 331
 security
 drive access, 30
 logging connection attempts, 232
 of drives, 125, 131, 319
 setting inactivity timeout, 322
 setting preferences for, 128, 134
 security. *See also* caller information
 selecting
 communications port, 63
 ACS, 70
 direct connection, 63
 Interrupt 14, 64
 modem, 61
 Telebit ACS, 71
 data rate, 63
 file-transfer protocol preferences, 111
 gateway, 80
 gateway options, 67
 modem, 62, 65
 NASI/NCSI device, 69
 network communications device, 67
 options from forms, 50
 printer, 102, 203
 protocol, 212
 recording file, 223
 versus choosing, 47, 50
 sending files, 212
 serial board, 240
 creating custom port for, 73
 serial communication
 definition of, 331

- serial connection
 - cable selection, 246
 - definition of, 19
 - RS-232 standard, 246
- serial hardware configuration
 - testing, 217
- serial interface
 - definition of, 331
- serial port, 61, 63, 239, 315
 - addressing, 239
 - definition of, 332
 - hardware configuration, 60
 - difference from network hardware configuration, 65
 - Interrupt 14, 64
 - interrupt handling, 241
 - number of, 215
 - use of for modem, 240
- server name, 43
- session, 332
- session configuration
 - changing, 87, 88, 204
 - creating reports for billing purposes, 233
 - definition of, 332
 - explanation of, 21
 - modifying, 87, 88
 - terminal settings, 204
 - what it does, 85
- Session Options menu, 143, 160, 186
- session. *See* communications session
- setting
 - host PC preferences, 134
 - remote PC preferences, 97
 - scan interval, 134
- sharing
 - caller information configuration file, 120
 - communications device, 77
 - modem, 79
 - network configuration file, 80
 - online session configuration file, 86
- signal state, 332
- signal, definition of, 332
- snow, 55, 219
 - definition of, 332
- software flow control (X-ON/X-OFF), 335
- software flow control (XON/XOFF), 246
- software handshake, 320, 321
- software requirements, 17
- space parity, 252
- Special Host Installation for Windows, 38
- Special Options
 - for host user, 164
 - for remote user, 166
- speed
 - computer, 254
 - data-transfer, 242
 - of screen update, 129
- spool file, 102, 203
- standard
 - installation
 - network, 42
 - PC, 36
 - installation network, 39
- start
 - gateway, 83
 - host PC, 144
 - host TSR, 144
 - remote operation, 154
 - remote PC, 154
 - session from host with a remote PC, 147
- start bit, definition of, 332
- status boxes, 48
- stop bit, definition of, 333
- suffix
 - choosing, 90, 133
 - definition of, 54, 333
- suspend session and connect to another host, 146, 163
- swap file, 111
 - definition of, 334
 - deleting, 111
- switched line, definition of, 333
- switches, modem, 243
- synchronized displays, 110, 111, 169
- synchronous transmission, definition of, 333

System Hardware... option, 61
 SYSTEM.INI, 37, 308
 backup file, 39

T

tagging files, 177, 178
 Telebit ACS, 65, 71, 333
 telephone
 callback number, 126
 choosing prefix/suffix, 90
 creation of prefix/suffix list, 55
 handset, 323
 leased line, 249
 number, 90
 default, 133
 entering manual modem settings, 244
 voice versus data communications, 242
 Televideo terminal emulation, 266, 268
 terminal emulation, 19, 197
 ADM 3A, 258
 ANSI, 260
 changing, 92
 on-line, 205
 definition of, 333
 DG 100/200, 260
 Hazeltine 1500, 264
 IBM, 264
 keyboard mapping, 257
 preferences, 92
 reference, 257
 specifying keyboard handler for, 131
 Televideo, 266, 268
 Viewpoint, 258
 VT 100/102/220, 270
 VT 52, 273
 Wyse, 275
 X3270, 278
 terminal mode, 333
 definition, 19
 terminal options, 201
 terminal settings, 204
 changing
 on-line, 204

terminal window, 48
 terminal, definition of, 333
 text
 wrapping, 92
 text files
 outputting log reports as, 236
 time and date of connection, 187
 Time Between Retries option, 188
 time limit for session, 124
 timeout, 138, 189
 after unanswered prompt, 140
 definition of, 334
 during downloading, 113
 inactivity, 123
 while entering password, 137, 138
 tone dialing, 318, 334
 transferring files. *See* file transfers
 translation table
 definition of, 334
 translation tables, 95, 209
 codes for, 280
 TSR. *See* host TSR

U

UART, 241
 16450, 241
 16550A, 241
 8250, 241
 unattended session, 143, 154, 194
 unidirectional gateway, 77, 78, 79, 323, 327
 definition of, 334
 setting up, 79
 specifying, 82
 uninstalling
 Norton pcANYWHERE for DOS, 44
 universal asynchronous receiver transmitter (UART), 241
 updating display of host screen, 129
 uploading files
 definition of, 334
 to online service, 212
 upper memory blocks, 29
 Use Gateway option, 334

user
 difference between host and remote, 18
 ID, 40

V

VGA
 support for, 29
 video adapter. *See also* screen
 video attributes
 changing, 56
 definition of, 312
 setting preferences, 108, 166, 167
 translating, 166
 video mode
 diagnostics, 22
 video RAM, 215
 viewing
 AUTOEXEC.BAT file, 217
 CONFIG.SYS file, 217
 screen snapshots, 228
 Viewpoint terminal emulation, 258
 voice communications, 242
 starting remote session with, 148
 switching from data, 173
 switching to data, 151
 Voice-First Connection option, 149, 151
 volume name, 43
 VT 100/102/220 terminal emulation, 270
 VT 52 terminal emulation, 273

W

wait
 after dial, 331
 before attempting a redial, 331
 Wait For A Call option, 150
 waiting mode, 144, 150, 197, 321
 remote, 156
 warm boot, 136
 warning boxes, 49
 WIN.INI, 38
 backup file, 39

Windows, 307, 309
 installation for, 37
 warning, 36
 swap file, 111
 definition of, 334
 Windows on host, 29
 WINHOST.EXE, 29, 38
 workstation
 installation on, 37
 workstation. *See also* node
 wrapping text, 92
 changing preference, 206, 207
 definition of, 334
 Wyse terminal emulation, 275

X

X3270 terminal emulation, 278
 XMODEM file-transfer protocols, 212
 X-ON/X-OFF, 331
 definition of, 335
 XON/XOFF, 246

Y

Yes/No menus, 49
 YMODEM file-transfer protocols, 212

Z

ZMODEM, 212
 error checking, 114
 file-transfer protocol, 114, 320