Remote Annex Server Tools for Windows NT®

User Guide

Part No. 166-025-305 Rev. A
January 1997

Bay Networks

Copyright © 1997 Bay Networks, Inc.

All rights reserved. Printed in the USA. April 1997.

The information in this document is subject to change without notice. The statements, configurations, technical data, and recommendations in this document are believed to be accurate and reliable, but are presented without express or implied warranty. Users must take full responsibility for their applications of any products specified in this document. The information in this document is proprietary to Bay Networks, Inc.

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

Restricted Rights Legend

Use, duplication, or disclosure by the United States 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.

Notice for All Other Executive Agencies

Notwithstanding any other license agreement that may pertain to, or accompany the delivery of, this computer software, the rights of the United States Government regarding its use, reproduction, and disclosure are as set forth in the Commercial Computer Software-Restricted Rights clause at FAR 52.227-19.

Trademarks of Bay Networks, Inc.

Annex, Remote Annex, Annex Manager, Remote Annex 2000, Remote Annex 4000, Remote Annex 6100, Remote Annex 6300, Remote Annex 5390/Async, Remote Annex 5391/CT1, Remote Annex 5393/PRI, Remote Access Concentrator 5399,BayStack Remote Annex 2000 Server, Quick2Config, Bay Networks, Bay Networks Press, and the Bay Networks logo are trademarks of Bay Networks, Inc.

Third Party Trademarks

All other trademarks and registered trademarks are the property of their respective owners.

Statement of Conditions

In the interest of improving internal design, operational function, and/or reliability, Bay Networks, Inc. reserves the right to make changes to the products described in this document without notice.

Bay Networks, Inc. does not assume any liability that may occur due to the use or application of the product(s) or circuit layout(s) described herein.

In addition, the program and information contained herein are licensed only pursuant to a license agreement that contains restrictions on use and disclosure (that may incorporate by reference certain limitations and notices imposed by third parties).

Revision Level History

Revision	Description
A	Initial release.

Contents

Preface

Chapter 1
Introduction

Chapter 2
Selecting Server Tools Options

Chapter 3
Understanding Erpcd

Chapter 4
Using Security Features

Appendix A
Browsing for Resources on a Microsoft Network

Preface

Remote Annex Server Tools for Windows NT® allows you to boot, configure, and manage Remote Annexes on a Windows NT® network. It performs user authentication and authorization from a Windows NT® network and supports:

- Remote Annex 2000
- Remote Annex 4000
- Remote Annex 6100 and 6300
- 5390, 5391, 5393
- 5399 Remote Access Concentrator (RAC) Module
- MicroCS
- Cabletron CSMIMII
- 3COM 6133C-XS
- 3COM 6117C-XS

The *Remote Annex Server Tools for Windows NT® User Guide* is intended for System Administrators or others who need to configure Remote Annex servers. It assumes that you are familiar with network protocols and that you know the parameter values needed to configure Remote Annexes.

This guide is part of the complete Remote Annex documentation set. You should refer to other manuals in the set for information not related to Remote Annex Server Tools for Windows NT®.

About This Book

This book documents Remote Annex Server Tools for Windows NT®. It explains the product's features and provides instructions for each of those features.

The *Remote Annex Server Tools for Windows NT® User Guide* includes the following chapters:

- *Chapter 1, Introduction,* provides an overview of Remote Annex Server Tools for Windows NT® features. For existing customers migrating to the Windows NT® environment, this chapter compares and contrasts several features and behaviors that were ported from UNIX. This chapter also lists minimum system requirements.
- Chapter 2, *Selecting Server Tools Options*, describes Windows NT® Server security options, and tells you how to set Remote Annex security parameters.
- Chapter 3, *Understanding Erpcd*, discusses the role of the **e**xpedited **r**emote **p**rocedure **c**all **d**aemon (or **erpcd**). **Erpcd** is a Remote Annex software sub-system that receives and responds to all Remote Annex boot, dump, and ACP security requests.
- Chapter 4, *Using Security Features*, discusses Windows NT® Server security and host-based network security.
- Appendix A, *Browsing for Resources on a Microsoft Network,* describes Microsoft client setup for locating resources on a Microsoft network.

Documentation Conventions

The following table lists the *Remote Annex Server Tools for Windows NT*® *User Guide* conventions:

Convention:	Represents:
Italics	chapter titles, book titles, and chapter headings.
`special type`	defines samples in the na utility.
bold	path names, program names, field names, or file names.
▼	one-step procedures.
✎	important information.
❗	conditions that can have adverse effects on processing.
⚡	dangerous conditions.

Chapter 1
Introduction

Remote Annex Server Tools for Windows NT® allows you to boot and configure Remote Annexes and 5399 Remote Access Concentrator (RAC) Module(s) on a Windows NT® network. You can manage one or more Remote Annexes using the **na** utility. In addition, the product takes advantage of Windows NT® domains to authenticate and authorize users.

NA Utility Features

The **na** utility is a command-line interface that lets you monitor and modify Remote Annex and 5399 RAC operating characteristics. It allows you to:

- Boot a Remote Annex/5399 RAC.
- Reset a Remote Annex/5399 RAC.
- Identify a Remote Annex/5399 RAC by its Internet address or host name.
- Set and show values for all Remote Annex/5399 RAC configuration parameters.
- Save current configuration parameter settings into script files.
- Copy the current configuration parameters from one port to another or from one Remote Annex/5399 RAC to another.
- Create new site defaults.

For the remainder of this manual, the term ‘Remote Annex’ is substituted for *Model 5399 Remote Access Concentrator Module*.

Windows NT® Server Access Security Features

Remote Annex Server Tools for Windows NT® works with a Windows NT® Server to provide access security. You define user and group access parameters in Windows NT®, and link the appropriate group definitions with the Remote Annex using the Server Tools Options graphical user interface.

Remote Annex Server Tools for Windows NT® allows you access to the standard Remote Annex log file, a RADIUS server log file, and the Windows NT® Event Log.

Using Remote Annex Documentation

In addition to this manual, you need the *Remote Annex Administrator's Guide for UNIX* or the *Module 5399 Remote Access Concentrator Network Administrator's Guide* and the *Remote Annex 6300 Supplement to the Remote Annex Administrator's Guide for UNIX* . These guides provide reference, procedure, and feature descriptions for the Remote Annexes in a UNIX environment.

Be aware that minor differences exist between Windows NT®-based **erpcd** and UNIX-based **erpcd**. This section lists these issues, and guides you to the appropriate manuals.

User Authentication Issues

Remote Annex Server Tools for Windows NT® takes full advantage of Windows NT® Server user authentication and authorization. Logon and remote dial-in events trigger security services from Windows NT®. For information about Remote Annex Server Tools for Windows NT® user authentication, see Chapter 2, Chapter 3, and Chapter 4 in this guide.

Name Server Issues

Remote Annex Server Tools for Windows NT® supports DNS and IEN-116 name servers. We do not ship IEN-116 for Windows NT®. For more information, see the *Remote Annex Administrator's Guide for UNIX*. Be aware that IEN-116 discussions do not apply to Remote Annex Server Tools for Windows NT®.

Logging Issues

Besides the standard Annex log destinations, you can configure Remote Annex Server Tools for Windows NT® to send Syslog and ACP log messages to the Windows NT® Event Log. See Chapter 3 in this guide for details. For additional logging information, refer to the numerous chapters in the *Remote Annex Administrator's Guide for UNIX* or the *Module 5399 Remote Access Concentrator Network Administrator's Guide* and the *Remote Annex 6300 Supplement to the Remote Annex Administrator's Guide for UNIX*.

Documentation Exceptions

Some information in the *Remote Annex Administrator's Guide for UNIX* and the *Module 5399 Remote Access Concentrator Network Administrator's Guide* does not apply to Remote Annex Server Tools for Windows NT®, due to innate differences between Windows NT® and UNIX environments. Certain UNIX-based Annex features are not implemented in Remote Annex Server Tools for Windows NT®. Use the following table as a guide to documentation that does not apply to Remote Annex Server Tools for Windows NT®.

Book/Chapter	Topic
A /1	UNIX Host-Originated Connections
A /2	Using the Terminal Server TTY (TSTTY)
	Using the Transport Multiplexing (TMux) Protocol
A /4	Terminal Server TTY
	How TSTTY Interacts with Annex Port Parameters
	Configuring the Annex for TSTTY
	Transport Multiplexing Protocol (TMux)
	tip and uucp
	getty
A /13	Printing from a BSD Host using aprint or rtelnet
	Printing from a System V Host using aprint or rtelnet
A /14	Installing Software Using bfs
	IEN-116 Name Server
	Setting Up a Host for 4.3BSD Syslogging
A /15	Configuring the acp_regime file
	Creating User Password Files
	Limiting Access to Hosts via acp_restrict
	Overview of Password History and Aging
	Enabling and Configuring Password Histories
	Overview of Blacklisting
	Viewing and Managing the acp_dbm Database
	Security for NDP Ports
	Using Kerberos Authentication
	Modifying the Supplied Security Application
	Using the ch_password Utility

(continued on next page)

Book/Chapter	Topic
B /2	TMux-Specific Annex Parameters vs. MIB Objects
C /4	aprint
	rtelnet

Platform Requirements

Remote Annex Server Tools for Windows NT® requires:

- Windows NT® Server version 3.51 or 4.0 configured to support the TCP/IP protocol.
- Administrative privileges on the server.
- 15 MB free disk space on an NTFS drive.
- One Windows NT® Server client license per Annex.
- A PC with an Intel Pentium (or higher) CPU, or any fully compatible CPU.
- 32 MB RAM.
- CD ROM drive to install the product.

Document References

Refer to the following document sets for additional information on the desired subjects. The topics from all three books share the same chapter contents (with the exceptions noted after the book titles below).

- *Remote Annex Adminstator's Guide to UNIX* (for *port numbers as profile attributes*)
- *Model 5399 Remote Access Concentrator Network Administrator's Guide* (for *port types as profile attributes*)
- *Remote Annex 6300 Supplement to Remote Annex Administrator's Guide to UNIX* (for *port types as profile attributes*)

Topic	Chapter
erpcd	A- 4
acp_userinfo	A-15
acp_keys	A-15
acp_dialup	A-15
na utility	C-1
CLI commands	C-3
port numbers as profile attributes	A-15
port types as profile attributes	A-15
parameter values	C-2
ACE/Server software	A-15
security types	A-15
backup security	A-15

Chapter 2
Selecting Server Tools Options

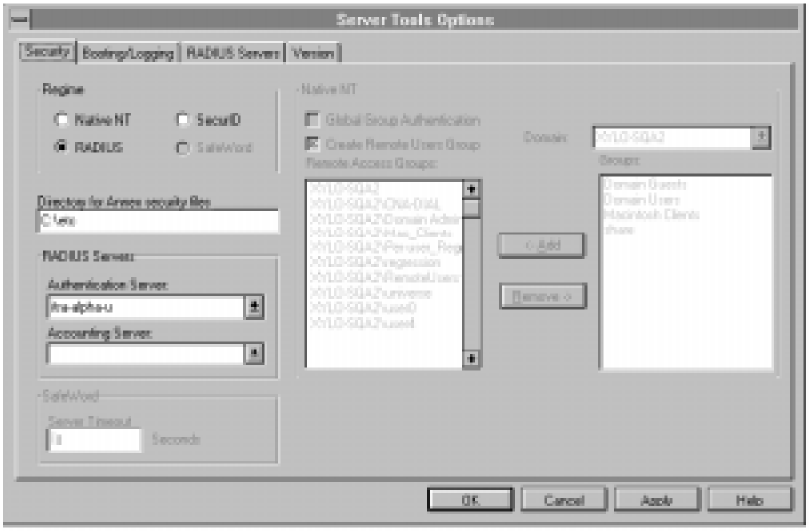
The **Server Tools Options** window appears after you complete the installation process. Double-click on the **Options** icon in the Bay Networks program group window. The **Server Tools Options** window has four tabbed dialog boxes that allow you to select a security server, select booting and logging options, choose and configure a RADIUS server, and view information about your current Remote Annex Server Tools for Windows NT® software version. This chapter includes:

- *Selecting a Security Server and Group Authentication*
- *Selecting Booting/Logging Options*
- *Configuring a RADIUS Server*
- *Displaying Version Information*

Selecting a Security Server

The **Security** tab dialog box allows you to choose a security regime, select RADIUS Authentication and Accounting servers, and add or remove domains and remote access groups.

▼ To view this information, click the **Security** tab on the **Server Tools Options** window (Figure 2-1 on page 2-2 illustrates the **Server Tools Options** dialog box).



Regime

○ Native NT ○ SecurID

● RADIUS ○ SafeWord

Directory for Annex security files: C:\etc

RADIUS Servers

Authentication Server: fra-alpha-u

Accounting Server:

☐ Global Group Authentication

☑ Create Remote Users Group

Domain: XYLO-SQA2

XYLO-SQA2
XYLO-SQA2\CNA-DIAL
XYLO-SQA2\Domain Admin
XYLO-SQA2\Mac_Clients
XYLO-SQA2\Persvses_Reg
XYLO-SQA2\vegession
XYLO-SQA2\RemoteUsers
XYLO-SQA2\universe
XYLO-SQA2\user0
XYLO-SQA2\user4

Domain Guests
Domain Users
Macintosh Clients
share

Figure 2-1. The Server Tools Options Dialog Box

To select options in the **Security** window:

Specify a Regime

Select the protocol you desire from the **Regime** radio box.

- Native NT (default selection)
- RADIUS Security
- SecurID

Native NT Security

1. If you select Native NT in the Regime radio box, the **Directory for Annex security files** field becomes active. Accept the default or enter a new destination drive and directory for the acp_logfile file.

   This field designates the drive on which you installed Remote Annex Server Tools for Windows NT® and the **etc** directory, where the system stores the **acp_dialup**, **acp_keys**, and **acp_userinfo** files.

2. If you select **Native NT** as your security protocol, click the **Global Group Authentication** check box.

   You must select this box if you want to use Windows NT® global groups to authenticate users. If you do not select it, the system will authenticate user names and passwords only.

3. If you select **Native NT** and want to create a default remote users group, click the **Create Remote Users Group** check box.

   If you want to create a new Remote Users Group, see *RADIUS Security* on page 2-4

4. If you select **Native NT**, choose an existing domain from the **Domain** field.

   When you choose a domain, the groups within that domain appear in the **Groups** list box.

5. If you select **Native NT**, choose a name from the **Groups** list box.

6. Click **Add** to move the group(s) you select to the **Remote Access Groups** list box.

   The groups you add appear in the **Remote Access Groups** list box preceded by their domain names. All users in these groups will be allowed access once Windows NT® domain security authenticates them. Any users who are not members of the groups listed here will not have access to the Remote Annexes, their ports, or networks.

You can double-click on a group name from the **Remote Access Groups** list, to move it to the **Groups** list. If you want to change your selections, highlight the group from the **Groups** list box and click on **Remove**, or double-click the group name.

If you install Remote Annex Server Tools for Windows NT® on a primary domain controller, the groups you select here must have local log on privileges to allow authentication. For more information about this privilege, refer to *Installing Remote Annex Network Software for NT®* included with your documentation set.

RADIUS Security

▼ If you select **RADIUS** as your security protocol, select the **Authentication Server** and **Accounting Server** in the **RADIUS Servers** list box.

If the only options available in these two drop–down lists are **local** and **same as authentication server** you need to create a list of servers from which to choose. For more information on this procedure, see *Configuring a RADIUS Server* on page 2-13. Additional information regarding RADIUS security can be found in Chapter 4.

Third Party Security

1. If you are using external software security **SecurID**, click the **SecurID** Regime radio box selection, and all of the fields become dimmed.
2. When you have completed your Security setup, click on OK to set the changes you made and close the dialog box.
3. Click on Cancel to close the dialog box without saving or applying your changes.
4. Click on Apply to set your changes and leave the **Server Tools Options** window open on your desktop. Use this option if you want to make changes in any of the other tabbed dialogs.

You can add or remove a new **Remote Users Group** (on the **Security** tab window) within the **Server Tools Options** application. However, unless this new group already exists, you must first create the new group and its information via the Windows NT® operating system.

▼ To add a new default group, click the **Create Remote Users Group** check box.

Remote Users Group appears automatically in the **Remote Access Groups** list. If you find you do not need the group, you can delete it before you click on **OK** or **Apply** by selecting it and clicking on **Remove,** or by deselecting the **Create Remote Users Group** check box.

To create a new Group:

1. Click on the **Administrative Tools** icon in the Windows NT® program group window.

   The Administrative Tools window appears.

2. Click on the **User Manager for Domains** icon.

   The User Manager for Domains dialog box appears.

3. Add the new Group and associated information.

   For more information, see the Windows NT® documentation on using the options in this window.

4. When you have completed adding your Group information, click on the **Security** tab in the **Server Tools Options** window.

   The Security dialog box opens.

5. Click on the **Domain** pull–down menu.

   The list boxes **Groups** and **Remote Access Groups** become active and list the group(s) you created in the above steps.

6. Select the newly created Group from the **Groups** list box and click on **Add.**

   The selected group appears in the Remote Access Groups list box.

7. When you have completed your changes, click on **OK** to set the changes you made and close the dialog box.

   Click on **Cancel** to close the dialog box without saving or applying your changes.

   Click on **Apply** to set your changes and leave the **Server Tools Options** window open on your desktop. Use this option if you want to make changes in any of the other tabbed dialogs.

Creating a RADIUS Authentication and Accounting Server

To create a RADIUS Authentication or Accounting server:

1. From the **Server Tools Options** window, click on the **RADIUS Servers** tab.

   The RADIUS Servers dialog box opens.

2. Click on **New.**

   All information fields become active.

3. Enter the **Host Name** of the RADIUS server to be created.

4. Tab to the **IP Address** text field and enter the **IP Address** that goes with the **Host Name.**

   Repeat step 4 to configure the **Secret** format, the **Timeout** period, and the number of **Retries** (for more details on Secret, Timeout, and Retries, see Chapter 4).

5. Click on **Accept** to apply the new server information or **Revert** to cancel your changes.

   You can modify any of the fields before you click on **Accept** or **Revert**. After Accept or Revert is chosen, the fields become inactive. To reactivate (for editing) these fields, select the server, then choose **Modify**.

6. Click on **OK** to save your changes and close the dialog box.

   Click on **Cancel** to close the dialog box without saving or applying your changes.

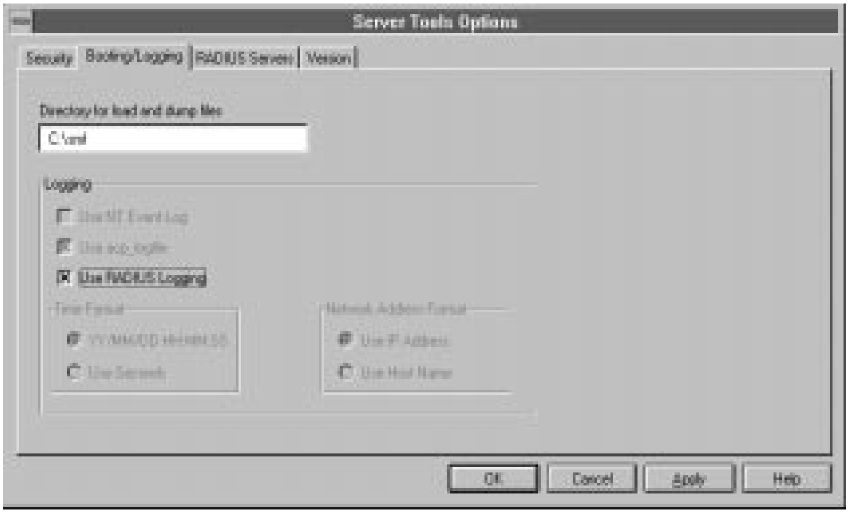
   Click on **Apply** to set your changes, and leave the **Server Tools Options** window open on your desktop. Use this option if you want to make changes in any of the other tabbed dialogs.

Before you select a Backup Server, you must create more than one new RADIUS server. When you create a second RADIUS server, the first RADIUS server then appears in the Backup Server drop–down list.

Selecting Booting/Logging Options

The **Booting/Logging** tab window allows you to select log files, to choose locations for load and dump files, and to choose directories, time formats and network address formats for the log file.

▼ To display this window, choose the **Booting/Logging** tab in the **Server Tools Options** window.



Directory for load and dump files: C:\xml

Logging

☐ Use NT Event Log

☑ Use acp_logfile

☒ Use RADIUS Logging

Time Format

● YY/MM/DD HH:MM:SS

○ Use Seconds

Network Address Format

● Use IP Address

○ Use Host Name

If you select **Use NT Event Log,** your settings for time and network address formats appear in the **acp_logfile** and in the **Detail** window of the NT® Event Log.

To select options in the **Booting/Logging** window:

1. In the **Directory for load and dump files** field, you can accept the default or enter a drive and directory for the Remote Annex system images and dump files.

   This field automatically lists the drive on which the Remote Annex Server Tools for Windows NT® is installed, and the **bfs** default directory, where the system stores load and dump files.

   If you enter a new directory, use the File Manager to move the Remote Annex software images to the new directory. If you do not move the images to the new directory, the Remote Annexes will be unable to boot.

2. Click either **Use NT Event Log, Use acp_logfile,** or **Use RADIUS Logging** to choose a method for storing log messages.

   You can log Remote Annex syslog messages, and **erpcd** or **RADIUS** security messages.

   - If you select **Use NT Event Log**, the system stores messages in the **Applications** portion of the standard Windows NT® Event Log.
   - If you select **Use acp_log file**, the system stores messages in the **acp_logfile** in the chosen directory in the **Security** dialog box. You can view the **acp_logfile** by double-clicking on the **acp_logfile** icon in the Bay Networks program group window.
   - If you select **Use RADIUS logging,** the system sends messages in the RADIUS server**.**

   RADIUS logging is not available (grayed–out) unless you select the RADIUS security regime from the Security dialog box.

3. If you select **Use acp_logfile** in the Booting/Logging dialog box, specify a time listings format, in the Time Format box.

   You can choose:

   - **YY/MM/DD HH:MM:SS** to display the date and time that an event occurred (e.g., 95/12/30 06:22:15).
   - **Use Seconds** to list time in seconds since January 1, 1970.

4. If you select **Use acp_logfile** or **NT Event Log** from the Booting/Logging dialog box, select an IP address or Host Name format from the **Network Address Format** box.

   You can choose:

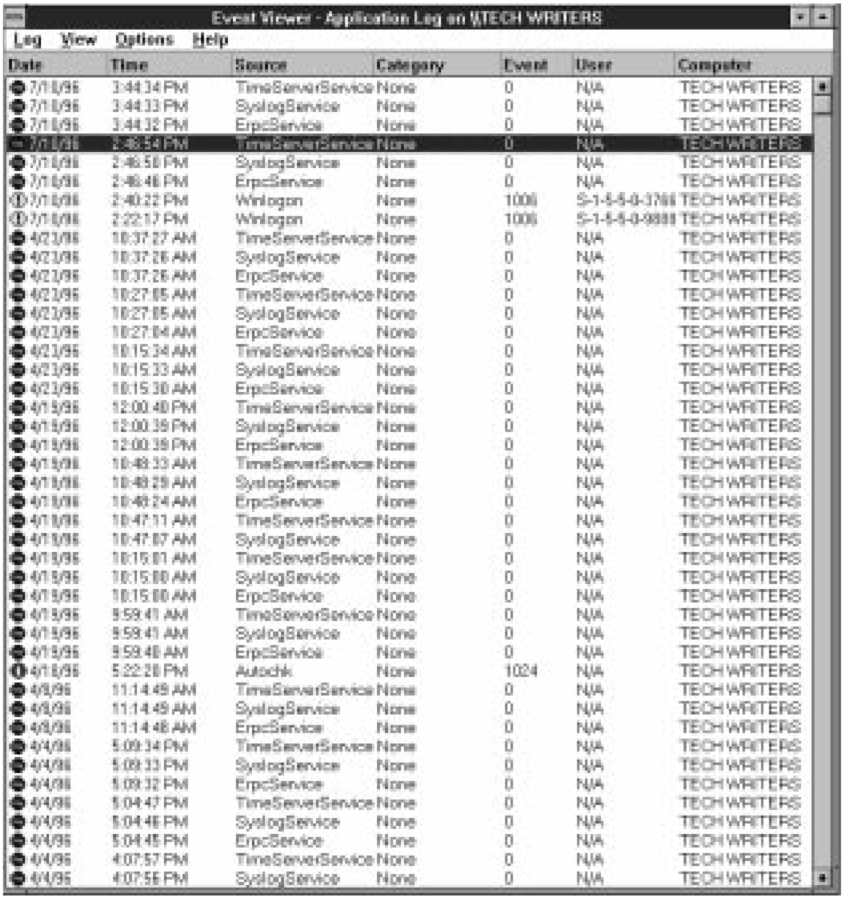
   - **Use IP Address** to place the Internet address of a Remote Annex that generates logging messages in the log files.
   - **Use Host Name** to include a Remote Annex name in the log files instead of the Remote Annex's Internet address.

The time and address formats you chose appear in the **acp_logfile** or **RADIUS logging**. If you chose **Use NT Event Log**, the format appears in the **Detail** window of the NT Event Log.

Using the Event Viewer

Remote Annex Server Tools for Windows NT® uses the standard Windows NT® Event Viewer. If you select **Use NT Event Log** from the **Booting/Logging** dialog box, the Windows NT® **Application** Event Log includes syslog and security messages.

▼ To view Windows NT® logs, double-click on the **Event Viewer** icon in **Administrative Tools** and select **Application** from the **Log** menu.



Date	Time	Source	Category	Event	User	Computer
7/10/96	3:44:34 PM	TimeServerService	None	0	N/A	TECH WRITERS
7/10/96	3:44:33 PM	SyslogService	None	0	N/A	TECH WRITERS
7/10/96	3:44:32 PM	ErpcService	None	0	N/A	TECH WRITERS
7/10/96	2:48:54 PM	TimeServerService	None	0	N/A	TECH WRITERS
7/10/96	2:46:50 PM	SyslogService	None	0	N/A	TECH WRITERS
7/10/96	2:46:46 PM	ErpcService	None	0	N/A	TECH WRITERS
7/10/96	2:40:22 PM	Winlogon	None	1006	S-1-5-5-0-3788	TECH WRITERS
7/10/96	2:22:17 PM	Winlogon	None	1006	S-1-5-5-0-9888	TECH WRITERS
4/23/96	10:37:27 AM	TimeServerService	None	0	N/A	TECH WRITERS
4/23/96	10:37:26 AM	SyslogService	None	0	N/A	TECH WRITERS
4/23/96	10:37:26 AM	ErpcService	None	0	N/A	TECH WRITERS
4/23/96	10:27:05 AM	TimeServerService	None	0	N/A	TECH WRITERS
4/23/96	10:27:05 AM	SyslogService	None	0	N/A	TECH WRITERS
4/23/96	10:27:04 AM	ErpcService	None	0	N/A	TECH WRITERS
4/23/96	10:15:34 AM	TimeServerService	None	0	N/A	TECH WRITERS
4/23/96	10:15:33 AM	SyslogService	None	0	N/A	TECH WRITERS
4/23/96	10:15:30 AM	ErpcService	None	0	N/A	TECH WRITERS
4/19/96	12:00:40 PM	TimeServerService	None	0	N/A	TECH WRITERS
4/19/96	12:00:39 PM	SyslogService	None	0	N/A	TECH WRITERS
4/19/96	12:00:39 PM	ErpcService	None	0	N/A	TECH WRITERS
4/18/96	10:48:33 AM	TimeServerService	None	0	N/A	TECH WRITERS
4/18/96	10:48:29 AM	SyslogService	None	0	N/A	TECH WRITERS
4/18/96	10:48:24 AM	ErpcService	None	0	N/A	TECH WRITERS
4/18/96	10:47:11 AM	TimeServerService	None	0	N/A	TECH WRITERS
4/18/96	10:47:07 AM	SyslogService	None	0	N/A	TECH WRITERS
4/15/96	10:15:01 AM	TimeServerService	None	0	N/A	TECH WRITERS
4/15/96	10:15:00 AM	SyslogService	None	0	N/A	TECH WRITERS
4/15/96	10:15:00 AM	ErpcService	None	0	N/A	TECH WRITERS
4/15/96	9:59:41 AM	TimeServerService	None	0	N/A	TECH WRITERS
4/15/96	9:59:41 AM	SyslogService	None	0	N/A	TECH WRITERS
4/15/96	9:59:40 AM	ErpcService	None	0	N/A	TECH WRITERS
4/10/96	5:22:28 PM	Autochk	None	1024	N/A	TECH WRITERS
4/8/96	11:14:49 AM	TimeServerService	None	0	N/A	TECH WRITERS
4/8/96	11:14:49 AM	SyslogService	None	0	N/A	TECH WRITERS
4/8/96	11:14:48 AM	ErpcService	None	0	N/A	TECH WRITERS
4/4/96	5:09:34 PM	TimeServerService	None	0	N/A	TECH WRITERS
4/4/96	5:09:33 PM	SyslogService	None	0	N/A	TECH WRITERS
4/4/96	5:09:32 PM	ErpcService	None	0	N/A	TECH WRITERS
4/4/96	5:04:47 PM	TimeServerService	None	0	N/A	TECH WRITERS
4/4/96	5:04:46 PM	SyslogService	None	0	N/A	TECH WRITERS
4/4/96	5:04:45 PM	ErpcService	None	0	N/A	TECH WRITERS
4/4/96	4:07:57 PM	TimeServerService	None	0	N/A	TECH WRITERS
4/4/96	4:07:56 PM	SyslogService	None	0	N/A	TECH WRITERS

Figure 2-2

The Windows NT® Event Log stores information in the following columns:

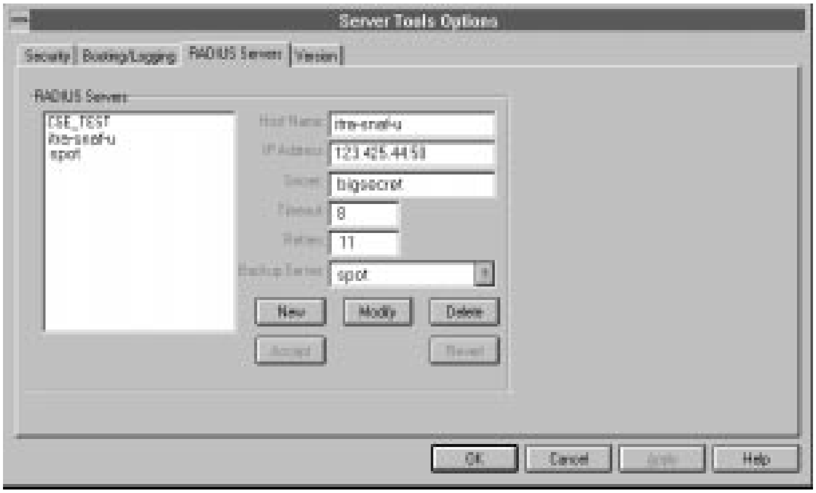
- An **icon** at the beginning of each line indicates the severity of the message**.**
- **Date** stores the date that the event was logged in Windows NT®.
- **Time** stores the time that the event was logged into Windows NT®. The**Detail** window of the Event Log lists the times events occur.
- **Source** lists the software that logged the event.
  - For syslog messages from a Remote Annex or from the network, `Annex_syslog` appears.
  - For messages generated by **erpcd**, the column displays `Annex_syslog`.
  - For security messages, the log entry reads `Annex_ACP`.
- **Category** classifies events.
- **Event** displays the event number (the Remote Annex generates a number to identify each event).
- **User** displays `N/A`. Remote Annex Server Tools for Windows NT® does not use this column.
- **Computer** displays the name of the host on which **erpcd** is installed.

You can view the **Detail** window of the Event Log by double-clicking on any line in the Windows NT® Event Log.

Configuring a RADIUS Server

The **RADIUS Servers** tab dialog box allows you to create, modify, delete and configure a RADIUS server, and to set the IP Address and Secret format parameters.

▼ To view this information, click on the **RADIUS Servers** tab of the **Server Tools Options** window.



RADIUS Servers
CSE_TEST
rtra-snafu
spot

Host Name: rtra-snafu
IP Address: 123.425.44.50
Secret: bigsecret
Timeout: 8
Retries: 11
Backup Server: spot

Figure 2-3 The Radius Servers Dialog Box

First Time Use

When you open the **RADIUS Servers** dialog box for the first time (after installation), the information fields are blank and inactive. You need to create and configure the RADIUS servers that you will be using. Use the following procedures to create, configure, modify, and delete your RADIUS servers and associated parameters.

Creating and Configuring a RADIUS Server

To create and configure a new RADIUS Server:

1. Click on **New**.

   All information fields become active.

2. Enter the **Host Name** of the RADIUS Server you are creating in the text field.

3. Tab to the **IP Address** text field and enter the IP address of the **Host Name**.

4. Repeat step 3 to configure the **Secret** format, the **Timeout** period, and the number of **Retries**.

5. Click on **Accept** to apply the new server information, or **Revert** to cancel your changes.

   You can modify any of the fields before you click on **Accept** or **Revert**. After Accept or Revert is chosen, the fields become inactive. To reactivate (for editing) these fields, select the server, then choose **Modify**.

6. Click **OK** to save your changes and close the **Server Tools** Options window.

   Click on **Cancel** to close the dialog box without saving or applying your changes.

   Click on **Apply** to set your changes, and leave the **Server Tools Options** window open on your desktop. Use this option if you want to make changes in any of the other tabbed dialogs.

Before you can select a Backup Server, you must create more than one new RADIUS servers. When you create a second RADIUS server, the first RADIUS server then appears in the Backup Server drop-down list.

Modifying RADIUS Server Information

1. Select a desired RADIUS server from the **RADIUS Servers** list box.

When you select a RADIUS server, the information fields on the right side of the dialog box automatically fill in with the appropriate information pertaining to the RADIUS server you chose. Click on **Modify**.

All information text fields become active, except the Host name.

2. Place your cursor in the information field you wish to change, and enter the new information.

3. Click on **Accept** to save the modified information or **Revert** to cancel your changes.

You can modify any of the fields before you click on **Accept** or **Revert**. After Accept or Revert is chosen, the fields become inactive. To reactivate these fields, select the server, then choose **Modify**.

4. Click **OK** to save your changes and close the **Server Tools Options** window.

Click on **Cancel** to close the dialog box without saving or applying your changes.

Click on **Apply** to set your changes and leave the **Server Tools Options** window open on your desktop. Use this option if you want to make changes in any of the other tabbed dialogs.

Deleting RADIUS Server Information

1. Select the RADIUS Server to be deleted and click on **Delete.**

All information text fields remain inactive and a confirmation dialog box appears.

2. Click **OK** to delete the RADIUS Server or **Cancel** to exit the confirmation dialog box without deleting any server information.

The confirmation dialog box closes.

3. Click **OK** to save your changes and close the **Server Tools Options** window.

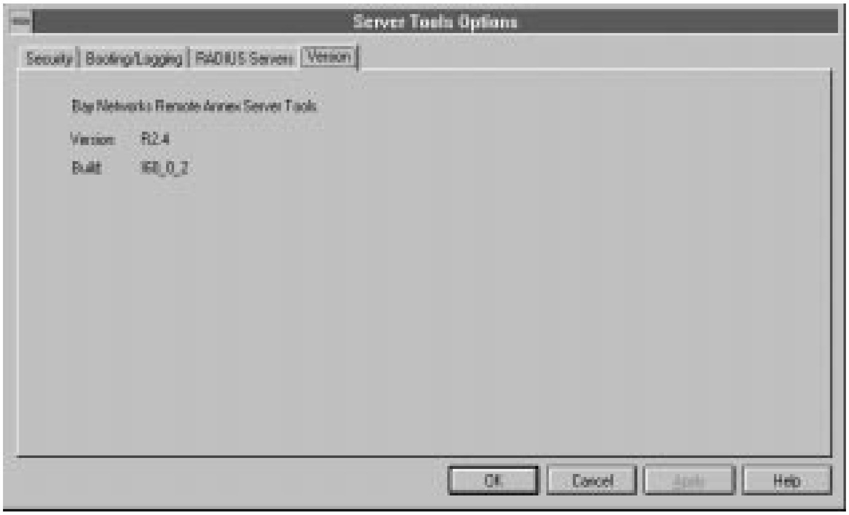
Click on **Cancel** to close the dialog box without saving or applying your changes.

Click on **Apply** to set your changes and leave the **Server Tools Options** window open on your desktop. Use this option if you want to make changes in any of the other tabbed dialogs.

Displaying Version Information

The **Version** tab window provides the company and product name, version number, and build number for the Remote Annex Server Tools for Windows NT®.

▼ To view this information, click on the **Version** tab of the **Server Tools Options** window.



Bay Networks Remote Annex Server Tools

Version: R2.4

Built: 168_0_2

Figure 2-4 The Version Dialog Box

Chapter 3
Understanding Erpcd

Remote Annex Server Tools for Windows NT®uses the **e**xpedited **r**emote **p**rocedure **c**all **d**aemon (**erpcd**) running on a Windows NT® server. **Erpcd** responds to all Remote Annex boot, dump, and ACP security requests. ACP's **eservices** file, stored in the **\etc** directory, lists the services that **erpcd** provides. **Eservices** includes controls for:

- The block file server (**bfs**) program sends boot files to a Remote Annex and collects dump files from a Remote Annex.
- The Access Control Protocol (**ACP**) program provides security when you define a Windows NT® server as a security server.

See *Document References* on page -6 to find sources of additional information about **erpcd**, the **acp_userinfo**, **acp_keys**, and **acp_dialup** files. The Remote Annex Server Tools implements erpcd differently, because it uses Windows NT domain authentication.

This chapter describes the files you can edit. It includes:

- *Editing Files*
- *Using the acp_userinfo File*
- *Using the acp_keys File*
- *Using the acp_dialup File*

Editing Files

You can edit the **acp_userinfo**, **acp_dialup**, and **acp_keys** files from the Bay Networks program group window. There is an icon for each file in the program group window.

▼ To open an individual file, such as the **acp_userinfo** file, from the Bay Networks program group window, double-click on the respective icon and the file will open in the Windows NT® Notepad editor.

The changes take effect immediately. User names and group names are not case-sensitive.

Using the acp_userinfo File

The **acp_userinfo** file stores information about the Remote Annex commands and protocols available to users. When a user logs into the server, **erpcd** matches the login environment with **acp_userinfo** entries, and controls user access based on these entries.

Defining User Profiles

Defining user profiles is useful only when you want to restrict user privileges for remote access connections.

Network access is controlled by the **acp_userinfo** file, based on user login environments. When you create a profile, **erpcd** authenticates users and attempts to match the user name with an entry from the **acp_userinfo** file. If a profile matches the login environment, **erpcd** downloads attribute information.

For example, if a user who belongs to the Engineering group requests access to a Remote Annex port on Monday morning at 10 a.m. and a profile excludes Engineering group members from using that Remote Annex on Mondays between 9 and 11 a.m., the user cannot log in to the port. In this case, Remote Annex Server Tools for Windows NT® authenticates the user's Windows NT® name and password, matches the current environment (the Remote Annex, port, day and time) to an entry in **acp_userinfo**, and downloads instructions (or attributes) so that the Remote Annex denies access to the user.

For detailed information about profiles and examples (using the **na** utility), please refer to *Document References* on page 1-6. Some terminology differs from this book, but keyword and attribute names and formats are identical in function.

User Profile Formats

The **acp_userinfo** file stores user profiles in the **user...end** block format. This format includes:

- `User` to begin the block.
- One or more keywords that specify the user environment. Entries must contain:
  - A keyword, an equal sign (=) and a value, without spaces. For an explanation of these keywords, refer to *User Environment Keywords* later in this chapter.
  - A semicolon (;) to separate keyword/value statements.
  - A backslash (\) at the end of a line if you continue the entry on a second line.

You cannot use each keyword more than once in any user profile. A line cannot exceed 80 characters.You cannot include spaces on either side of the equal sign, the semicolon, or within the value, except in a value for time.

- The attributes that **erpcd** applies when all user profile elements match the login environment of the user.
- `end` to conclude the profile.

The **acp_userinfo** file can include as many user profiles as you need. The matching process requires that all elements in a user profile match the login environment of the user.

Using Profile Environment Keywords

User profiles contain one or more keywords that define user login conditions. **Erpcd** matches these conditions to environment conditions listed in a user profile.

Since **erpcd** uses the first profile it finds that matches the login environment of a user, you need to specify profiles in the order you want them to match.

Username and Group Keywords

The **username** keyword specifies a single Windows NT® user. The **group** keyword allows you to create a user profile for any member of a Windows NT® group.

▼ To use these keywords, enter `username=` or `group=` followed by a user or group name.

If you do not enter a user or group name, the profile applies to all users. Use an asterisk as a wildcard following a partial name,or an asterisk alone to indicate that the profile applies for all users or group members who meet the criteria.

If you do not enter a domain name, **erpcd** assumes the user is registered in the domain in which Remote Annex Server Tools for Windows NT® is installed. If you create a profile for a user or group in a different domain, you must enter the domain name, two backslashes, and the user or group name (e.g., `Marketing\\Russell`).

time Keyword

The **time** keyword defines a period of time during which profile attributes apply.

▼ To use this keyword, type `time=` followed by one or more of the following:

- A day of the week (e.g., `Thursday`).
- A specific date, including the month and the date (e.g., `March 1`).
- A range of hours in **hh:mm** format (e.g., `06:30`). You must enter start time and end time. You can enter `a.m.` or `p.m.` following the times.

If you do not enter a day and/or a date, **erpcd** applies the start and end time every day of the week. If you omit `a.m.` or `p.m.`, the time defaults to the 24-hour format.

protocol Keyword

The **protocol** keyword defines a protocol by which a user can connect to a Remote Annex.

▼ To define a protocol, type `protocol=` followed by **`slip`**, **ppp**, or **`cli`**.

You cannot enter more than one protocol on a line. However, you can repeat the `protocol=` format and add a second or third profile.

annex and ports Keywords

The **annex** and **ports** keywords specify the Remote Annexes and ports to which profile attributes will apply.

▼ To list Remote Annexes and/or ports, type `annex=` and/or `ports=` followed by one or more Remote Annex names or IP addresses and one or more port numbers, respectively.

Use an asterisk to specify a partial Remote Annex name or IP address. You can enter individual port numbers separated by commas or a range of port numbers using dashes (e.g., `ports=1,3,6-22`).

To combine the **annex** and **port** keywords in one line, separate keyword/value entries with a semicolon (e.g., `annex= Annex 02, 245.132.88.22; ports=1,3,6-22`). If you omit Remote Annex names or addresses and list one or more ports, the profile attributes apply to all Remote Annexes.

Understanding Profile Attributes

In each user profile, one or more attributes follow keywords and their values. This section explains the attributes you can include.

accesscode

The **accesscode** attribute controls the text users enter when logging in to a dial-back port. Before you can use the accesscode attribute, you must define at least two modem pools (one for dial-in and one for dial-out) in the **acp_userinfo** file. A modem pool groups asynchronous ports on one or more Remote Annexes.

Modem pool definitions appear at the end of the **acp_userinfo** file. To define a modem pool:

1. From the Bay Networks program group window, double-click on the appropriate icon to open the **acp_userinfo** file.

   The **acp_userinfo** file opens in the Notepad editor.

2. Find the area of the file where entry information resides and type `pool` followed by a name for the modem pool (e.g., `pool inboundpool1`).

3. Type `ports` followed by one or more port numbers, @, and one or more Remote Annex names or IP addresses.

   Separate port numbers with commas and/or enter a range of numbers with dashes (e.g., `ports 1,6-10@Annex01`).

The **acp_userinfo** file can store **accesscode** attributes in a user profile. To create an **accesscode** entry:

1. Type `accesscode` followed by a code name.

   For IPX clients, enter **`IPX`** for the access code.

2. Type `phone_no` followed by an actual phone number (e.g., `phone_no 634-5789`).

   If you do not enter a phone number, the system prompts the user for it. Enter `charge_back` for IPX clients, and the system prompts a user for a phone number, drops the connection, and calls the user back at that number.

3. Type `in_pool` followed by the name of an inbound modem pool (e.g., `in_pool inboundpool1`).

4. Type `out_pool` followed by the name of an outbound modem pool (e.g., `out_pool outboundpool1`).

5. Type `job` followed by one CLI command, its arguments, and `end`.

   You do not need to enter a **job** specification.

6. Type `end`.

clicmd

The **clicmd** attribute lists CLI commands that **erpcd** will execute if the profile matches. To use this attribute:

1. From the Bay Networks program group window, double-click on the appropriate icon to open the **acp_userinfo** file.

   The **acp_userinfo** file opens in the Notepad editor.

2. Find the area of the file where entry information resides and type `clicmd`.

3. Enter a single user or superuser CLI command, or the name of an existing macro defined for a Remote Annex.

4. **Type** `end`.

   Repeat the line you created in Steps 1-3 if you want to use more than one CLI command. **Erpcd** executes CLI commands in the order they appear.

5. Add `clicmd...end` following the last line that lists a CLI command.

   Use this line if you want to continue the CLI session after **erpcd** executes the last CLI command.

You cannot use **clicmd** unless you set the **cli_security** parameter to `Y`. Do not include the same CLI command in the **clicmd** and **climask** entries.

climask

The **climask** attribute limits the CLI commands users can execute. To use this attribute:

1. From the Bay Networks program group window, double-click on the appropriate icon to open the **acp_userinfo** file.

   The **acp_userinfo** file opens in the Notepad editor.

2. Find the area of the file where entry information resides and type `climask`.

3. Enter the CLI commands. If you enter more than one command, separate commands with spaces.

4. Type `end` to conclude the climask entry.

Use include files in place of repeated **climask** entries. To use these files, type `include` and the file name. Store Include files in the same directory as is the **acp_userinfo** file.

When a user name and password match the profile, **erpcd** sends this list to the Remote Annex, which prevents the user from executing the commands.

You cannot use **climask** unless the **cli_security** parameteris set to **Y**. Do not include the same CLI command in the **clicmd** and **climask** entries.

For detailed information about CLI commands, please refer to *Document References* on page 1-6.

deny

The **deny** attribute prevents a user from connecting to a Remote Annex. To use the command:

1. From the Bay Networks program group window, double-click on the appropriate icon to open the **acp_userinfo** file.

   The **acp_userinfo** file opens in the Notepad editor.

2. Find the area of the file where entry information resides **and** type `deny` following a user name or group name.

If you include additional attributes in a profile that uses **deny**, the profile will not execute them.

When **erpcd** denies access to a Remote Annex, it generates a message in the log file. For CLI users, the message appears on the screen.

filter

The **filter** attribute sets network address restrictions for specific users or groups. These restrictions apply to the port on which a user logs in.

To use the attribute:

1. From the Bay Networks program group window, double-click on the appropriate icon to open the **acp_userinfo** file.

   The **acp_userinfo** file opens in the Notepad editor.

2. Find the area of the file where entry information resides, and type `filter`.
3. Enter a filter definition.
4. Type `end`.

   Repeat the line you created in Steps 1-3 if you want to use more than one filter. **Erpcd** executes filter attributes in the order of appearance.

Each filter definition includes categories for direction, scope, family, criteria, and actions. Separate each part of the filter definition with a space.

- **Direction** applies the filter to incoming or outgoing packets. You can enter **`input`** or **`output`**. To apply a filter to incoming as well as outgoing packets, you must create two separate definitions.
- **Scope** controls how **erpcd** matches the filter definition. You can enter `include` to apply the filter to packets that match the definition, or `exclude` to apply the filter to packets that do not meet the definition.
- **Family**, an optional part of the definition, specifies the protocol to which the filter applies. Currently, the system supports only `ip`.

- **Criteria** includes the conditions for the filter. This section uses a keyword followed by a value. You can enter:
  - `dst_address` (the destination address of the packet) followed by an IP address.
  - `dst_port` (the destination port) followed by a port number from 1-65535 or by a service name.
  - `src_port` (the source port number) followed by a port number from 1-65535 or by a service name.
  - `src_address` (the source address of the packet) followed by an IP address.
  - `address_pair` for incoming or outgoing packets passing between two addresses, followed by two IP addresses. Enter both addresses, separated by a space, on the same line. If you use this keyword, you cannot use `dst_address` or `src_address`.
  - `port_pair` for incoming or outgoing packets passing between two ports or services, followed by a port number or service name. If you use this keyword, you cannot use `dst_port` or `src_port`.
  - `protocol` (the transport protocol of the packet) followed by a number from 1 to 65535 or by `tcp`, `udp`, or `icmp`.

To match all addresses or port numbers, enter `-1` or `*` in place of an address or **port number**. For service names, you can enter `domain`, `finger`, `ftp`, `name`, `nfs`, `nntp`, `rlogin`, `route`, `routed`, `router`, `rtelnet`, `sftp`, `smtp`, `telnet`, `tftp`, `time`, `who`, or `login`. For the port numbers that correspond to these service names, see *Document References* on page 1-6.

- **Actions** specify activity of a filter when its criteria match a packet. Enter one or more of the following actions:
  - `discard` discards the packet. If you use `syslog`, `icmp`, or `netact` with `discard`, the system discards the packet after it takes those actions.
  - `icmp` discards the packet and sends an ICMP message indicating that the destination is unreachable.
  - `netact` defines activity for a SLIP or PPP dynamic dial-out line. When you use `netact` in a filter that is enabled on SLIP or PPP dynamic dial-out line, packets that match the filter constitute activity on the line. If the line is not up, `netact` discards the packet.
  - `no_start`, used with `include` (in the **Scope** category), specifies that packets defined as activity will not activate a dynamic dial-out line, but will keep the line up and will reset the **net_inactivity timer** parameter to `0`.
  - `syslog` logs the event in the log files.

route

The **route** attribute defines the IP routes that a router makes available through a Remote Annex when it dials in. Use this attribute when you do not want a router to incur overhead in running a routing protocol itself. To use this attribute, you must:

1. From the Bay Networks program group window, double-click on the appropriate icon to open the **acp_userinfo** file.

   The **acp_userinfo** file opens in the Notepad editor.
2. Find the area of the file where entry information resides and type `route`.
3. Enter an IP address for the destination of the route.
4. Enter a subnet mask for the address of the destination.

5. Enter an IP address for the gateway that is the next hop for the route.

   If you enter an asterisk, the Remote Annex uses the remote address of the port as the gateway.

6. If necessary, you can enter a number from 1 to 15 to indicate the number of hops to the destination, or `-h` to indicate that the route is hardwired.

   You can skip this step. You do not have to enter a number of hops or `-h`.

7. Type `end`.

at_zone

The **at_zone** attribute lists AppleTalk zones on a network. To use this attribute:

1. From the Bay Networks program group window, double-click on the appropriate icon to open the **acp_userinfo** file.

   The **acp_userinfo** file opens in the Notepad editor.

2. Find the area of the file where entry information resides and type `at_zone`.

3. Enter one or more zone names.

   If you use more than one zone name, separate names using spaces (e.g., `at_zone zone1 zone2`). Zone names use 1-32 characters; you cannot use non-printable characters. If you enter a name that contains spaces, enclose the entire name in double quotation marks.

4. Type `end`.

at_connect_time

The **at_connect_time** attribute specifies the number of minutes that an ARA connection can remain open. To use this attribute:

1. From the Bay Networks program group window, double-click on the appropriate icon to open the **acp_userinfo** file.

   The **acp_userinfo** file opens in the Notepad editor.

2. Find the area of the file where entry information resides and type `at_connect_time` followed by the number of minutes.

```
user john
    at_connect_time 12
end
```

The above example limits the session to twelve minutes.

at_nve_filter

The **at_nve_filter** attribute allows you to include or exclude users from specific objects, network numbers, subzones, and zones. Specify one **at_nve_filter** attribute for each user in a profile. To use this attribute:

1. From the Bay Networks program group window, double-click on the appropriate icon to open the **acp_userinfo** file.

   The **acp_userinfo** file opens in the Notepad editor.

2. Find the area of the file where entry information resides and type `at_nve_filter`.
3. Type `include` or `exclude`.
4. Enter an object name followed by a colon (:).
5. Enter a network number or subzone name followed by **@**.
6. Enter a zone name.
7. Type `end`.

```
user username=john
    at_passwd smith
    at_nve_filter exclude joe*:*@ *:*@sales end
end
```

For object names, network numbers or subzone names, and zone names, you can use an asterisk as a wildcard. All entries in steps 3, 4, and 5 are case-sensitive and can use up to 32 characters.

at_password

The **at_password** attribute stores a passwords for registered AppleTalk users. Remote Annex Server Tools for Windows NT® uses the passwords to authenticate all AppleTalk users. To use this attribute:

1. From the Bay Networks program group window, double-click on the appropriate icon to open the **acp_userinfo** file.

   The **acp_userinfo** file opens in the Notepad editor.

2. Find the area of the file where entry information resides and type `at_password` followed by a password using 1 to 9 characters.

   Include punctuation marks in the password. If you use spaces and/or hexadecimal values, use the backslash (/) preceding these characters.

If you want to allow AppleTalk guests access to the network, you should use the **na** utility to set the **at_guest** parameter to Y. You can, however, create an **at_password** attribute here using **`Guest`** (case sensitive) as a user name.

chap_secret

The **chap_secret** attribute defines the token used for authentication when you use the CHAP protocol for PPP links. CHAP authenticates users based on the user names in the **acp_userinfo** file. To create a token:

1. From the Bay Networks program group window, double-click on the appropriate icon to open the **acp_userinfo** file.

   The **acp_userinfo** file opens in the Notepad editor.

2. Find the area of the file where entry information resides and type `chap_secret` following by the token.

   Each token can use up to 32 alphanumeric characters. We recommend that all tokens use at least 16 characters.

Using the acp_keys File

The **acp_keys** file stores Remote Annex names or IP addresses and corresponding encryption keys. **Erpcd** uses the keys you define here to create encryption keys that the security server and a Remote Annex use to exchange messages. When the security server receives an encrypted message from a Remote Annex, it matches the key with an associated Remote Annex in the **acp_keys** file. If there is no match, the Remote Annex and the server cannot communicate.

To create an entry in the **acp_keys** file:

1. From the Bay Networks program group window, double-click on the appropriate icon to open the **acp_keys** file.

   The **acp_keys** file opens in the Notepad editor.

2. Find the area of the file where entry information resides and enter one or more Remote Annex names or IP addresses.

   Use an asterisk (wildcard) for any part of an IP address. If you list more than one Remote Annex, you must separate names or IP addresses using commas.

3. Type a colon to separate Remote Annex names or addresses from the encryption key.

4. Enter an encryption key that uses up to **15** characters.

   You cannot use spaces or tabs here. Encryption keys are case-sensitive. For additional information, refer to *Creating Encryption Keys* on page 3-17.

For example, `annex1, annex2: abcxyz` is a simple entry that defines an encryption key for two Remote Annexes. If you need to continue an entry on a second line, use the backslash (/) at the end of the first line.

Erpcd first attempts to match complete IP address entries in the **acp_keys** file. If **erpcd** does not find an exact match, it searches entries that contain wildcards. In either case, **erpcd** uses the first key entry it finds.

Creating Encryption Keys

Define encryption keys by setting the **acp_key** parameter for each Remote Annex. If the key value is not the same in the **acp_keys** file and for the **acp_key** parameter, the Remote Annex and the server cannot communicate. In addition, you must set the **enable_security** parameter to `Y` to use security features.

To set up encryption keys:

1. From the Bay Networks program group window, double-click on the appropriate icon to open the **acp_keys** file.

   The **acp_keys** file opens in the Notepad editor.

2. Find the area of the file where entry information resides and enter Remote Annex names or IP addresses and encryption keys in the **acp_keys** file.

3. Use the Remote Annex **admin** utility to set the **acp_key** parameter for each Remote Annex you listed in the **acp_keys** file.

4. Use the **Services** control panel to stop or pause **erpcd**.
5. Use the **reset annex security** of the **admin** utility command to reset security for the Remote Annexes whose keys you added or changed.
6. Use the **Services** control panel to restart **erpcd.**

Using the acp_dialup File

The **acp_dialup** file stores user names, Remote Annex names and addresses, and port numbers. **Erpcd** matches Annex and user entries to provide IP addresses for users dialing in to the network. It denies access to users if it does not find a matching entry.

To use the information in **acp_dialup**, you must set the **address_origin** parameter to `ACP` via the **na** utility. This allows a Remote Annex to search the **acp_dialup** file for the remote client’s user name and for local and remote addresses.

To create an entry in the **acp_dialup** file:

1. From the Bay Networks program group window, double-click on the appropriate icon to open the **acp_dialup** file.

   The **acp_dialup** file opens in the Notepad editor.

2. Go to the end of the file and enter a user name. If authentication is performed with multiple domain controllers, enter the domain name and the user name like this:

   ```
   domain-name\\user-name
   ```

3. Enter one or more port numbers followed by @ and one or more Remote Annex names or IP addresses.

   Separate port numbers with commas and/or enter a range of numbers with dashes (e.g., `1,3,6-10@Annex01`).

4. Enter a remote address followed by a local address.

   Use an asterisk (wildcard) for any part of an IP address. You must use spaces to separate the user name, port number/Remote Annex, Local Address, and Remote Address fields.

Using Local and Remote Addresses

If the **acp_dialup** file contains a matching user name and local and remote addresses exist in the file, the Remote Annex uses those values. If the **acp_dialup** file contains a matching user name and a remote address but not a local address, the Remote Annex uses the remote address from the file, and uses the Remote Annex's IP address for the local address.

If the file does not contain a matching user name, the Remote Annex uses values from the **local_address** and **remote_address** parameters.

- If both parameters contain addresses, the Remote Annex uses these values.
- If both parameters are set to `0.0.0.0`, the Remote Annex negotiates for both addresses with the remote PPP client. The connection is denied for a remote SLIP client.
- If **local_address** contains a value and **remote_address** is set to `0.0.0.0`, the Annex uses the local address and negotiates with the remote PPP client for the remote address. The connection is denied for a remote SLIP client.

Chapter 4
Using Security Features

Remote Annex Server Tools for Windows NT® uses standard Windows NT® domain security and Remote Annex-based security features to protect your network from unauthorized access. To use Remote Annex Server Tools for Windows NT® security features, you need to:

- Use the Windows NT® **Administrative Tools/User Manager for Domains** to create groups, user names, and passwords.
- Use the **na** utility to set security parameters on the Remote Annex for the types of security you want.

> Erpcd authentication is not case sensitive. Group names cannot contain spaces.

Use group authentication by selecting options in the **Security** dialog box:

- Select **Global Group Authentication**.
- Select a domain, then select the groups whose members can be authenticated.

> If you are using Global Group Authentication, select Native NT as your Security Regime.

For more information on group authentication, see Chapter 3.

This chapter summarizes most security features and explains the relationship between Windows NT® domain security and server-based security. It includes:

- *Using Windows NT® Domain Security*
- *Setting Remote Annex Security Parameters*
- *Using ACE/Server Security*
- *RADIUS Security*

Although this manual documents the differences between UNIX and Windows NT® implementation, the RADIUS for Windows NT® implementation is significantly different from the UNIX implementation. Therefore to avoid confusion, all RADIUS for Windows NT® information is included in this chapter.

Using Windows NT® Domain Security

When a user logs on to a Remote Annex, to one of its ports, or to a network, the system performs authentication based on the security parameters you enter. Once you set the parameters that enable a type of security:

- The system checks the Windows NT® user name and password.
- If you selected **Global Group Authentication** and chose groups for remote access in the **Server Tools Options** windows, the system performs additional authentication. If the user name and password are valid, the system determines whether the user is a member of any groups you select.

Support for Multiple Domains

Remote Annex Server Tools for Windows NT® can authenticate users from domains other than the default domain of the security server. To facilitate this feature, the Windows NT® administrator must establish at least a one-way trust relationship.

A trusting domain controller can be linked to one or more trusted domain controllers. When a cross-domain authentication request arrives at the (trusting) domain controller, the request is transferred to the appropriate (trusted) domain controller. The domain security of the trusted controller accounts manager database includes the user in question and authenticates that user.

Multiple Domain Authentication Setup Procedure

Follow these Windows NT® steps to facilitate support for multiple domain authentication:

Windows NT® steps

1. Establish the appropriate trust relationship among domains.
2. Load the Remote Annex Server Tools for Windows NT® on the trusting domain controller.
3. Define the user(s) in the trusted domain's security accounts manager database.

Server Tools steps

All Windows NT® users who require authorization must use the Remote Annex Server Tools software to configure these services. Those definitions are accomplished in the following steps:

1. Add a valid entry(s) in the **acp_userinfo** file.
2. If the caller requires a dial-up address, add a valid entry(s) in the **acp_dialup** file.

The name of the user must be defined in the **acp_userinfo** and **acp_dialup** file in the format:

```
domain-name\\user-name
```

For example, a user named Stephen from the Marketing domain would log on as `Marketing\\Stephen`.Windows NT®, Windows for Workgroups®, and Windows 95® use this format.

Setting Remote Annex Security Parameters

The Access Control Protocol (ACP) of the Remote Annex provides server-based security. When you define one network server as a security server, use ACP software default settings or modify the software to create a customized security policy for your network. This section includes:

- *Security Requirements*
- *Types of Security*

Security Requirements

Before you can use server-based security, you must use the **na** utility to:

- Set the **enable_security** parameter to Y.
- Define one server as the primary security server by entering its address in the **pref_secure1_host** parameter. Define a backup security server in the **pref_secure2_host** parameter.
  - If a Remote Annex queries the primary server and does not receive a response within the time defined in the **network_turnaround** parameter, the Remote Annex queries the backup server.
- If the backup server does not respond within the time specified, the Remote Annex broadcasts to the network for another server running **erpcd** (as long as the **security__broadcast** parameter is set to Y).

For instructions on using the **na** utility and detailed explanations for each parameter, see *Document References* on page 1-6.

You can customize security features by editing several ACP files. These files are maintained by the security server through the Remote Annex Server Tools for Windows NT® program window.

- The **acp_keys** file includes encryption key information.
- The **acp_dialup** file contains user names and addresses for dial-up connections.
- The **acp_userinfo** file contains initial login environment information and start-up CLI commands.

See *Document References* on page 1-6 to find sources of additional information and detailed discussions about server-based security and examples using the **na** utility. Use these sources for reference. However, some instructions and examples refer to the **acp_regime**, **acp_restrict, acp_group**, and **acp_password** files. Remote Annex Server Tools for Windows NT® servers does not use the **acp_regime**, **acp_restrict, acp_group**, or **acp_password** files. You should skip the steps that discuss these files.

Types of Security

Configure your system for several types of server-based security by using the **na** utility to set security parameters. Once these parameters are set, Remote Annex Server Tools for Windows NT® uses Windows NT® user names and passwords to authenticate users. This section describes the type of server-based security that use Windows NT® domain security. It includes:

- *PPP Security*
- *CLI Security*
- *Virtual CLI Security*
- *AppleTalk Security*
- *Port Server Security*

You need to set certain parameters to enable each type of security described here. Once you set parameters, each user will have to enter a user name and password. Remote Annex Server Tools for Windows NT®grants access only to those user names and passwords listed in any Windows NT® global group you selected in the **Remote Access Groups** tab window.

PPP Security

Point-to-Point (PPP) provides a link between hosts that carry IP, IPX, and ARA protocols. After PPP negotiates Link Control Protocol (LCP) options, the hosts at either end of the link authenticates their identities using **PAP** or **CHAP** security protocols.

- **PAP** is a two-way handshake in which hosts exchange user names and passwords in clear text.
- **CHAP** is a three-way handshake that uses a secret token defined in the **acp_userinfo** file to authenticate users.

▼ To configure Windows NT® security for PPP links, you must set the **ppp_security_protocol** parameter.

- If you set **ppp_security_protocol** to **pap**, the system uses Windows NT® user names and passwords for authentication.
- If you set **ppp_security_protocol** to **chap–pap**, the system first requests CHAP security. If CHAP is not acknowledged, it requests PAP.

CHAP does not authenticate Windows NT® user names, passwords, or remote access groups. It authenticates based on user names from the **acp_userinfo** file and the CHAP token.

- To log user access for PPP, set the **slip_ppp_security** parameter to **Y**.

> If you want to set **ppp_security_protocol** and **slip_ppp_security** to values other than the ones described here, the system will not use Windows NT® user names and passwords for authentication. Please see *Document References* on page 1-6 to find sources of additional information about system behavior with other parameter values.

CLI Security

The Command Line Interpreter (CLI) of the Remote Annex allows users to connect to hosts, move between established sessions, modify port characteristics, and display statistics for the Remote Annex, hosts, and the network. CLI provides superuser commands for network administration and management.

- To configure server-based security for CLI connections, set the **cli_security** parameter to **Y**.

Virtual CLI Security

Virtual CLI (VCLI) connections allow network users access to CLI commands. When a user enters a telnet command to connect to a Remote Annex, and requests the CLI at the port server prompt, the Remote Annex’s port server process creates a virtual CLI connection.

AppleTalk Security

Remote Annex Server Tools for Windows NT® authenticates AppleTalk users via the **acp_userinfo** file. This file includes entries for usernames and passwords, a guest profile for anonymous access, and an AppleTalk connection timer.

- To authenticate AppleTalk users, set the **at_security** parameter to Y.

Port Server Security

The port server process of the Remote Annex allows it to accept **telnet** or **rlogin** connection requests from network users, hosts, and applications. When a user connects to a Remote Annex via **telnet** or **rlogin** and responds to the port prompt by entering a port or rotary number, the security server requires an Windows NT® domain user name and password.

To configure server-based security:

- For port server connections, set the **port_server_security** parameter to Y.
- For VCLI connections, set the **vcli_security** parameter to Y.

Third Party Security Types

Remote Annex Server Tools for Windows NT® supports:

- ACE/Server (SecurID) security.

Using ACE/Server Security

The ACE/Server token is an access control security token used to identify users of computer systems and secure TCP/IP networks. Used in conjunction with the SecurID card hardware or software access control modules (ACMs), the ACE/Server token automatically generates a unique, unpredictable access code every 60 seconds. The ACE/Server, a daemon that interfaces with the user database, allows the system administrator to monitor login attempts and generate reports.

1. To use ACE/Server (SecurID) security, select the security regime **SecurID** radio button in the **Security** dialog box.

Creating a SecurID Client for an NT Server:

You must transfer a binary copy of the sd_conf.rec file from the SecurID server to the Windows NT root directory. Also the server must be registered as a SecurID client.

Supported ACE/ Server Releases

Remote Annex Server Tools for Window NT$^{®}$ offers support for ACE/ Server Release 2.1.1 and 2.2.

ACE/Server is supported using ACP. For more information on configuring SecurID security using the graphical user interface, see Chapter 2, *Selecting Server Tools Options* . For more information resources on installing, configuring, and using ACE/Server Software, see *Document References* on page 1-6.

Additional Security Types

Remote Annex Server Tools for Windows NT$^{®}$ supports port server, CLI, VCLI, and PPP security using Windows NT$^{®}$ domain user names and passwords. Remote Annex Server Tools for Windows NT$^{®}$ supports:

- Security Filters, ARA and Dial-back security defined in the **acp_userinfo** file.
- Dial-up security defined in the **acp_dialup** file.

Remote Annex Server Tools for Windows NT® and UNIX-based systems support local Remote Annex security and Proprietary IPX security in the same way. Remote Annex Server Tools for Windows NT® does not support the following server-based security types (see *Document References* on page 1-6 to find sources of additional information*)*:

- Connection Security
- Password History and Aging
- Blacklisting
- Kerberos Authentication

RADIUS Security

RADIUS is an IETF- developed protocol that defines a communication standard between a Network Access Server (NAS) and a host-based communication server. RADIUS modes are as follows:

- RADIUS Authentication includes authentication of the dial-up user to the RADIUS server, and authentication of the RADIUS server to the NAS. RADIUS supports authentication modes PAP and CHAP (Challenge Handshake Authentication Protocol).
- RADIUS Accounting, another IETF-developed protocol, defines a communication standard between an NAS and a host-based accounting server. It records duration of service, packet throughput, and raw throughput.
- Although RADIUS Authorization is not supported in this release, Authorization is addressed by the Access Control Protocol (ACP). Authorization of the **acp_userinfo**, **acp_restrict**, and **acp_dialup** files applies to users that are authenticated through RADIUS.

RADIUS and ACP Protocol Operation

RADIUS and ACP servers work together to provide the user with a standard means of communication between a Network Access Server and a host-based server.

When or If...	The...
the security profile matches the **Server Tools Options** dialog box RADIUS On/Off radio button,	expedited remote procedure call daemon (**ERPCD**)/ACP prompts the Remote Annex for the user name and password.
the **user name** and **password** are entered correctly,	ERPCD/ACP sends a RADIUS **Access-Request** packet to the RADIUS server (this packet contains the normal RADIUS header and the **Access-Request** attributes).
the **Access-Accept**, **Access-Reject**, or **Access-Challenge** packet fails to arrive in the specified amount of time,	ERPCD/ACP re-sends the packet.
no response is received,	ERPCD/ACP sends the **Access-Request** packet to the backup RADIUS server, if configured in the **Server Tools Options** dialog box.
ERPCD/ACP receives an **Access-Accept** packet,	ERPCD/ACP considers the user validated.
ERPCD/ACP receives an **Access-Reject** or an unsupported **Access-Challenge** or the backup RADIUS server also fails to respond,	ERPCD/ACP considers the user invalidated.

RADIUS Authentication

RADIUS authentication supports the authentication modes PAP and CHAP. This section covers the following topics:

- PPP and CHAP Support
- Access-Request Attributes
- Access-Accept and Access-Reject Attributes

PPP and CHAP Support

RADIUS requires PPP/CHAP enforcement to be in the RADIUS server.:

The...	Then...
Remote Annex sends the ACP server an **ACP Authorization-Request** message containing the CHAP information,	the ACP server determines if RADIUS is to be used (set in **Server Tools Options** dialog box) and sends a request to the RADIUS server containing the CHAP information needed for validation.
RADIUS server validates the information and returns either an **Access-Accept** or **Access-Reject** message,	the ACP server responds to the Remote Annex with **REQ_GRANTED** or **REQ_DENIED** for authorization.

If the RADIUS On/Off radio button in the **Server Tools Options/ Security** dialog box is set to off, the ACP server validates against the **chap_secret** entry in the **acp_userinfo** file.

Access-Request Attributes

ERPCD/ACP sends Access-Request packets which indicate how the user connects to the Annex. This information is used by the server as a hint or a restriction. The following section defines the available access-request attributes:

User-Name

Indicates the name of the user that the RADIUS server will authenticate. An unterminated ASCII string identical to the user name that ERPCD/ACP retrieves via the user name prompt. You can specify up to 31 alphanumeric characters.

User-Password

Specifies the user password that the RADIUS server will authenticate.

CHAP-Password

Specifies the response value of a CHAP user in response to the password challenge.

NAS-IP-Address

Indicates the IP address of the Annex authenticating the user or sending an Accounting packet.

NAS-Port-Type

Specifies the Remote Annex port handling the user session. This value corresponds to the physical port type. Supported port types:

- Async (0)
- ISDN Sync (2)
- ISDN Async V.120 (3)
- Virtual (5)

NAS-Port

Specifies the current port number connection.

NAS–Port number example:

```
nxxx (decimal)
```

n=	Description
0	Serial interface port
2	Virtual (VCLI, FTP)
3	Dial-out
4	Ethernet (outbound)

Although not an attribute, **CHAP-Challenge** appears in the Authenticator of the RADIUS header.

Framed-Protocol

Specifies the link level protocol type allowable to the user. Supported values are:

- PPP
- SLIP

Service-Type

Specifies the type of service the user will receive. Supported types of service are:

- Login
- Framed
- NAS–Prompt
- Outbound
- Administrative

Access-Accept and Access-Reject Attributes

In this version, attributes included in the RADIUS Access-Accept and Access-Reject packets are ignored by ERPCD/ACP. However, ERPCD/ACP does instruct the Remote Annex to display text sent in a Reply-Message attribute as long as the user is a CLI or port server user.

RADIUS Accounting

RADIUS Accounting defines a communication standard between a NAS and a host-based accounting server. It records duration of service, packet throughput and raw throughput. This section covers the following topics:

- RADIUS Accounting Process
- Accounting-Request Attributes

To utilize RADIUS Accounting, select the **Use RADIUS Logging** radio button in the **Booting/Logging** dialog box.

RADIUS Accounting Process

The following table describes the RADIUS accounting process:

When or If...	The...

the Remote Annex sends an ACP **Audit-log** to the server,	security profile for the **ACP Authorization-Request** must match the **Security** dialog box **RADIUS Regime** On/Off radio button setting.
	On = RADIUS security active.
	Off = Native NT security active.

ERPCD/ACP receives a login or logout log request,	ERPCD/ACP sends an **Accounting-Request** packet to the RADIUS Accounting server.
The ERPCD/ACP server receives the RADIUS **Accounting-Response**,	ERPCD/ACP returns the ACP audit log verification PDU to the Remote Annex.

Accounting-Request Attributes

ERPCD/ACP sends Accounting-Request packets with the following attributes:

Acct-Status-Type

Marks whether the Accounting packet sent to the RADIUS server is the beginning or end of a dial-up session.

- Start (1) - ERPCD/ACP login events
- Stop (2) - ERPCD/ACP logout events
- Accounting-on (7) - ACP logging connection becomes active
- Accounting-off (8) - ACP audit logging connection becomes inactive

Acct-Delay-Time

Specifies the time (in seconds) the RADIUS client has been trying to send a specific Accounting packet.

Acct-Input-Octets

Specifies number of octets received during the session.

Acct-Output-Octets

Specifies number of octets sent during the session.

Acct-Session-Id

A numeric string identifid with the session reported in the packet.

Acct-Authentic

Specifies how the user is authenticated. Always set to RADIUS.

Acct-Input-Packets

Specifies how many packets received during the session.

Acct-Output-Packets

Specifies how many packets sent during the session.

Acct-Session-Time

Specifies the elapsed session time as calculated in RADIUS.

Other Attributes

All attributes that are included in the Access-Request packet are also included in the Accounting-Request packet.

RADIUS Configuration Management

Configuring the RADIUS Authentication and Accounting server involves setting parameters to define the operating and administrative attributes of the server. This section covers the following topics:

- The RADIUS Servers dialog box:
    - RADIUS Servers
    - Fail-over Algorithm
    - Secret Format
    - Response Timeout and Number of Retries Format
    - Backup Server

Default Values

If there is no configuration record for a RADIUS server, the following default values are used:

Attribute	Value
Secret	0x0
Timeout	4 seconds
Retries	10
Backup server	None

RADIUS Authentication Server and Accounting Server

- *RADIUS Authentication Server* is the host name of the RADIUS Authentication server.
- *Accounting Server* is the host name of the RADIUS Accounting server.

If an Accounting server is not specified, it defaults to the ACP server. If a RADIUS server is not specified, the RADIUS server defaults to the ACP server.

Secret Format

The format for *secret* is an ASCII string or a hexadecimal string. The hexadecimal string format always starts with **0x** followed by a string of bytes, with each two hexadecimal digits indicating one byte. The maximum limit is 16 in ASCII, or the hexadecimal equivalent.

2

Response Timeout and Number of Retries Format

The Response Timeout and Number of Retries values are set in the RADIUS Servers dialog box.

timeout	The number of seconds to wait for a response before sending a retry.
retries	The number of times to retry before fail-over to the backup server, or authentication is discontinued.

Fail-over occurs if the *host* is the original primary server. This entry must be on one line.

Backup Server

The host name or Internet address of the backup RADIUS server or RADIUS Accounting server is configured using the RADIUS Server's dialog box:

1. From the **Server Tools Options** dialog box, click on the **Security** tab.
2. Select the **RADIUS** radio button to enable the RADIUS security server.

   If you do not select this option, your security server will default to native Windows NT® security.
3. From the **Server Tools Options** dialog box, click on the **RADIUS Server**s tab.
4. Click the **Backup Server** down arrow to select the backup RADIUS server or RADIUS accounting server.

   If **None** is displayed in the Backup Server drop–down list, see *Configuring a RADIUS Server* on page 2-13, for information on creating new RADIUS servers.

Fail-over Algorithm Process

The following table describes the fail-over algorithm process for authentication and accounting.

When or If...	The...
a user is to be authenticated,	RADIUS server first polled is specified in the **Server Tools Options** dialog box.
an **Access-Request** packet is sent to the RADIUS server,	ERPCD/ACP waits the specified timeout value (4 seconds by default) for the response packet.
the time expires,	ERPCD/ACP retries the request

(continued on next page)

When or If...	The...
the maximum number of retries (10 by default) is reached without a response from the server,	attempt to authenticate against the primary server fails and ERPCD/ACP attempts to authenticate against the backup server (if defined).
no response is received from the backup server,	user is rejected.
an **accounting fail-over** occurs, the server remains the same until,	failure of the backup server.
both the accounting primary server and backup fail,	the **acp_logfile** records RADIUS accounting.

Backup Security

If you configure port server, CLI, VCLI, and PPP security to use Windows NT® domain names and passwords, and the ACP security server is not available, the Remote Annex uses its locally stored password parameters to restrict user access. These parameters settings serve as backup security.To use backup security, you must set the parameters listed in the following table.

For:	Back-up Security uses:
Port Server	port_password
Incoming Port	port_password
VCLI	vcli_password

For additional sources of information about back-up security and settings for these parameters, please refer to *Document References* on page 1-6.

RADIUS Dictionary File

Included on the distribution kit is a reference RADIUS dictionary file which resides in the security files area. The **erpcd** server does not use this file, it is provided as documentation and a convenience. This file defines keywords, types, and values for RADIUS attributes and their corresponding code points. The file is in a format that is used as input by some RADIUS servers to parse messages, and write text output files. Customers might have existing dictionaries with differences in the keyword names, and may want to evaluate the impact to their databases and output reports.

The file we provide includes the latest IETF definitions of the RADIUS protocol at the time of release. It includes all attributes and values that are needed to support our Remote Annex and **erpcd** implementation. It is not necessary that our definitions be used directly, but other dictionaries may have to be extended to cover our usage.

This file may be used as a reference to add or change existing RADIUS dictionaries as need be. Since it is in the format of some of the popular RADIUS servers, in some cases it may be used as a direct replacement.

However, the network manager should review the dependencies and make a decision on how to apply the differences.

The following is a partial example of the some of the dictionary contents:

ATTRIBUTE	User-Name	1	string
ATTRIBUTE	Password	2	string
ATTRIBUTE	CHAP- Password	3	string
ATTRIBUTE	NAS-IP-Address	4	ipaddr
ATTRIBUTE	NAS-Port	5	integer
ATTRIBUTE	Service-Type	6	integer
ATTRIBUTE	Framed-Protocol	7	integer
ATTRIBUTE	Framed-IP-Address	8	ipaddr
<...>			

#	Framed Protocols		
VALUE	Framed-Protocol	PPP	1
VALUE	Framed-Protocol	SLIP	2
VALUE	Framed-Protocol	ARAP	3
VALUE	Framed-Protocol	Gandalf-SL/MLP	4
VALUE	Framed-Protocol	IPX/SLIP	5

#	User Service Types		
VALUE	Service-Type	Login-User	1
VALUE	Service-Type	Framed-User	2
VALUE	Service-Type	Callback-Login-User	3
VALUE	Service-Type	Callback-Framed-User	4
VALUE	Service-Type	Outbound-User	5
VALUE	Service-Type	Administrative-User	6
VALUE	Service-Type	NAS-Prompt	7
VALUE	Service-Type	Authenticate-Only	8
VALUE	Service-Type	Callback-NAS-Prompt	9
<...>			

Appendix A
Browsing for Resources on a Microsoft Network

Browsing is locating network resources in a Domain or workgroup. Domains and workgroups are Microsoft's logical grouping of computers and other resources into managed groups. Browsing is implemented by accessing Browsers, which are computers that maintain resource lists for the Domain, rather than trying to directly locate the resource. Therefore locating a resource becomes a question of locating a Browser. This location process becomes a problem in subnetted TCP/IP networks because the location process utilizes UDP broadcasts which are generally not passed through routers between subnets. IPX is not a problem because the datagram location mechanisms used are not generally blocked by routers. However, in mixed protocol environments, the browser will use TCP/IP. This discussion assumes a TCP/IP only network. Some points of location and discovery of Browsers are different for other protocols.

Microsoft now provides a Windows Internet Naming Service (WINS) for the Windows NT® server that eliminates many of the problems with locating Browsers.

This discussion assumes that WINS is not available. The WINS solution is outlined at the end of the document.

Browser Definition

Browsers are distributed on the network based on the domain, subnet, and number of workstations. The Browsers are assigned through a weighted election process that allows replacement of Browsers when they fail or are shutdown. This can make Browsers difficult to locate because they may not always be on the same machine.

The Primary Domain Controller (PDC) which provides authentication for the Domain, serves as the Domain Master Browser (DMB). The DMB has the responsibility of keeping track of and coordinating all the Master Browsers in the Domain as well as correlating information from other domains. The PDC wins the DMB election because it is heavily weighted by being the PDC.

Master Browsers

Master Browsers (MB) are located on each subnet and are responsible for tracking resources on the subnet. They provide updated subnet resource lists to the DMB and receive domain resource lists from the DMB. When a MB first comes up, it broadcasts on the subnet asking all resources to identify themselves. Resources are required to reply within 30 seconds. New resources should announce their presence to the MB. The MB also exchanges lists with the DMB. This exchange is repeated every 15 minutes and when new resources announce themselves on the subnet. Resources are removed from the list when they either announce their departure or they fail to respond 3 times to the 15 minute update query (45 minutes).

Subnets

There should be one MB for each subnet. If the number of active stations on a subnet exceeds 32, a backup browser is selected for each 32 stations. The MB is responsible for keeping the backup browser's browse list up to date. When a station wants to access a Browser for the first time, it receives a list (explained below) of all the available browsers on its subnet. The station caches the location of up to 3 browsers and accesses them in the future in a random pattern. The browse request load is thereby spread among the available browsers.

Configuration and Election Process

Browsers are selected through configuration and an election process. It is possible to set a station to be a MB. This only gives it additional weight in the election process. Another weight in the election process is the type of operating system running (Microsoft Windows NT®, Windows 95, Windows for Workgroups). An election is held between all potential MBs to select the MB for the subnet. This process can be affected by such things as boot speed (after a power failure) and is a very dynamic process. Except for the DMB, it is not always possible to statically determine the address of a MB. If the current MB shuts down or certain other conditions occur, a new MB election can be triggered, although in general, once a MB has been selected, it remains the MB, even if other stations may now be a better weighted choice.

Locating Browsers

The client station maintains a cache of IP addresses and important services and will first (a) check its cache for browsers. If the cache does not contain any browsers, the next step is to (b) generate a NetBIOS over an IP broadcast to try to locate a MB on its subnet. If the subnet MB responds, the client will send a directed query to the MB to get a list of browsers on the subnet. The MB returns a list of browsers on the Domain/ subnet being queried. The client caches up to 3 browsers as previously mentioned. The broadcast time out occurs if there is no MB on the client's subnet. There is no way to direct a client to a MB outside its subnet. Therefore, if there is no MB on the subnet, a client on that subnet can not browse. If the client can not find the MB after 3 attempts, a Force Election broadcast is issued to force election of a new MB for the subnet. However, a station on a slow link (remote access) is prevented from being a Browser. So even if the remote access client is capable of acting as a Browser, the link type prevents it. A remote access client calling into a subnet with no MB will be unable to browse the network.

The WINS Solution

WINS is a service that runs on a Windows NT® server. It is provided with Windows NT® 3.5 or greater. WINS primary function is to provide name services without broadcasts because WINS queries are directed datagrams. The current version of WINS, along with some client updates, also assists with browsing across subnets that do not contain Browsers.

A WINS server can provide the location of the PDC which is also the DMB to a client. When the PDC comes up, it registers a couple of special names with WINS. These names consist of the domain name followed by characters <1B> and <1D> (ex. eng<1B> and eng<1D>). These special names are associated with the IP address of the DMB. When a client attempts to browse on a subnet with no MB, the client first does a broadcast to locate the MB, which fails. The client also directs a NameQuery to WINS asking for the special version of the domain name followed by <1B>. WINS returns the IP address of the DMB. The client can then query the DMB for the browse list for the domain.

Clients

The following clients can use the enhanced WINS browse capability (are WINS aware):

- Windows NT®
- Windows 95
- Windows for Workgroups - with latest drivers

  Requires VREDIR.386 included on Windows NT® 3.5 server

  Requires Microsoft TCP/IP 32 drivers (32 bit TCP/IP)

Required Configuration Details

The following configuration details are required to make the browsing operation work correctly:

- The PDCs of all domains should be Windows NT® server Version 3.5 or later.
- All stations must use WINS to allow services to be recorded properly.
- The client should disable the ability to be a browse master. This will prevent the client from browsing except when the user asks for a browse list. This reduces delays caused by broadcasting for the MB in the background.
- For Windows 95:
  - Control panel - Networks - File and Print Sharing for Microsoft
  - Networks - Properties - Advanced - BrowseMaster - Disabled
- For WFW 3.11:
  - system.ini
  - [Network]
  - MaintainServerList=No

Note that this is only necessary on clients that will encounter browsing problems because their broadcast queries will not be routed correctly. If a master browser exists on the subnet, the disabling will not be necessary.

Remote Annex Example

The Remote Annex forwards IP broadcasts from a remote access client to the network that the Annex is on. If that network is a subnet that has no PCs capable of being a master browser, the remote client must be configured to use WINS to be able to browse Microsoft resources. Another possible option might be to configure the router to pass IP broadcasts, but this is probably not desirable.

Number of PCs on the Subnet

Another issue to consider is the number of PCs on the subnet that can act as master browsers. The number and type of machines may give unpredictable behavior for a remote access client. Consider for example, a remote client that is not configured to use WINS. During the day, the subnet dialed into has several Windows 95 stations that can act as master browsers. The PDC and other resources are on a different subnet. When the client dials in during the day, a broadcast finds one of the Windows 95 systems and browsing works as expected. However, it is company policy to shut down PCs at night, so when everyone goes home all Windows 95 machines are shut down. Now the remote client dials in, broadcasts to the subnet, but no master browsers are available. Browsing works during the day, but not at night. WINS would overcome this problem by finding the DMB when the Windows 95 machines were not available.

Note also that the **ip_forward_broadcast** parameter on the Annex controls broadcast traffic from the ethernet to the remote client. It has no effect on broadcasts generated by the client for the ethernet. Client to ethernet broadcasts are on and can not be configured off. Replies to the client browser broadcasts are directed datagrams and will not be affected by the **ip_forward_broadcast** setting.

Resource Visibility

The problem of resource visibility becomes especially important when the remote “client” is another network that may have resources to be shared. The remote network should have a machine capable of acting as a MB. A MB locates resources by broadcasts on its subnet. If there is no MB on the remote net, there must be one on the network the Annex is on and the **ip_forward_broadcast** parameter should be Y to allow the MB request to reach the resource. WINS will also be useful in this environment to assure reliable communication between all the browser components.

Additional Information

Resolve a Name to an IP Address

When a client tries to resolve a name to an IP address, it follows the following steps:

1. **Check**s **internal cache of resolved names.**
2. **Ask**s **WINS (if enabled).**
3. **Broadcast**s **to resolve name.**
4. **Check**s LMHOSTS **file.**

Preload PDC Address

Preloading the cache at start-up with the address of the PDC may simplify the authentication process, even if WINS is configured. It may be required if WINS is not used. This is done by adding an entry to the client’s **lmhosts** file.

Example

```
NT:  \Winnt35\System32\Drivers\Etc\lmhosts

Windows 95:\windows\lmhosts

555.555.55.555     servername        #PRE #DOM:dept  #net
group’s DC
```

This gives the IP address (555.555.55.555) of the PDC (servername):

- *#DOM:dept* indicates that server name is a domain controller for the dept domain
- *#PRE* indicates this entry is preloaded into the cache at start-up, this will allow the address to be found when the cache is searched and eliminate the WINS query and/or broadcast

Workgroups and Domains

Windows 95 allows specification of a workgroup name (Control Panel - Networks - Identification - Workgroup). Users should be aware that workgroups and domains are very similar concepts. Domain membership is used for authentication but resource visibility and access can be limited by workgroup membership. If you log in to the domain but are specified to be a member of a workgroup other than the domain, resources may not be visible to you depending on how those resources are configured.