

RADIUS for Windows NT Administrator's Guide

Lucent Technologies

Remote Access Business Unit

4464 Willow Road

Pleasanton, CA 94588

925-737-2100

800-458-9966

October 1998

950-1274A

Copyright and Trademarks

© 1998 Lucent Technologies. All rights reserved.

PortMaster, ComOS, and ChoiceNet are registered trademarks of Lucent Technologies, Inc. RADIUS ABM, PMVision, and IRX are trademarks of Lucent Technologies, Inc. All other marks are the property of their respective owners.

Disclaimer

Lucent Technologies, Inc. makes no express or implied representations or warranties with respect to the contents or use of this manual, and specifically disclaims any implied warranties of merchantability or fitness for a particular purpose. Lucent Technologies, Inc. further reserves the right to revise this manual and to make changes to its content at any time, without obligation to notify any person or entity of such revisions or changes.

Contents

About This Guide

Audience	ix
PortMaster Documentation	ix
Security Dynamics Documentation	xi
Additional References	xi
RFCs	xi
Books	xiii
Document Conventions	xiii
Document Advisories	xiv
Contacting Lucent Remote Access Technical Support	xv
For the EMEA Region	xv
For North America, Latin America, and the Asia Pacific Region	xv
PortMaster Training Courses	xvi
Subscribing to PortMaster Mailing Lists	xvi

1. Introducing RADIUS

Introduction to RADIUS	1-1
Overview of RADIUS Features	1-1
How RADIUS Works	1-2
Basic RADIUS Functions	1-2
Ease-of-Use Enhancements	1-4
RADIUS Directory Structure	1-6
RADIUS Installation and Configuration	1-7

2. Configuring a RADIUS Server

Getting Started	2-1
Selecting a RADIUS Server Host	2-1
Determining a Shared Secret	2-3
Installing RADIUS on a Windows NT Host	2-3
Prerequisites	2-3
Preparation	2-4
Installation	2-6
Removing RADIUS as a Service	2-10
Configuring RADIUS on a Windows NT Host	2-10
Logging RADIUS Messages to a File	2-11
Configuring the Users Cache	2-13
Configuring Multitask Authentication	2-15
Changing the Default Directories	2-16
Changing RADIUS Ports	2-17
Setting the Authentication Request Queue Size	2-18
Setting the Request Packet Timeout	2-19
Configuring RADIUS Accounting	2-20
Associating Your Database with the ODBC Driver	2-26
Server Utilities	2-29
RADIUS Menu Bar	2-30

3. Adding a RADIUS Client

Accessing the Clients File	3-1
Modifying the Clients File	3-3
Configuring the PortMaster Using the Command Line Interface	3-3
Configuring the PortMaster Using PMVision or PMconsole	3-5

4. Configuring User Information

User Profile Format	4-2
Matching User Profiles	4-4
Editing User Profiles	4-4
Default User Profiles	4-5
Check Items	4-7
Passwords	4-7
Password Encryption	4-10
Username Prefixes and Suffixes	4-11
Called-Station-Id	4-13
Calling-Station-Id	4-13
Client Information	4-14
Connect-Rate	4-14
Framed-Protocol	4-15
Group	4-15
Service-Type	4-16
Reply Items	4-16
Service-Type	4-16
Callback-Id	4-22
Callback-Number	4-22
Compression	4-23
Framed-IP-Address	4-23
Framed-IP-Netmask	4-24
Framed-Protocol	4-24
Framed-Route	4-25
Framed-Routing	4-26
Filter-Id	4-26

Idle-Timeout	4-28
IPX Network	4-29
Login-Service	4-30
Login-IP-Host	4-31
Login-TCP-Port	4-32
Menu	4-32
MTU	4-33
Port-Limit	4-33
Session-Timeout	4-34
Termination-Menu	4-34
Check and Reply Item Summary Table	4-34
Using RADIUS with PAP and CHAP	4-40
PAP	4-40
CHAP	4-41
Configuring Database Caching of User Profiles	4-42
Example PPP User Profile	4-43
5. Using RADIUS for NT Utilities	
Testing RADIUS Authentication	5-1
Copying Database Tables	5-4
Operating System Utilities	5-9
6. Configuring RADIUS Menus	
Menu File Format	6-1
Single-Level Menu	6-2
Nested Menus	6-3
Termination Menus	6-4
Menus Called by Reference	6-4
Menu Filenames	6-4

7. Installing and Configuring SecurID

Overview of SecurID Components	7-2
How SecurID Works with RADIUS	7-3
ACE/Server Installation on a Windows NT Host	7-3
Getting Started	7-4
Installing a Master Server	7-6
Installing a Master Server and a Slave Server	7-7
Configuring the Master Server	7-8
Installing ACE/Client on the Server	7-11
Starting the ACE/Server	7-12
Testing SecurID Server-to-Client Communication	7-13
Installing Other ACE/Server Features	7-14
RADIUS Configuration for SecurID	7-14
PIN Assignment	7-15
Entering an Invalid Token Code	7-17
Troubleshooting SecurID	7-18

8. Implementing RADIUS Accounting

How RADIUS Accounting Works	8-1
Getting Started	8-3
Client Configuration	8-4
Accounting Server Configuration	8-4
Configuring Accounting Database Logging	8-5
Configuring Accounting Detail File Logging	8-6
Determining the Server Version	8-6
Changing the Accounting Directory Location	8-7
Specifying an ODBC Data Source	8-7
Accounting Attributes	8-10

Acct-Authentic	8-10
Acct-Delay-Time	8-10
Acct-Input-Octets and Acct-Output-Octets	8-10
Acct-Session-Id	8-10
Acct-Session-Time	8-11
Acct-Status-Type	8-11
Acct-Terminate-Cause	8-11
Acct-Timestamp	8-13
Called-Station-Id and Calling-Station-Id	8-13
Datestamp	8-13
NAS-Port-Type	8-14
Request-Authenticator	8-14
Examples	8-15
A. Troubleshooting RADIUS	
Troubleshooting RADIUS Authentication	A-1
Testing for Successful Authentication	A-1
NIC Problems	A-1
Checking the RADIUS NT Service	A-1
Checking the PortMaster	A-3
Checking /etc/raddb/users	A-3
Host Unavailable	A-4
Invalid Login after 30-Second Wait	A-5
Result of Debug Output	A-6
Troubleshooting RADIUS Accounting	A-8
B. RADIUS Actions	
Index	

About This Guide

The *RADIUS for Windows NT Administrator's Guide* provides complete installation, configuration, and troubleshooting instructions for the Remote Authentication Dial-In User Service (RADIUS) invented by the Remote Access Business Unit of Lucent Technologies, Inc.—formerly Livingston Enterprises, Inc. This product is referred to as RADIUS for Windows NT or RADIUS for NT. This guide covers RADIUS server release 2.0.1 for Microsoft Windows NT 4.0 platforms.

RADIUS can be used with the PortMaster® family of products available from Lucent Remote Access, as well as with the ChoiceNet® client/server packet-filtering software.

To install and configure these products, see “PortMaster Documentation” below.

RADIUS for Windows NT can be used on systems running Windows NT Server 4.0 or Windows NT Workstation 4.0 with Service Pack 3 or later versions.

Audience

This guide is designed to be used by qualified system administrators and network managers. Knowledge of Windows NT and basic networking concepts is required to successfully install RADIUS. If you use RADIUS with SecurID, you must be familiar with SecurID installation, configuration, and use.

PortMaster Documentation

The following manuals are available from Lucent Remote Access. The hardware installation guides are included with most PortMaster products; other manuals can be ordered through your **PortMaster** distributor or directly from Lucent Remote Access.

The manuals are also provided as PDF and PostScript files on the *PortMaster Software CD* shipped with your PortMaster.

In addition, you can download PortMaster information and documentation from **<http://www.livingston.com>**.

- *ChoiceNet Administrator's Guide*

This guide provides complete installation and configuration instructions for ChoiceNet server software.

- *PortMaster Command Line Reference*

This reference provides the complete description and syntax of each command in the ComOS® command set.

- *PortMaster Configuration Guide*

This guide provides a comprehensive overview of networking and configuration issues related to PortMaster products.

- PortMaster hardware installation guides

These guides contain complete hardware installation instructions. An installation guide is shipped with each PortMaster product.

- *PortMaster Routing Guide*

This guide describes routing protocols supported by PortMaster products, and how to use them for a wide range of routing applications.

- *PortMaster Troubleshooting Guide*

This guide can be used to identify and solve software and hardware problems in the PortMaster family of products.

- *RADIUS for UNIX Administrator's Guide*

This guide provides complete installation and configuration instructions for Lucent Remote Authentication Dial-In User Service (RADIUS) software on UNIX platforms.

- *RADIUS for Windows NT Administrator's Guide*

This guide provides complete installation and configuration instructions for Lucent Remote Authentication Dial-In User Service (RADIUS) software on the Microsoft Windows NT platform.

Security Dynamics Documentation

If you are using the ACE/Server security software from Security Dynamics Technologies, Inc., refer to the current manual set:

- *ACE/Server v 2.3 for Windows NT Administration Manual*
- *ACE/Client for Windows NT v 4.0*

Contact Security Dynamics for the manuals.

- By voice, dial 1-800-995-5095 within the United States or +44-118-936-2699 from elsewhere.
- By electronic mail (email), send mail to **info@securid.com**.
- Using the World Wide Web, see **<http://www.securid.com/>**.

Additional References

RFCs

Use any World Wide Web browser to find a Request for Comments (RFC) online.

- RFC 768, *User Datagram Protocol*
- RFC 791, *Internet Protocol*
- RFC 792, *Internet Control Message Protocol*
- RFC 793, *Transmission Control Protocol*
- RFC 854, *Telnet Protocol Specification*
- RFC 950, *Internet Standard Subnetting Procedure*
- RFC 1058, *Routing Information Protocol*
- RFC 1112, *Host Extensions for IP Multicasting*
- RFC 1144, *Compressing TCP/IP Headers for Low-Speed Serial Links*
- RFC 1157, *A Simple Network Management Protocol (SNMP)*
- RFC 1166, *Internet Numbers*
- RFC 1213, *Management Information Base for Network Management of TCP/IP-based Internets: MIB-II*
- RFC 1256, *ICMP Router Discovery Messages*
- RFC 1321, *The MD5 Message-Digest Algorithm*
- RFC 1331, *The Point-to-Point Protocol (PPP) for the Transmission of Multiprotocol Datagrams over Point-to-Point Links*
- RFC 1332, *The PPP Internet Protocol Control Protocol (IPCP)*

RFC 1334, *PPP Authentication Protocols*
RFC 1349, *Type of Service in the Internet Protocol Suite*
RFC 1413, *Identification Protocol*
RFC 1490, *Multiprotocol Interconnect Over Frame Relay*
RFC 1541, *Dynamic Host Configuration Protocol*
RFC 1542, *Clarifications and Extensions for the Bootstrap Protocol*
RFC 1552, *The PPP Internet Packet Exchange Control Protocol (IPXCP)*
RFC 1587, *OSPF NSSA Options*
RFC 1597, *Address Allocations for Private Internets*
RFC 1627, *Network 10 Considered Harmful (Some Practices Shouldn't be Codified)*
RFC 1634, *Novell IPX Over Various WAN Media (IPXWAN)*
RFC 1661, *The Point-to-Point Protocol (PPP)*
RFC 1700, *Assigned Numbers*
RFC 1771, *A Border Gateway Protocol 4 (BGP-4)*
RFC 1812, *Requirements for IP Version 4 Routers*
RFC 1814, *Unique Addresses are Good*
RFC 1818, *Best Current Practices*
RFC 1824, *Requirements for IP Version 4 Routers*
RFC 1825, *Security Architecture for the Internet Protocol*
RFC 1826, *IP Authentication Header*
RFC 1827, *IP Encapsulating Payload*
RFC 1828, *IP Authentication Using Keyed MD5*
RFC 1829, *The ESP DES-CBC Transform*
RFC 1877, *PPP Internet Protocol Control Protocol Extensions for Name Server Addresses*
RFC 1878, *Variable Length Subnet Table for IPv4*
RFC 1918, *Address Allocation for Private Internets*
RFC 1965, *Autonomous System Confederations for BGP*
RFC 1966, *BGP Route Reflection, An Alternative to Full Mesh IBGP*
RFC 1974, *PPP Stac LZS Compression Protocol*
RFC 1990, *The PPP Multilink Protocol (MP)*
RFC 1994, *PPP Challenge Handshake Authentication Protocol (CHAP)*
RFC 1997, *BGP Communities Attribute*
RFC 2003, *IP Encapsulation within IP*
RFC 2104, *HMAC: Keyed-Hashing for Message Authentication*
RFC 2125, *The PPP Bandwidth Allocation Protocol (BAP), The PPP Bandwidth Allocation Control Protocol (BACP)*
RFC 2138, *Remote Authentication Dial In User Service (RADIUS)*
RFC 2139, *RADIUS Accounting*
RFC 2178, *OSPF Version 2*

Books

Building Internet Firewalls. D. Brent Chapman and Elizabeth D. Zwicky. Sebastopol, CA: O'Reilly & Associates, Inc., 1995. (ISBN 1-56592-124-0)

DNS and BIND, 2nd ed. Paul Albitz and Cricket Liu. Sebastopol, CA: O'Reilly & Associates, Inc., 1992. (ISBN 1-56592-236-0)

Firewalls and Internet Security: Repelling the Wily Hacker. William R. Cheswick and Steven M. Bellovin. Reading, MA: Addison-Wesley Publishing Company, 1994. (ISBN 0-201-63357-4) (Japanese translation: ISBN 4-89052-672-2). Errata are available at **ftp://ftp.research.att.com/dist/internet_security/firewall.book**.

Internet Routing Architectures. Bassam Halabi. San Jose, CA: Cisco Press, 1997. (ISBN 1-56205-652-2)

Internetworking with TCP/IP, Volume 1: Principles, Protocols, and Architecture. Douglas Comer. Prentice Hall, Inc. 1995. (ISBN 0-13-216987-8 (v.1))

Routing in the Internet. Christian Huitema. Upper Saddle River, NJ: Prentice Hall PTR, 1995. (ISBN 0-13-132192-7)

TCP/IP Illustrated, Volume 1: The Protocols. W. Richard Stevens. Reading, MA: Addison-Wesley Publishing Company. 1994. (ISBN 0-201-63346-9)

TCP/IP Network Administration. Craig Hunt. Sebastopol, CA: O'Reilly & Associates, Inc. 1994. (ISBN 0-937175-82-X)

Document Conventions

The following conventions are used in this guide:

Convention	Use	Examples
Bold font	Indicates a user entry—a command, menu option, button, or key—or the name of a file, directory, or utility, except in code samples.	<ul style="list-style-type: none">• Enter version to display the version number.• Press Enter.• Open the permit_list file.

Convention	Use	Examples
<i>Italic font</i>	Identifies a command-line placeholder. Replace with a real name or value.	<ul style="list-style-type: none"> • set <i>Ether0</i> address <i>Ipaddress</i> • Replace <i>Area</i> with the name of the OSPF area.
Square brackets ([])	Enclose optional keywords and values in command syntax.	<ul style="list-style-type: none"> • set nameserver [2] <i>Ipaddress</i> • set <i>S0</i> destination <i>Ipaddress</i> [<i>Ipmask</i>]
Curly braces ({ })	Enclose a required choice between keywords and/or values in command syntax.	set syslog <i>Logtype</i> {[disabled] [<i>Facility.Priority</i>]}
Vertical bar ()	Separates two or more possible options in command syntax.	<ul style="list-style-type: none"> • set <i>S0 W1</i> ospf on off • set <i>S0</i> host default prompt <i>Ipaddress</i>

Document Advisories



Note – means take note. Notes contain information of importance or special interest.



Caution – means be careful. You might do something—or fail to do something—that results in equipment failure or loss of data.



Warning – means danger. You might do something—or fail to do something—that results in personal injury or equipment damage.

Contacting Lucent Remote Access Technical Support

The PortMaster comes with a 1-year hardware warranty.

For all technical support requests, record your PortMaster ComOS version number and report it to the technical support staff or your **authorized sales channel partner**.

New releases and upgrades of PortMaster software are available by anonymous FTP from **<ftp://ftp.livingston.com.pub/le/>**.

In North America you can schedule a 1-hour software installation appointment by calling the technical support telephone number listed below. Appointments must be scheduled at least one business day in advance.

For the EMEA Region

If you are an Internet service provider (ISP) or other end user in Europe, the Middle East, Africa, India, or Pakistan, contact your local Lucent Remote Access sales channel partner. For a list of authorized sales channel partners, see the World Wide Web at **<http://www.livingston.com/International/EMEA/distributors.shtml>**.

If you are an authorized Lucent Remote Access sales channel partner in this region, contact the Lucent Remote Access EMEA Support Center Monday through Friday between the hours of 8 a.m. and 8 p.m. (GMT+1), excluding French public holidays.

- By voice, dial +33-4-92-92-48-88.
- By fax, dial +33-4-92-92-48-40.
- By electronic mail (email) send mail to **emea-support@livingston.com**.

For North America, Latin America, and the Asia Pacific Region

Contact Lucent Remote Access Monday through Friday between the hours of 7 a.m. and 5 p.m. (GMT -8).

- By voice, dial 800-458-9966 within the United States (including Alaska and Hawaii), Canada, and the Caribbean, or +1-925-737-2100 from elsewhere.
- By fax, dial +1-925-737-2110.
- By email, send mail as follows:

- From North America and Latin America to **support@livingston.com**.
- From the Asia Pacific Region to **asia-support@livingston.com**.
- Using the World Wide Web, see **<http://www.livingston.com/>**.

PortMaster Training Courses

Lucent Remote Access offers hands-on, technical training courses on PortMaster products and their applications. For course information, schedules, and pricing, visit the Lucent Remote Access website at **<http://www.livingston.com>**, click **Services**, and then click **Training**.

Subscribing to PortMaster Mailing Lists

Lucent Remote Access maintains the following Internet mailing lists for PortMaster users:

- **portmaster-users**—a discussion of general and specific PortMaster issues, including configuration and troubleshooting suggestions. To subscribe, send email to **majordomo@livingston.com** with **subscribe portmaster-users** in the body of the message.

The mailing list is also available in a daily digest format. To receive the digest, send email to **majordomo@livingston.com** with **subscribe portmaster-users-digest** in the body of the message.

- **portmaster-radius**—a discussion of general and specific RADIUS issues, including configuration and troubleshooting suggestions. To subscribe, send email to **majordomo@livingston.com** with **subscribe portmaster-radius** in the body of the message.

The mailing list is also available in a daily digest format. To receive the digest, send email to **majordomo@livingston.com** with **subscribe portmaster-radius-digest** in the body of the message.

- **portmaster-announce**—announcements of new PortMaster products and software releases. To subscribe, send email to **majordomo@livingston.com** with **subscribe portmaster-announce** in the body of the message. All announcements to this list also go to the portmaster-users list. You do not need to subscribe to both lists.

Introduction to RADIUS

The Remote Authentication Dial-In User Service (RADIUS) is a client/server security protocol created by Lucent Remote Access. RADIUS is a proposed Internet official protocol standard. See RFCs 2138, 2139, and 2200 for more information.

User profiles are stored in a central location, known as the RADIUS server. RADIUS clients (such as a PortMaster communications server) communicate with the RADIUS server to authenticate users. The server specifies back to the client what the authenticated user is authorized to do. Although the term **RADIUS** refers to the network protocol that the client and server use to communicate, it is often used to refer to the entire client/server system.

Overview of RADIUS Features

RADIUS offers the following features:

- Security

In large networks, security information can be scattered throughout the network on different devices. RADIUS allows user information to be stored on one host, minimizing the risk of security loopholes. All authentication and access to network services is managed by the host functioning as the RADIUS server.

- Flexibility

RADIUS software from Lucent Remote Access—version 2.0 and higher—can be used with any communications server that supports the RADIUS protocol as long as you own at least one Lucent Remote Access hardware product. For more information see the Livingston Enterprises Software Licensing Agreement at **<ftp://ftp.livingston.com/pub/le/LICENSE>**.

- Simplified management

The RADIUS server stores security information in text files at a central location; you add new users to the database or modify existing user information by editing these text files. You can use scripts, templates, and automated processes to further simplify management.

- Extensive auditing capabilities

RADIUS provides extensive audit trail capabilities, referred to as **RADIUS accounting**. Information collected in a log file or database can be analyzed for security purposes or used for billing.

The RADIUS for NT 2.0.1 server is available for the following operating systems:

- Windows NT Workstation 4.0
- Windows NT Server 4.0

How RADIUS Works

RADIUS performs three primary functions. The RADIUS server version 2.0.1 for Windows NT adds enhancements for ease of use.

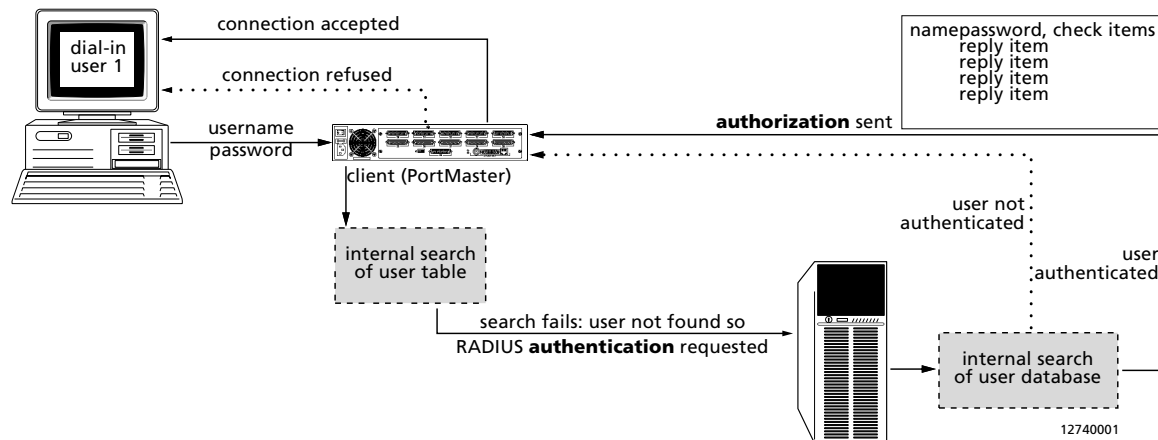
Basic RADIUS Functions

The primary functions of RADIUS are authentication, authorization, and accounting. Figure 1-1 shows authentication and authorization.

- Authentication

RADIUS authenticates users for dial-in remote access. Authentication information is stored in a local **users** file or accessed from external authentication mechanisms, such as a Windows NT User Manager or SecurID ACE/Server database.

Figure 1-1 RADIUS Authentication and Authorization



For example, when user *bob* attempts to log in to a PortMaster, the following authentication sequence takes place:

1. The PortMaster prompts *bob* for his username and password, and then compares the username-password pair to the PortMaster user table.
2. The PortMaster sends an **access-request** message to the RADIUS server if the following conditions are met:
 - Username is not found in the user table
 - Security for the port is set to **on**
 - RADIUS server is set

The access-request message contains the information necessary for the RADIUS server to authenticate the user.

3. The RADIUS server checks its database to determine if user *bob* is present. For *bob*'s login to be successful, a matching username and password must be found in the RADIUS database.
4. User *bob* is either accepted or rejected:
 - If a matching entry is found in the RADIUS **users** file, if the password requirement is met, and if all check items in the **users** file are matched by additional attributes in the access-request message, the RADIUS server sends an **access-accept** message to the PortMaster indicating that *bob* has been

successfully authenticated. It also sends authorization information—reply items—about the services *bob* can access and configuration information about *bob*'s connection.

- If the password request is not satisfied or if other check items—required in the RADIUS users file—fail, the RADIUS server sends an **access-reject** packet to the PortMaster indicating that the authentication attempt has failed. The PortMaster terminates *bob*'s connection attempt.

If third-party security software—such as SecurID—is used, the user is prompted for more information before being accepted or rejected.

- Authorization

Authorization controls access to specific services on the network. Once a user is authenticated, RADIUS reports to the PortMaster what a user is authorized (permitted) to access. For example, user *bob* might be authorized to use the Point-to-Point protocol (PPP) for his connection, use IP address 192.168.200.4, and filter his traffic using a packet filter.

- Accounting

RADIUS accounting collects usage information for dial-in users. This information is often used for billing purposes. See Chapter 8, “Implementing RADIUS Accounting,” for more information.

Ease-of-Use Enhancements

RADIUS 2.0.1 for Windows NT provides the following enhancements to improve RADIUS functionality:

- Account disabling

The Auth-Type check item can reject a user's authentication attempt without having to delete the user profile from the **users** file. To do this, include Auth-Type = Reject in the user profile check items.

Auth-Type = Reject can also be used to prevent standard system IDs from being used by DEFAULT entries, such as Administrator, Guest, and other IDs made available by the Windows NT operating system.

- Password encryption

The Crypt-Password check item enables you to store user passwords in the UNIX CRYPT format. Encrypted passwords can be used with scripted logins or with the Password Authentication Protocol (PAP). They cannot be used with the Challenge Handshake Authentication Protocol (CHAP).

- Maximum connection rate

The Connect-Rate check item specifies the maximum connection rate permitted for a user. This item is functional on PortMaster 3 products running ComOS version 3.7 or higher.

- Restriction of authentication to groups of users

The Group check item restricts authentication to the users defined as members of the specified group. The Auth-Type check item must be set to **System**.

- Longer passwords

Local user passwords can now be up to 48 characters in length.

- ODBC compatibility

On the Windows NT platform, the RADIUS accounting server can store RADIUS accounting records directly to a database using open database connectivity (ODBC), in addition to the standard flat text file. You can access the data in the database using structured query language (SQL).

- Administrative logins

New Service-Type reply items enable you to grant full or limited administrative abilities to login users. The Service-Type = Administrative-User reply item grants the user full configuration ability and access to all PortMaster commands. The Service-Type = NAS-Prompt-User reply item grants the user limited administrative ability, but no configuration ability.

- Additional check items

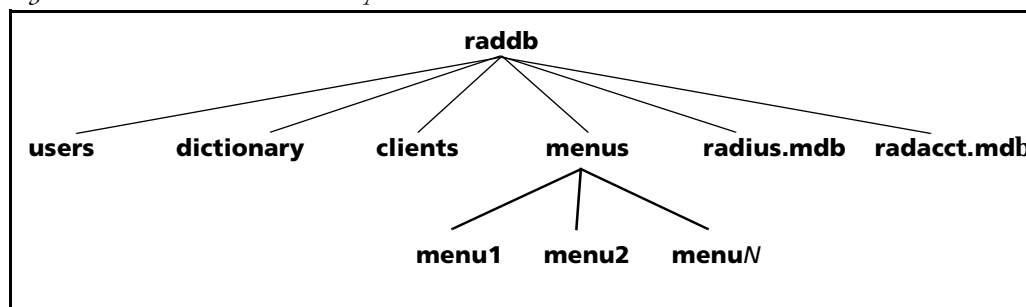
You can use the number the user has called—**Called-Station-Id**—and the number the user is calling from—**Calling-Station-Id**—as check items if the RADIUS client is capable of sending them in an access-request. The PortMaster must be running ComOS 3.7 or later. Called-Station-Id and Calling-Station-Id are supported over an ISDN Primary Rate Interface (PRI) on a PortMaster 3, and over an ISDN Basic Rate Interface (BRI) on other PortMasters.

RADIUS Directory Structure

RADIUS server files are stored in the **raddb** (RADIUS database) directory. The RADIUS for NT installer places the RADIUS files in the **C:\winnt\system32\drivers\etc** folder by default. Lucent Remote Access recommends that you use this default.

The **raddb** directory contains files and one subdirectory organized as shown in Figure 1-2 and explained in the list that follows.

Figure 1-2 RADIUS Directory Structure



- The **users** file stores user profiles, which consist of authentication and authorization information for all users authenticated by RADIUS.
- The **dictionary** file contains definitions of all the attributes and values used to authenticate and authorize users. The dictionary also includes RADIUS accounting attributes. After you modify this file, you must restart RADIUS to apply your changes.
- The **clients** file contains the IP addresses of all RADIUS clients and the secrets shared between the clients and the RADIUS server(s).
- The **menus** subdirectory contains individual menu text files. You can optionally use menus to provide users with different login options once the users have been authenticated.
- The **radius.mdb** file contains the table definitions so that you can add authentication records to the RADIUS database.
- The **radacct.mdb** file contains the table definitions so that you can add accounting records to the RADIUS database.

The RADIUS server uses the User Datagram Protocol (UDP) and the following UDP ports:

- Port 1645 for authentication
- Port 1646 for accounting

You can specify different UDP ports by modifying the `\etc\services` file on Windows NT hosts. See Appendix B, “RADIUS Actions,” for more information.



Note – PortMasters use ports 1645 and 1646 by default; this is specified by ComOS and cannot be modified in ComOS versions prior to 3.8. If you change the port number as stated above, RADIUS might work with other network access servers (NASs) but cannot authenticate users or gather accounting data for sessions on PortMasters.

RADIUS Installation and Configuration

Table 1-1 provides a quick overview of the tasks required to install and configure RADIUS.

Table 1-1 Overview of RADIUS Installation and Configuration Tasks

Task	Instructions
1. Select a host to use as the RADIUS server.	See “Getting Started” on page 2-1.
2. Install the RADIUS server software on the host.	See “Installing RADIUS on a Windows NT Host” on page 2-3 and “Configuring RADIUS on a Windows NT Host” on page 2-10.
3. Configure client information on the RADIUS server.	See “Modifying the Clients File” on page 3-3.
4. Configure the PortMaster as a RADIUS client.	See one of the following: <ul style="list-style-type: none">• “Configuring the PortMaster Using the Command Line Interface” on page 3-3.• “Configuring the PortMaster Using PMVision or PMconsole” on page 3-5.

Table 1-1 Overview of RADIUS Installation and Configuration Tasks (*Continued*)

Task	Instructions
6. Configure user profiles and test representative user profiles	See Chapter 4, "Configuring User Information," and Chapter 5, "Using RADIUS for NT Utilities."
7. You can optionally define menus to enable authenticated users to select different login options.	See Chapter 6, "Configuring RADIUS Menus."
8. You can optionally install and configure SecurID. ¹	See Chapter 7, "Installing and Configuring SecurID."
9. Configure RADIUS accounting.	See Chapter 8, "Implementing RADIUS Accounting."

1. This installation requires ACE/Server and ACE/Client software.

This chapter includes the following topics:

- “Getting Started” on page 2-1
- “Installing RADIUS on a Windows NT Host” on page 2-3
- “Configuring RADIUS on a Windows NT Host” on page 2-10
- “Associating Your Database with the ODBC Driver” on page 2-26
- “Server Utilities” on page 2-29
- “RADIUS Menu Bar” on page 2-30

Getting Started

Before installing and configuring RADIUS software, select a host or hosts to use as a RADIUS server and determine one or more shared secrets for authentication.

Selecting a RADIUS Server Host

Primary RADIUS Authentication Server. Select or create a host with the following characteristics to use as a RADIUS authentication server:

- Secure physical location
- Root—administrative—access limited to the security officer or system administrator
- Limited number of user accounts—preferably none
- Basic memory and disk space
- Database support with the appropriate open database connectivity (ODBC) drivers installed

Lucent Remote Access suggests the following additional characteristics for the host:

- Inaccessibility from outside your local network

- Absence of public network services such as email, FTP, HTTP, netnews, Telnet, rlogin, and rcp.



Warning – RADIUS performance varies with the number of users being authenticated and with other demands on the server. Running public network services or other applications on the server concurrently with RADIUS for Windows NT can consume most of your CPU resources. You can experience a reduction in performance—such as access denials or dropped calls—if you have insufficient CPU resources. Lucent Remote Access strongly recommends that you do **not** run a Web server on the RADIUS for Windows NT server; if you do, you can be attacked by multiple hits on the Web server, adversely affecting RADIUS processes.

Lucent Remote Access recommends the following minimum hardware requirements:

- Pentium 166 CPU with 64MB of RAM and a 2GB of disk space. RADIUS for Windows NT requires 10MB free disk space for installation.
- 50MB hard disk space per 1000 users per month. If you archive accounting records on the server, you must allocate more storage than this minimum. Keep in mind that allocating too much space is preferable to allocating too little; your usage can vary.

RADIUS accounting data continues to grow unless you archive this information on a regular schedule—weekly or monthly, for example. Lucent Remote Access recommends you maintain no more than 3 months of raw accounting data and 6 months of processed billing data on the primary server.

Secondary RADIUS Authentication Server. Lucent Remote Access recommends the use of a secondary RADIUS server. The PortMaster always queries the primary RADIUS server first; if the server does not respond, it is queried a second time. Then both the primary and secondary servers are queried up to eight more times at 3-second intervals until one responds or until 3 seconds after the tenth query without a response.

RADIUS Accounting Server. If you implement RADIUS accounting, you must also select one or more RADIUS accounting servers. The RADIUS accounting server can be located on the same host as the RADIUS server used for authentication, or on a separate host. See Chapter 8, “Implementing RADIUS Accounting,” for more information.

Secondary RADIUS Accounting Server. You can define a secondary accounting server to serve as a backup if the primary server cannot be contacted. The PortMaster always sends accounting packets to the primary RADIUS accounting server first, and retries it once every 45 seconds. If the primary server does not respond within 10 minutes, or if more than 50 accounting packets are waiting to be sent, the PortMaster sends the accounting packets to the secondary RADIUS accounting server.

Determining a Shared Secret

Each PortMaster using RADIUS and its RADIUS server(s) share an authentication key—called the **shared secret**—that consists of up to 15 printable, nonspace, ASCII characters. Each PortMaster can share a different secret with the RADIUS server, or multiple PortMasters can share the same secret. Different, nontrivial shared secrets are recommended for each PortMaster.

You configure the shared secret on each RADIUS server and the PortMaster. It is stored as clear text in the **clients** file on the RADIUS server and in the nonvolatile memory of the PortMaster. See Chapter 3, “Adding a RADIUS Client,” for more information.

Installing RADIUS on a Windows NT Host

Prerequisites

You are responsible for providing, properly installing, and configuring a structured query language (SQL) database for storing user information **before** you install RADIUS for Windows NT.

You must install the following Microsoft software on your Windows NT host or RADIUS for Windows NT will not work properly:

- Windows Service Pack 3 available for download at
<http://support.microsoft.com/Support/NTServer/Content/ServicePacks/>
- Microsoft Data Access Components 1.5 available for download at
<http://www.microsoft.com/data/mdac15.htm>

Use the **radiusnt.exe** file to install RADIUS for Windows NT. The file is available via anonymous FTP from **<ftp://ftp.livingston.com/pub/le/software/pc>** and on the Lucent Remote Access *PortMaster Software CD*.



Note – Always use the latest **radiusnt.exe** file, available from the Lucent Remote Access FTP site.

Preparation

Before installing RADIUS, you must log in to your Windows NT server or workstation as a member of a group having default administrator rights and the additional following rights:

- Act as part of the operating system
- Increase quotas
- Replace a process level token

Typically, you assign these additional rights to the Administrators group and ensure that you are a member of that group.



Note – Some users may choose to have some group other than Administrators manage the RADIUS server. You might choose to create a new group specifically for RADIUS administration. If you do this, then substitute that group name for Administrators and ensure that it has all the default Administrators rights as well as the additional rights specified above.

To determine what rights are assigned to a group, perform the following steps:

1. **Click the Windows NT Start button and select**
Programs⇒Administrative Tools (Common)⇒User Manager.

The User Manager window appears.

2. **Select Policies⇒User Rights from the menu bar.**

The User Rights Policy dialog box appears.

3. **Select** Show Advanced User Rights.

4. **Select a right from the drop-down list.**

The groups to which the right have been assigned appear in the browser below the list.

To configure the Administrator login with these rights, perform the following steps:

1. **Click the Windows NT Start button and select**
Programs⇒Administrative Tools (Common)⇒User Manager.

The User Manager window appears.

2. **Select Policies⇒User Rights... from the menu bar.**

The User Rights Policy dialog box appears.

3. **Select Show Advanced User Rights.**
4. **Select Act as part of the operating system from the drop-down list.**
5. **Click Add... to display the Add Users and Groups dialog box.**
6. **Select Administrators in the browser, and click Add; then click OK.**

This returns you to the User Rights Policy dialog box.

7. **Repeat Steps 3 through 6 for other required advanced rights.**
8. **Click OK in the User Rights Policy dialog box to apply the rights.**

You must also verify that the Windows NT event log is set to overwrite entries. If this is not done, RADIUS may cause problems. To configure the event log, perform the following steps:

1. **Click the Windows NT Start button and select Programs⇒Administrative Tools (Common)⇒Event Viewer.**

The Event Viewer window appears.

2. **Select Log⇒Log Settings... from the menu bar.**

The Event Log Settings dialog box appears.

3. **Select the desired level of event log wrapping.**

Choose one of the following:

- **Overwrite Events as Needed.** This option ensures that all new events are recorded, even if the log is full. When the log is full, the oldest entry in the log is overwritten.
- **Overwrite Events Older Than *n* Days.** This option enables you to protect log entries from being overwritten by new events for any period from 1 to 365 days. New events can overwrite entries older than the specified period.

Installation



Complete the following steps to install RADIUS for Windows NT:

Note – If you are updating to a newer version of RADIUS for Windows NT, you must first uninstall the previous version from your Windows NT server or workstation. Use the RADIUS for Windows NT 2.0.1 **uninstall** utility. This utility removes the previous **radius.mdb** file and overwrites the existing **radsvc.ini** file.

1. Copy radiusnt.exe to an empty directory.

For example, copy **radiusnt.exe** to **C:\temp\rad**.

2. Double-click radiusnt.exe in the Windows Explorer to expand the compressed RADIUS for Windows NT server files.

Alternatively, you can run **radiusnt.exe** from the MS-DOS prompt.

3. Double-click Setup.exe in the Windows Explorer to run the RADIUS for Windows NT setup program.

Alternatively, you can run **setup.exe** from the MS-DOS prompt.

In either case:

- a. Follow the instructions on each screen.

You must restart the host computer before you can run RADIUS for Windows NT.

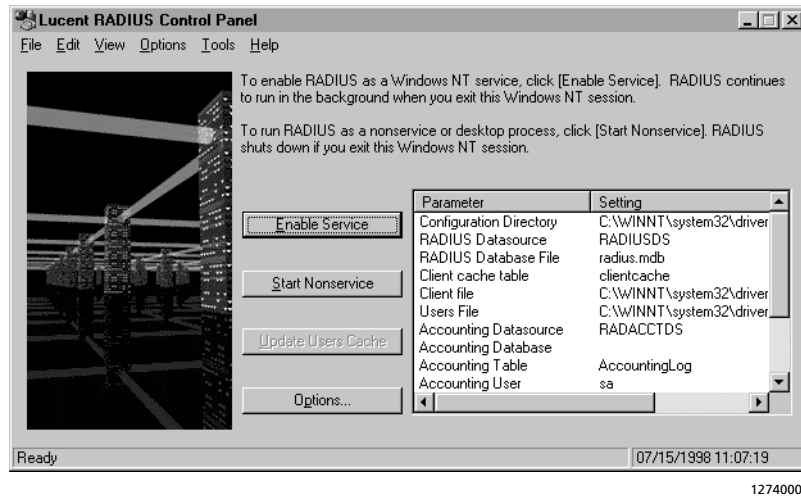
- b. Click **Restart** at the end of the setup program to restart the host computer.

If you do not want to restart the host computer at this time, click **Don't Restart** to close the RADIUS for Windows NT setup wizard.

The RADIUS NT setup program places the RADIUS for Windows NT files in **C:\winnt\system32\drivers\etc** by default. The setup program also creates a **Lucent RADIUS 2.0.1** folder within the Program Manager Start menu.

4. To start RADIUS, click the Windows NT Start button, then select Programs ➔ Lucent RADIUS 2.0.1 ➔ Lucent RADIUS NT.

The RADIUS Control Panel appears.



Note – If you did not properly configure the administrator rights as described in “Preparation” on page 2-4, a pop-up window displays the user rights required to start the RADIUS service. Configure the user rights before continuing with the installation procedure.

5. Decide whether to install RADIUS for Windows NT as a Windows NT service or as a nonservice or desktop process.

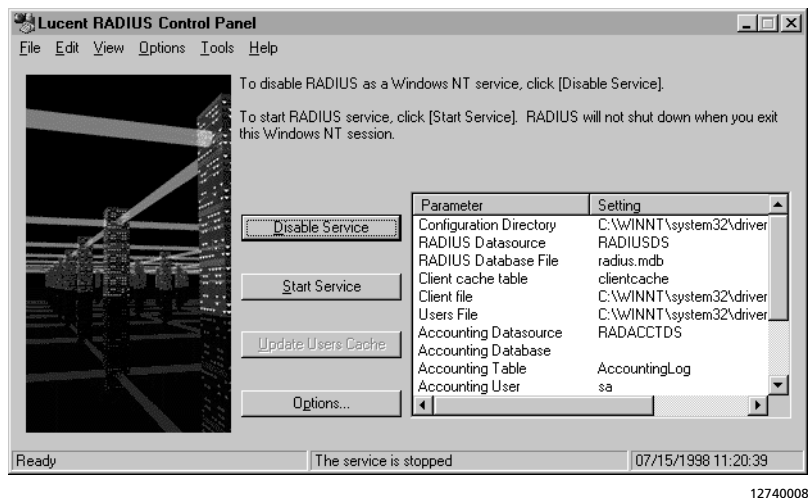
- To run RADIUS as a Windows NT service, go to Step 6 on page 2-7. Running RADIUS as a service enables the server to start automatically when a user logs off the session or when the system is rebooted.
- To run RADIUS as a nonservice, go to Step 7 on page 2-8.



Note – Lucent Remote Access recommends that you run RADIUS for Windows NT as a nonservice until you complete configuration and operational testing of the installation. Thereafter, install RADIUS for Windows NT as a Windows NT service and perform final testing. Running RADIUS in this manner enables you to log off a Windows NT session without affecting the operation of RADIUS; the service continues to run.

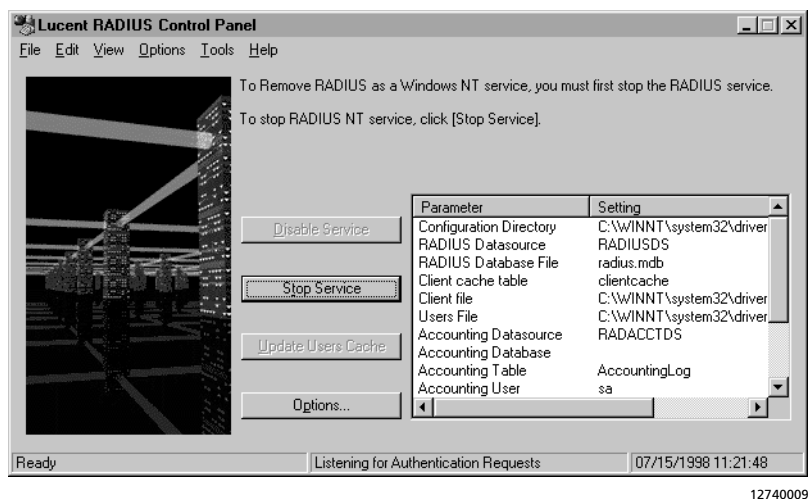
6. To run RADIUS as a Windows NT service, click the **Enable Service** button.

The button label toggles to **Disable Service**.



To start the service, click the **Start Service** button. The button label toggles to **Stop Service**.

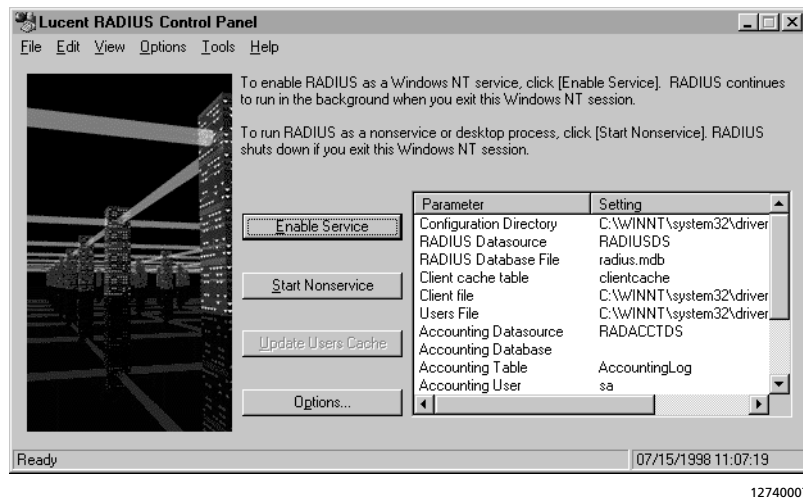
To stop the service, click the **Stop Service** button.



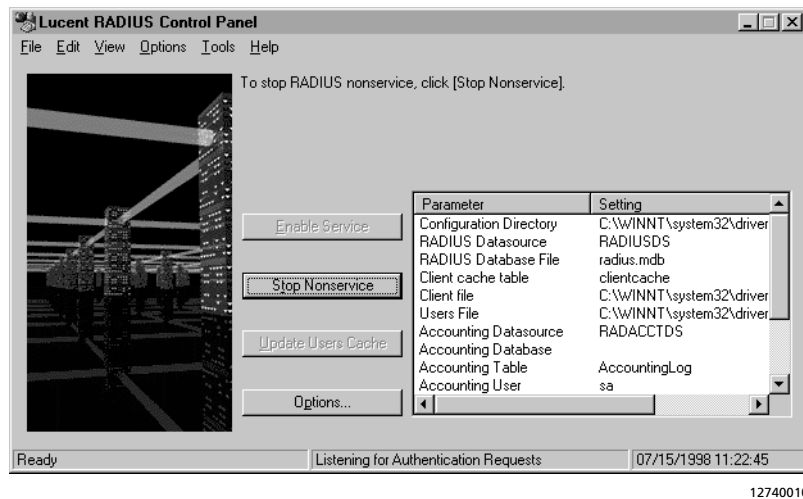
Go to Step 8 on page 2-10.

7. To run RADIUS as a nonservice, click the **Start Nonservice** button.

When installed in this way, RADIUS shuts down when you log off or close the NT session.



To stop RADIUS, click the **Stop Nonservice** button.



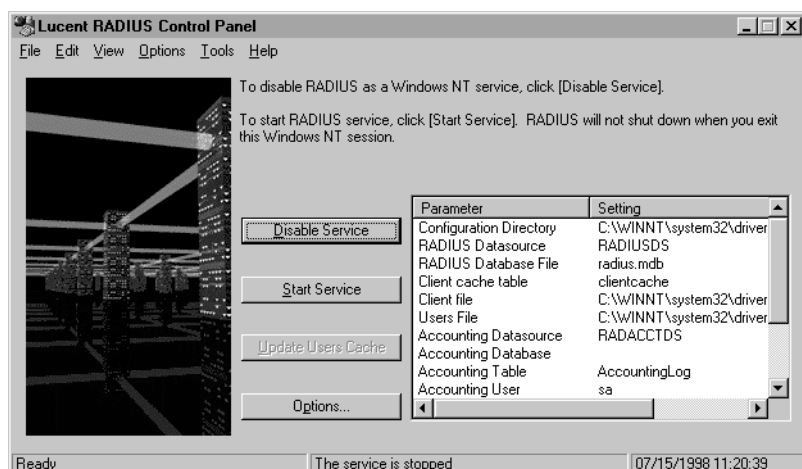
8. If you previously installed RADIUS for Windows NT and selected the option to cache user information, do one of the following if you want to update the users cache:

- Click the **Update Users Cache** button.
- Choose the corresponding menu item from the File menu.

Removing RADIUS as a Service

If you installed RADIUS as a service and want to remove it, do one of the following:

- If RADIUS is running, click **Stop Service**, then click **Disable Service**.
- If RADIUS is not running, click **Disable Service**.



12740008

Configuring RADIUS on a Windows NT Host

You configure RADIUS options from the Logging, Users Cache, Multitask Authentication, Directories, Ports, Queue, Timeout, and Accounting tabs in the RADIUS Options dialog box.

Navigate to the desired tab by one of the following methods:

- From the RADIUS Control Panel, do one of the following:

- Choose the desired option from the Options menu.
- Click the **Options** button to display the RADIUS Options dialog box, and then click the desired tab.
- From the RADIUS Options dialog box, click the desired tab.

When you alter a configuration value in the RADIUS Options dialog box, the **Apply** button becomes operational. You can click on **Apply** to save your changes and leave the window open. Or you can click the **OK** button to save your changes, close the RADIUS Options dialog box, and return to the RADIUS Control Panel. If you click the **Cancel** button, your changes are not saved.

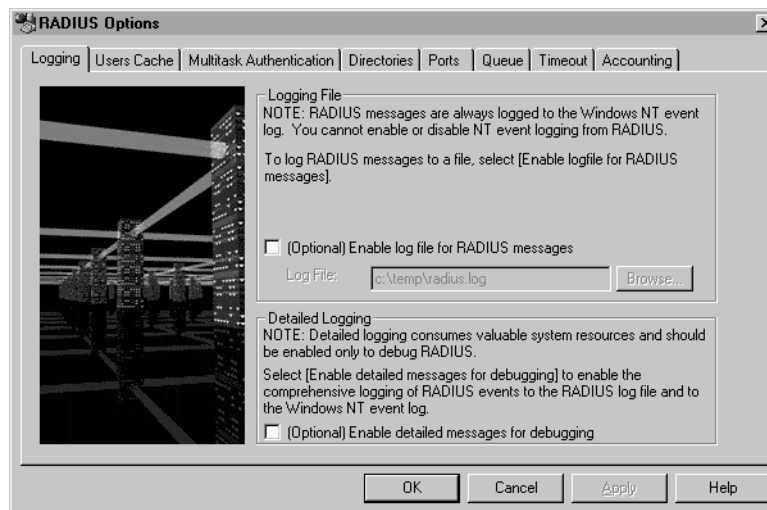


Note – RADIUS for NT uses the settings in effect when it is started. If you make and apply or save configuration changes, you must stop and restart RADIUS NT for the configuration changes to take effect.

Logging RADIUS Messages to a File

To log RADIUS messages to a file for monitoring or debugging purposes, complete the following steps:

1. Display the Logging tab.



12740011

2. Ensure that the Enable logfile for RADIUS messages option is selected.

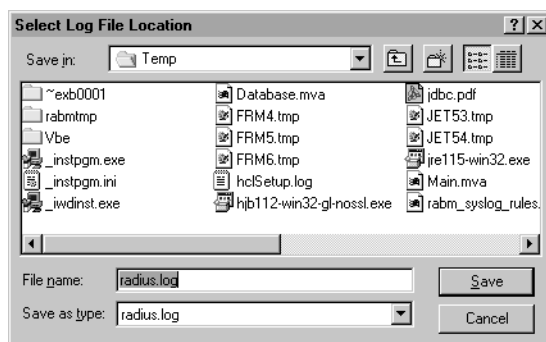


Note – The Windows NT event log is not affected by selecting this option. RADIUS events continue to be logged to the event log.

The location of the log file appears in the text box. By default, the log file **radius.log** is placed in **C:\temp**.

3. To change the location of the log file, do one of the following:

- Enter the filename manually in the text box.
- Click the **Browse** button, select the location, and click **Save** to save the location.



12740012

4. To turn on verbose logging, ensure that the Enable detailed messages for debugging option is selected.

Detailed logging is disabled by default. When you enable detailed (verbose) logging, the messages are stored in the log file and in the event log.

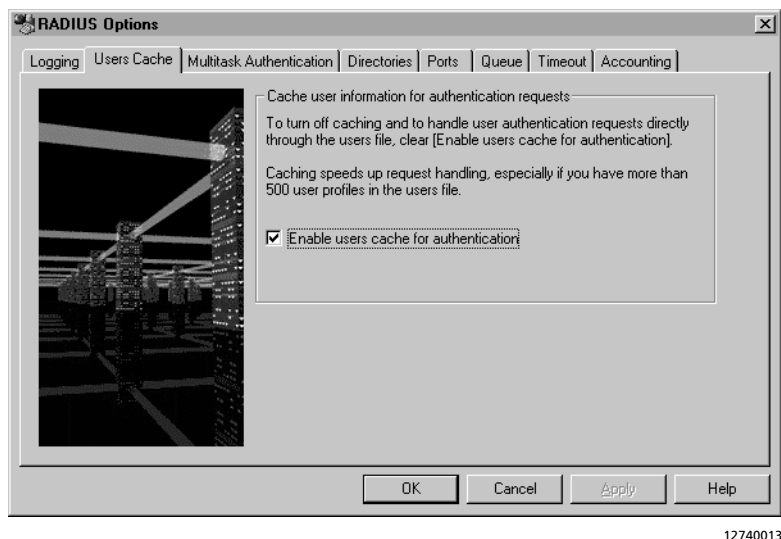
5. Determine whether you have finished configuring the options in the RADIUS Control Panel.

- If you have finished, click the **OK** button to apply your changes and close the RADIUS Options dialog box. Go to Chapter 3, “Adding a RADIUS Client.”
- If you have not finished, click the **Apply** button to apply your changes, and continue configuring options.

Configuring the Users Cache

To configure the users cache, complete the following steps:

1. Display the Users Cache tab.



2. To use the database to cache the users file for fast response to requests, ensure that the Enable users cache for authentication option is selected.

If this option is not selected, the **Update Users Cache** button on the RADIUS Control Panel is disabled and appears dimmed.

Lucent Remote Access recommends that you enable caching of the **users** file when the **users** file contains more than 500 user profiles.

If caching is used, you must update the database each time the **users** file is updated.

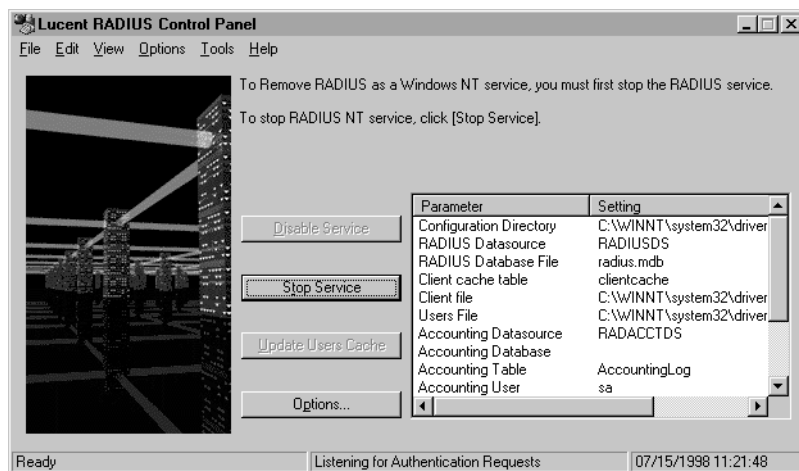
3. To update the database, do one of the following:

- Click the **Update Users Cache** button on the RADIUS Control Panel.
- Choose **Update Users Cache** from the File menu on the RADIUS Control Panel.

- From the command prompt, run the following command:

```
C:\>"\program files\lucent\RADIUS\radsvc.exe" -bulddb
```

You can use this command in a scheduler to update the user cache on a periodic basis or as a part of a script or batch job.



12740009

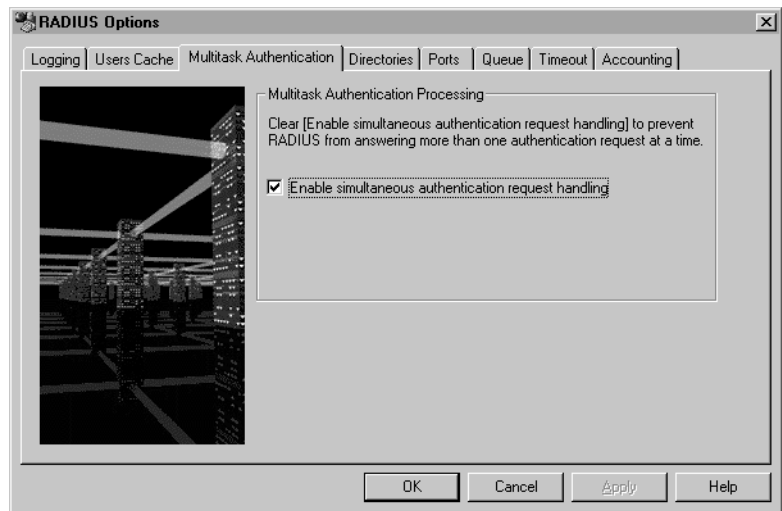
4. Determine whether you have finished configuring the options in the RADIUS Options dialog box.

- If you have finished, click the **OK** button to apply your changes and close the RADIUS Options dialog box. Go to Chapter 3, “Adding a RADIUS Client.”
- If you have not finished, click the **Apply** button to apply your changes, and continue configuring options.

Configuring Multitask Authentication

When multitask authentication is on, RADIUS for Windows NT handles multiple, simultaneous authentication requests. To configure multitask authentication, complete the following steps:

1. **Display the Multitask Authentication tab.**



12740014

2. **To turn on multitask authentication, ensure that the Enable simultaneous authentication request handling option is selected.**

To turn off multitask authentication, uncheck this option.

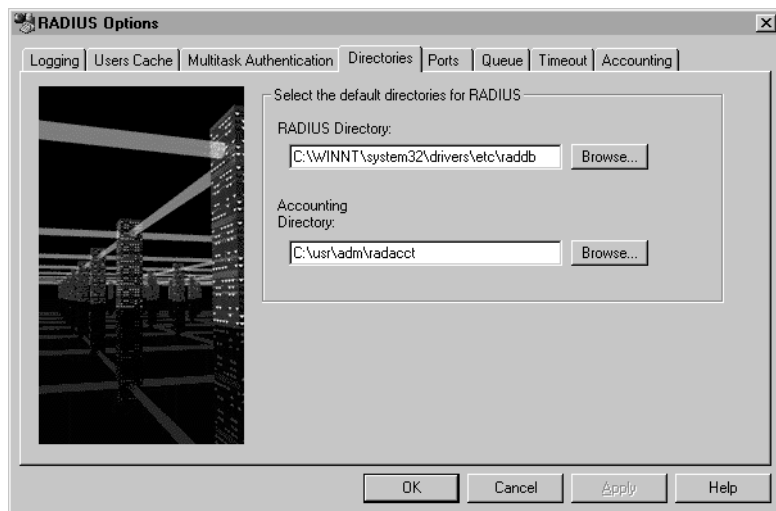
3. **Determine whether you have finished configuring the options in the RADIUS Options dialog box.**

- If you have finished, click the **OK** button to apply your changes and close the RADIUS Options dialog box. Go to Chapter 3, "Adding a RADIUS Client."
- If you have not finished, click the **Apply** button to apply your changes, and continue configuring options.

Changing the Default Directories

To change the default directories for RADIUS server and accounting files, complete the following steps:

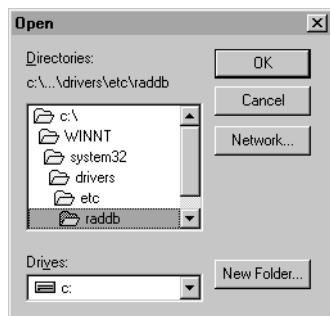
1. Display the Directories tab.



12740015

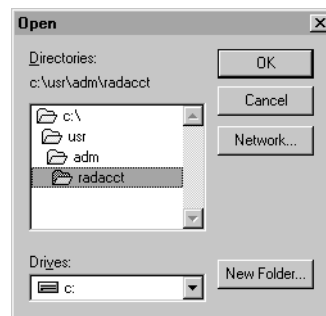
2. Enter the desired directory locations manually in the text boxes, or click the Browse button and select the desired directory locations.

RADIUS Directory



12740016

Accounting Directory



12740017

C:\winnt\system32\drivers\etc\raddb is the default RADIUS for Windows NT directory. The default accounting directory is **C:\usr\adm\radacct**.

RADIUS for Windows NT automatically creates a subdirectory within the **C:\usr\adm\radacct** directory for each PortMaster serving as a PortMaster accounting client.

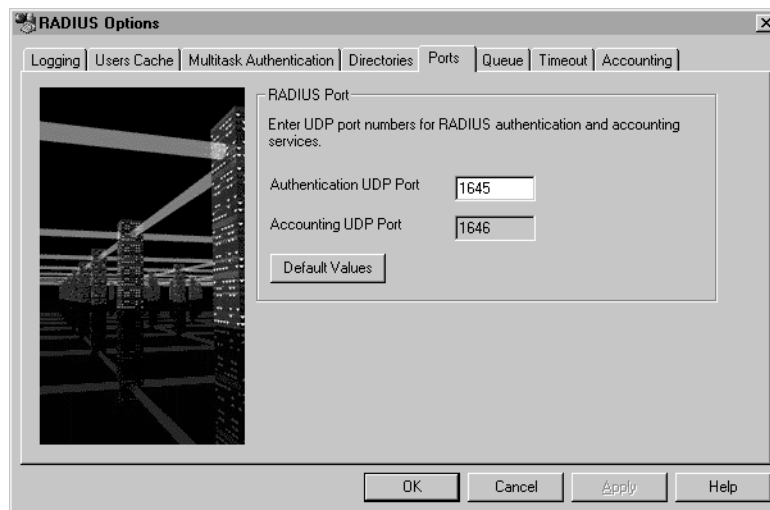
3. Determine whether you have finished configuring the options in the RADIUS Options dialog box.

- If you have finished, click the **OK** button to apply your changes and close the RADIUS Options dialog box. Go to Chapter 3, “Adding a RADIUS Client.”
- If you have not finished, click the **Apply** button to apply your changes, and continue configuring options.

Changing RADIUS Ports

By default, RADIUS uses port 1645 for the authentication service and port 1646 for the accounting service. If other services are using these ports, you must change the ports those services use or change the port values for RADIUS for Windows NT. To change these values, complete the following steps:

1. Display the Ports tab.



12740048

2. Enter the desired port value in the Authentication UDP Port field.

The RADIUS accounting port is always one greater than the authentication port. When you change the authentication port value, the accounting port value automatically increases by one. You cannot edit the accounting value.

3. Click OK.

To restore the default port values, click **Default Values** and then click **OK**.

4. Determine whether you have finished configuring the options in the RADIUS Options dialog box.

- If you have finished, click the **OK** button to apply your changes and close the RADIUS Options dialog box. Go to Chapter 3, “Adding a RADIUS Client.”
- If you have not finished, click the **Apply** button to apply your changes, and continue configuring options.

Setting the Authentication Request Queue Size

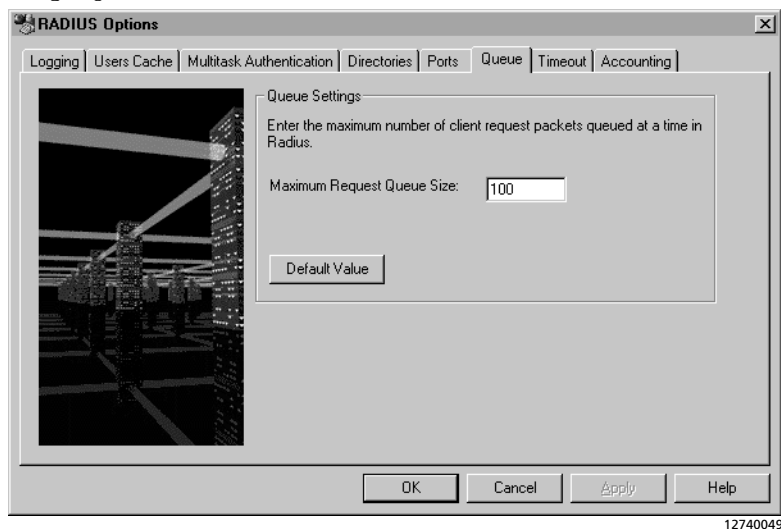
You can specify the maximum number of request packets from the client that RADIUS can queue at any given time. The default value is 100 packets.



Note – Lucent Remote Access recommends you do not modify the authentication request queue value unless instructed to do so by Technical Support.

To specify the queue size, complete the following steps:

1. Display the Queue tab.



2. Enter the desired value in the **Maximum Request Queue Size** field.

3. Click **OK**.

To restore the default queue value, click **Default Value** and then click **OK**.

4. **Determine whether you have finished configuring the options in the RADIUS Options dialog box.**

- If you have finished, click the **OK** button to apply your changes and close the RADIUS Options dialog box. Go to Chapter 3, “Adding a RADIUS Client.”
- If you have not finished, click the **Apply** button to apply your changes, and continue configuring options.

Setting the Request Packet Timeout

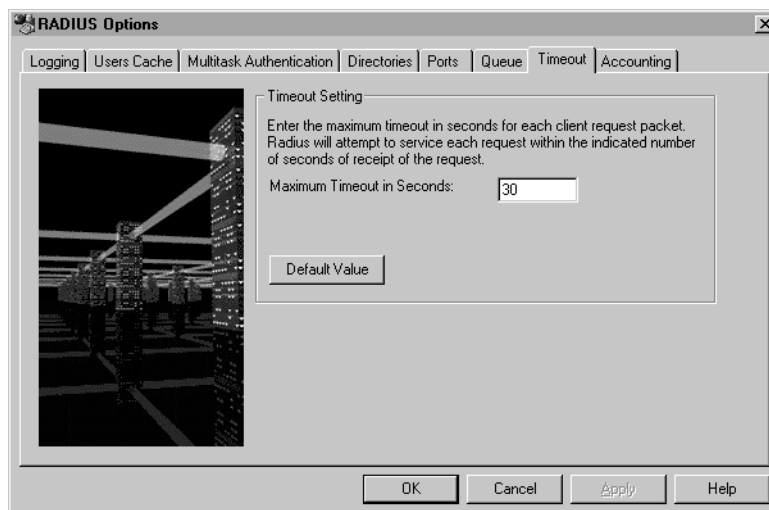
You can specify the maximum timeout allowed for each request packet from the client. The default value is 30 seconds.



Note – Lucent Remote Access recommends you do not modify the maximum timeout value unless instructed to do so by Technical Support.

To specify the timeout value, complete the following steps:

1. **Display the Timeout tab.**



12740050

2. Enter the desired value in the **Maximum Timeout in Seconds** field.
3. Click **OK**.

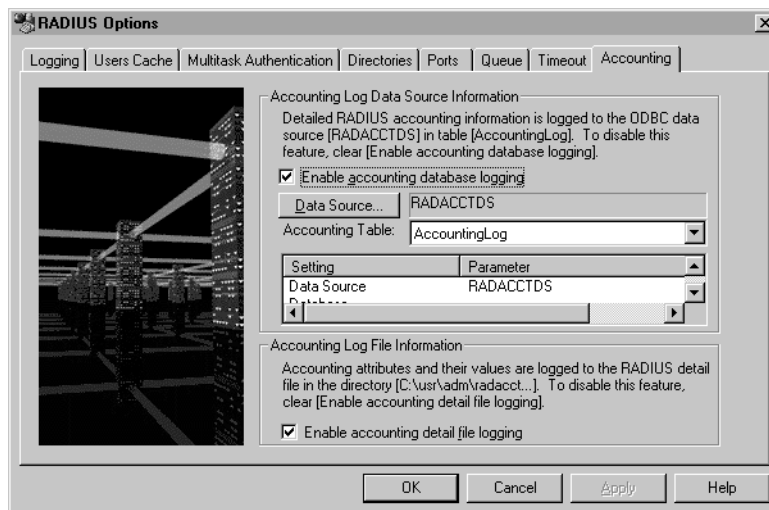
To restore the default timeout value, click **Default Value** and then click **OK**.

4. **Determine whether you have finished configuring the options in the RADIUS Options dialog box.**
 - If you have finished, click the **OK** button to apply your changes and close the RADIUS Options dialog box. Go to Chapter 3, “Adding a RADIUS Client.”
 - If you have not finished, click the **Apply** button to apply your changes, and continue configuring options.

Configuring RADIUS Accounting

To configure RADIUS accounting, complete the following steps:

1. **Display the Accounting tab.**



12740018

When accounting database logging is on, RADIUS for Windows NT logs detailed RADIUS accounting information to the open database connectivity (ODBC) data source in the specified table.

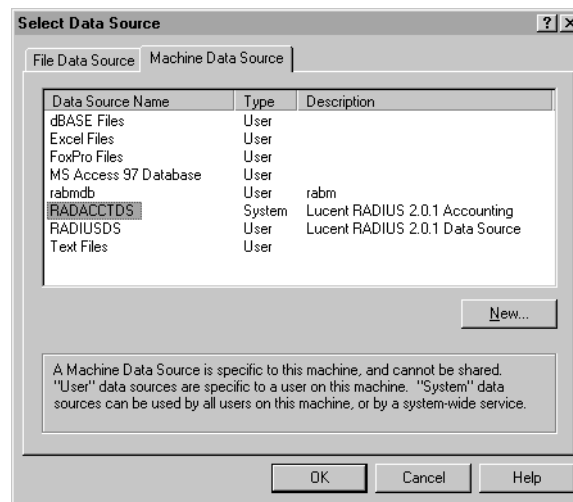
2. Set accounting database logging.

- To turn on accounting database logging, ensure that the **Enable accounting database logging** option is selected.
- To turn off accounting database logging, clear this option.

3. Specify the ODBC data source by clicking Data Source....

The Select Data Source dialog box appears.

4. Select the Machine Data Source tab.



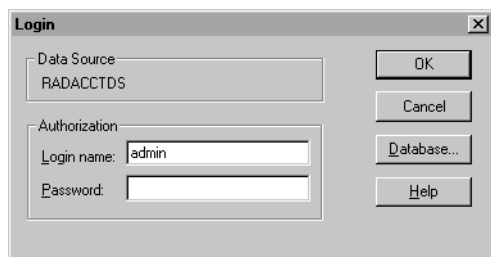
12740019



Note – The machine data source is specific to your server and cannot be shared. If you have selected a file data source, RADIUS might not appear to the system as a service. Selecting a file data source generates an error window and the data source is rejected.

5. Select the *RADACCTDS* data source name and click OK.

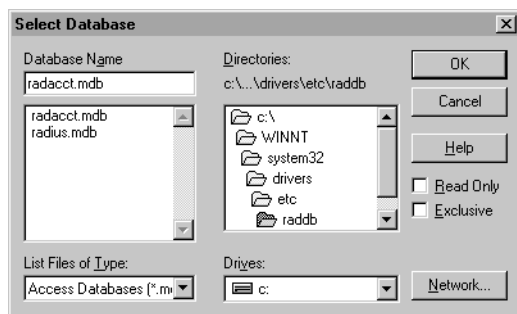
6. The Login dialog box appears.



12740020

7. Click Database....

The Select Database dialog box appears.

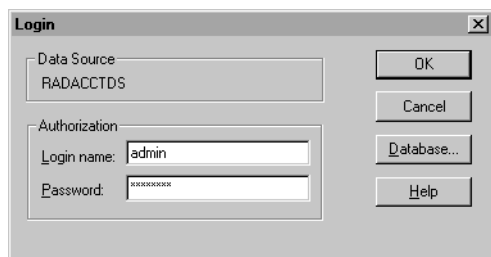


12740021

8. Verify the radacct.mdb database is selected and click OK.

The installed path for this is **C:\winnt\system32\drivers\etc\raddb**. You are returned to the Login dialog box.

9. Enter your administrator's Login Name and Password, and click OK.

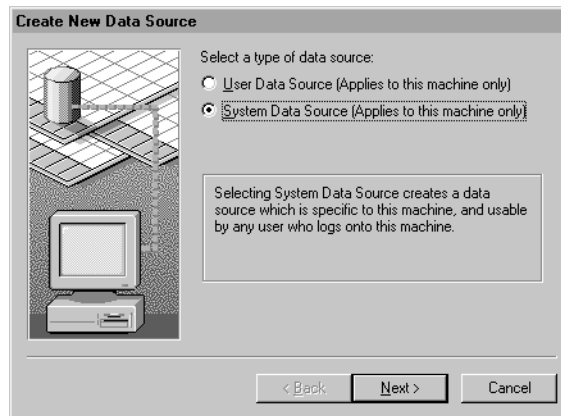


12740047

This fulfills database sign-on requirements and enables the RADIUS server to access the database as a database user.

You can create new data sources by clicking **New** in the Select Data Source dialog box and following the directions in each subsequent dialog box. This enables you to use ODBC-compliant databases other than Microsoft Access. Or you could create another accounting database for RADIUS to use while you are working on the original database.

When RADIUS is enabled as a Windows NT service, the server considers the system—rather than you, the logged-in user—to be running RADIUS.

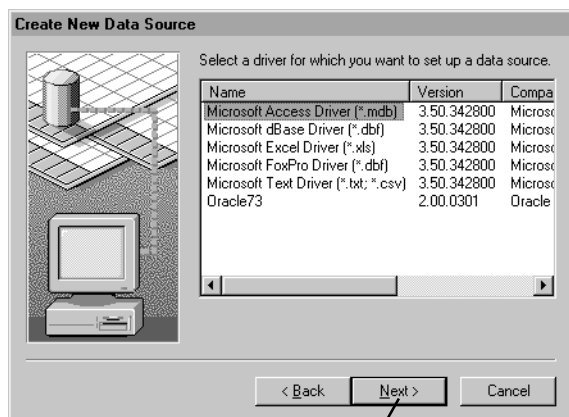


12740023

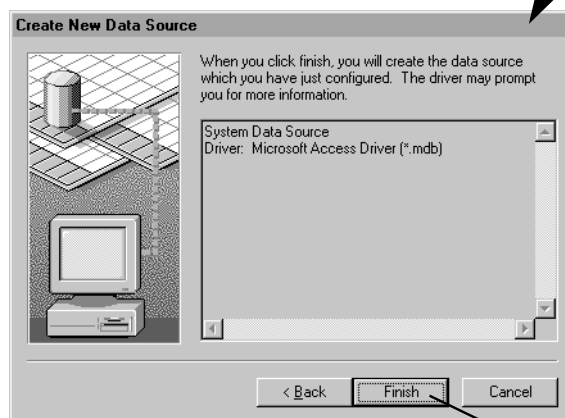


Note – Selecting the user source type generates an error window and the data source is rejected.

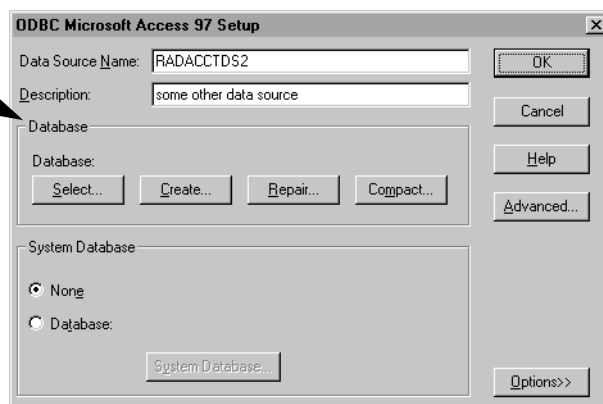
10. Click Next and follow the directions in each panel and dialog box.



12740024



12740025

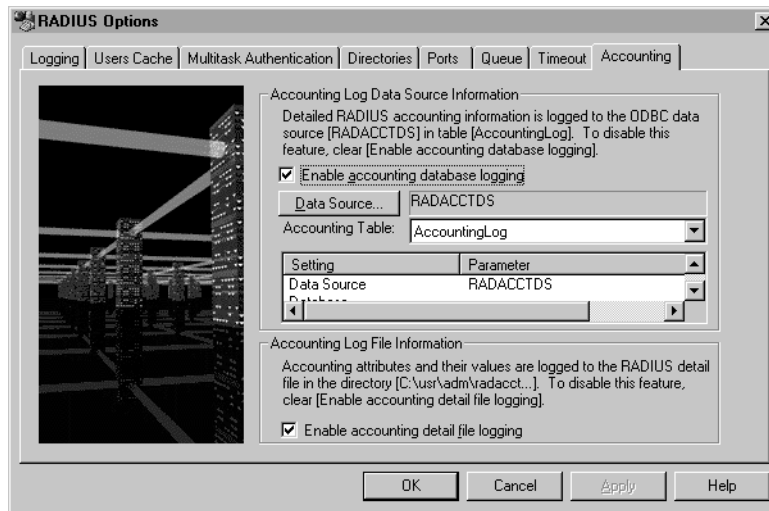


12740026

11. Configure accounting detail file logging.

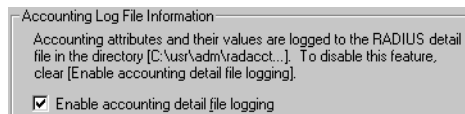
When accounting detail file logging is on, RADIUS for Windows NT logs detailed RADIUS accounting information into the flat text **detail** file in the **C:\usr\adm\radacct\portmastername** directory.

- To enable this feature, select the **Enable accounting detail file logging** option.

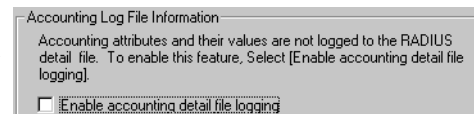


12740018

To disable this feature, clear the **Enable accounting detail file logging** option.



12740027



12740028



Note – If you have selected both options on this tab, RADIUS accounting data is saved in both the ODBC database and the flat **text** detail file.

12. Determine whether you have finished configuring the options in the RADIUS Options dialog box.

- If you have finished, click the **OK** button to apply your changes and close the RADIUS Options dialog box. Go to Chapter 3, “Adding a RADIUS Client.”
- If you have not finished, click the **Apply** button to apply your changes, and continue configuring options.

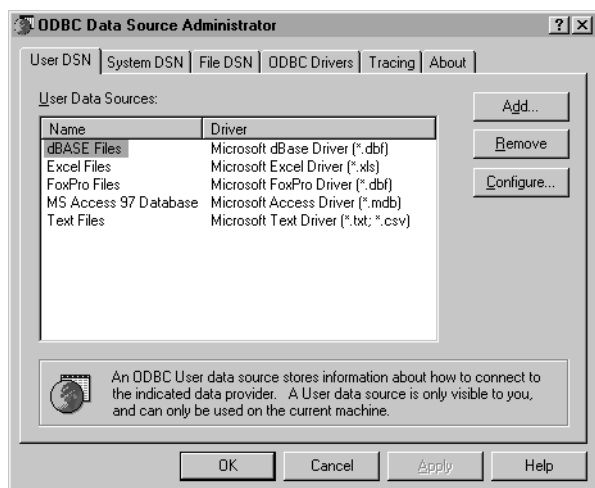
Associating Your Database with the ODBC Driver

An empty database is included with RADIUS for Windows NT. The installer loads the empty **radius.mdb** and **radacct.mdb** databases into the default directory **C:\winnt\system32\drivers\etc\raddb**. If you want to use a database to store and manage the RADIUS accounting data, you must associate the database with the Windows ODBC driver by performing the following steps:

1. In the Start menu, select Settings⇒Control Panel⇒ODBC.

This opens the ODBC Data Source Administrator dialog box.

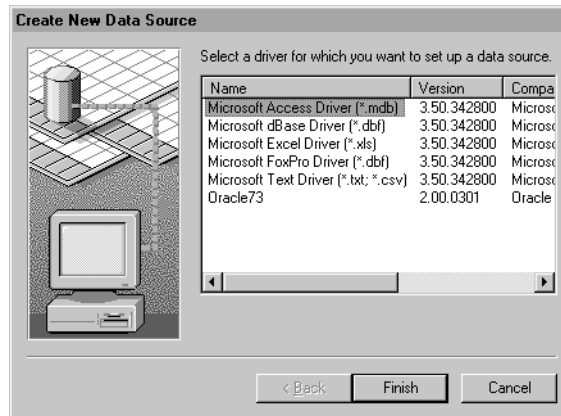
2. Select the User DSN tab.



12740038

3. Click Add.

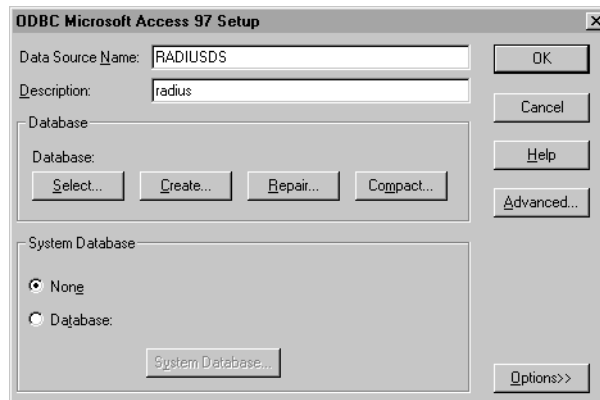
This opens the Create New Data Source panel.



12740039

4. **Verify the appropriate driver is selected—in this example, the Microsoft Access Driver (*.mdb)—and click Finish.**

The ODBC Microsoft Access 97 Setup dialog box appears. The title of the dialog box varies with the database you are using.



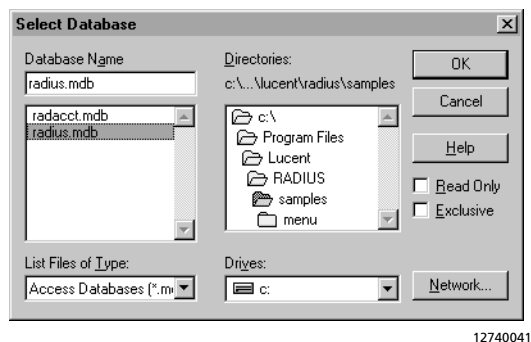
12740059

5. **Complete the Data Source Name field.**
 - Enter **RADIUSDS** if you are associating the **radius.mdb** database
 - Enter **RADACCTDS** if you are associating the **radacct.mdb** database
6. **Complete the Description field.**

- Enter **radius** if you are associating the **radius.mdb** database.
- Enter **radius accounting** if you are associating the **radacct.mdb** database.

7. Click Select in the Database box.

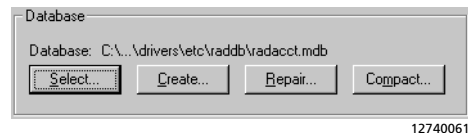
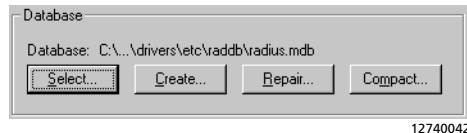
This opens the Select Database dialog box.



8. Navigate to the desired database and click OK.

- The typical path for the radius.mdb database is **C:\winnt\system32\drivers\etc\raddb\radius.mdb**.
- The typical path for the radacct.mdb database is **C:\winnt\system32\drivers\etc\raddb\radacct.mdb**.

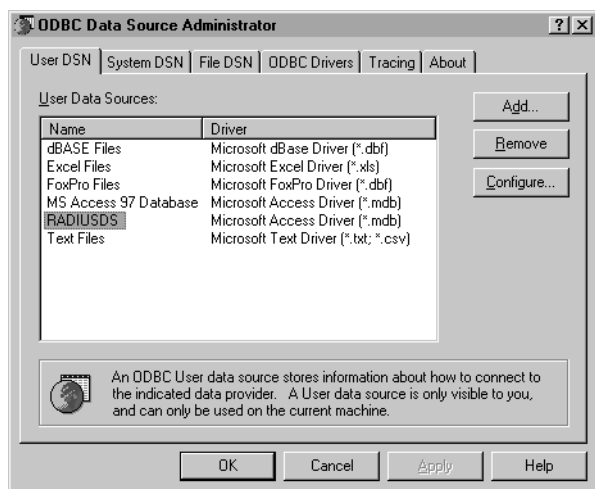
Verify the Database box displays the correct database path.



9. Click OK to close the setup dialog box.

This returns you to the User DSN tab.

10. Verify that the data source name you entered earlier—**RADIUSDS** or **RADACCTDS**—appears as the name associated with the appropriate driver on the **User DSN** tab.



12740043

11. Click **OK** to close the **ODBC Data Source Administrator** dialog box.

Server Utilities

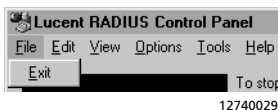
The RADIUS Control Panel provides the following utilities:

- **Authentication Test Utility**—enables you to test RADIUS authentication request packets to verify authentication is working and to troubleshoot some user problems. For instructions on using this utility, see Chapter 5, “Using RADIUS for NT Utilities.”
- **Data Source/Table Copy Utility**—enables you to copy the schema for one or more data source tables into a new table. For instructions on using this utility, see Chapter 5, “Using RADIUS for NT Utilities.”
- **User Manager Utility**—provides a convenient way to bring up the Windows NT User Manager window from within the application.
- **System Diagnostics Utility**—provides a convenient way to bring up the Windows NT Diagnostics window from within the application.

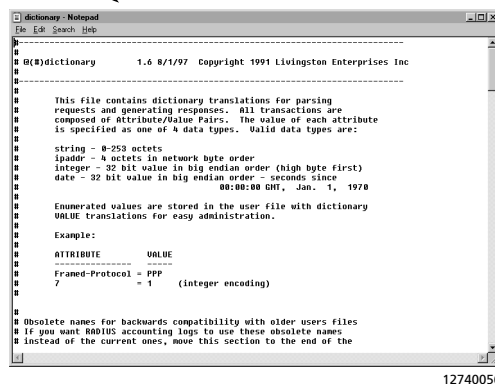
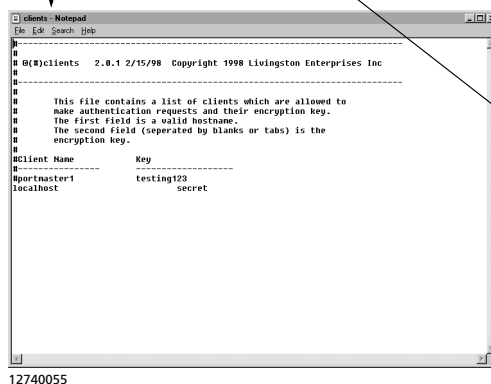
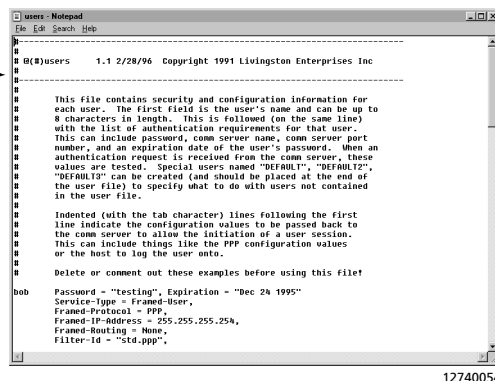
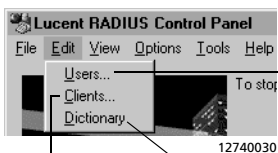
RADIUS Menu Bar

You can use the menu bar on the RADIUS Control Panel to manage the RADIUS server.

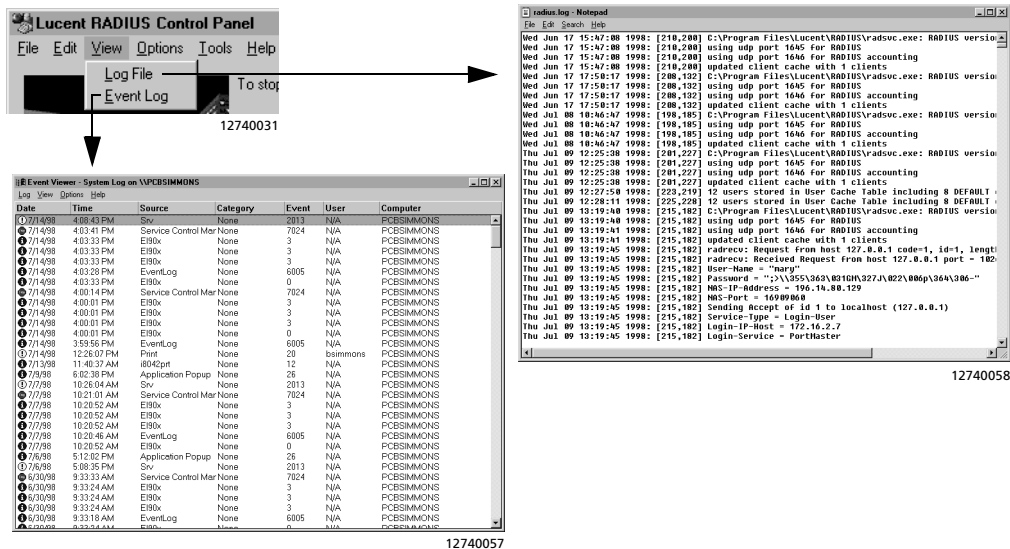
- Use the File menu to exit from RADIUS.



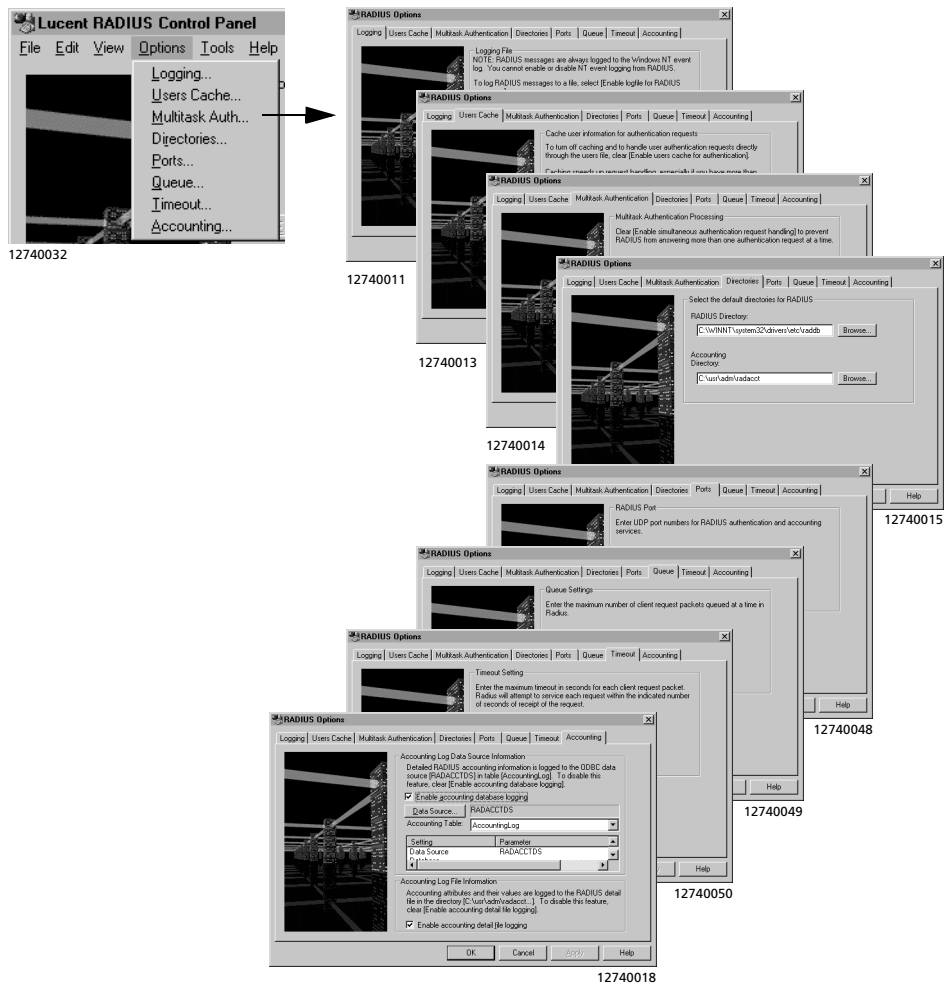
- Use the Edit menu to modify the **users**, **clients**, and **dictionary** files.



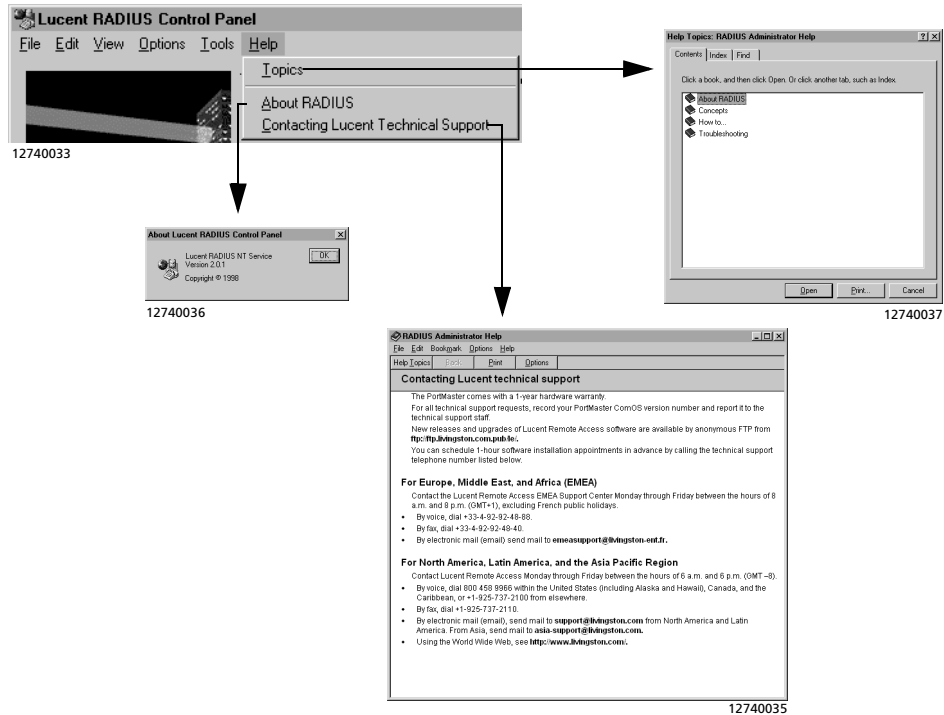
- Use the View menu to look at the log file or the event log.



- Use the Options menu to configure RADIUS options. Alternatively, you can click the **Options...** button on the RADIUS Control Panel.



- Use the Help menu to access RADIUS help or to determine the version of RADIUS you are running.



This chapter includes the following topics:

- “Accessing the Clients File” on page 3-1
- “Modifying the Clients File” on page 3-3
- “Configuring the PortMaster Using the Command Line Interface” on page 3-3
- “Configuring the PortMaster Using PMVision or PMconsole” on page 3-5

This chapter describes how to add a PortMaster as a RADIUS client. There are two steps to adding a RADIUS client:

1. **Modify the clients file to add the PortMaster and shared secret to the clients file on the RADIUS server.**
2. **Configure the following information on the PortMaster.**
 - Security enabled on all ports
 - IP addresses of the primary and optional alternate RADIUS authentication servers
 - IP addresses of the primary and optional alternate RADIUS accounting servers, if accounting is to be performed
 - RADIUS shared secret

You configure RADIUS clients using the PortMaster command line interface (see “Configuring the PortMaster Using the Command Line Interface” on page 3-3) or using a graphical user interface (GUI) (see “Configuring the PortMaster Using PMVision or PMconsole” on page 3-5).

Accessing the Clients File

The **clients** file is a flat text file installed on the RADIUS server. The **clients** file stores information about RADIUS clients, including each client’s name or IP address and its shared secret. The shared secrets must be protected from casual access. You control access to the **clients** file by granting read and write access to a group limited to those

who you want to be able to start and run RADIUS. Typically, you specify the Administrators group, but you can choose to create a unique group for restricted access. This group functions as the Windows NT equivalent of UNIX root users.

Perform the following steps to verify that only the desired group has read and write access to the **clients** file:

1. **In the Windows Explorer, click the right mouse button on the folder for the C:\winnt\system32\drivers\etc\raddb directory and select Properties.**

The **raddb** directory contains the **clients** file. You assign access rights or permissions on the directory level.

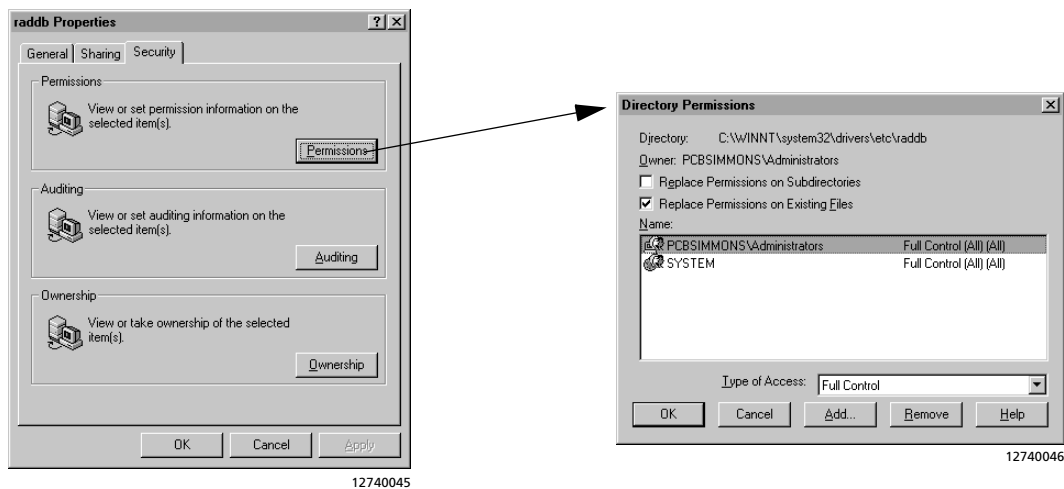
2. **In the raddb Properties dialog box that appears, select the Security tab and click Permissions.**

This displays the Directory Permissions dialog box.

3. **Look in the Name browser to verify that only members of the desired group have read and write access the directory and its contents (Figure 3-1).**

The permissions granted to this group can be either **Change (RWXD) (RWXD)** or **Full Control (All) (All)**.

Figure 3-1 Group Permissions Settings on Windows NT.



See "Preparation" on page 2-4 for more information on groups.

Modifying the Clients File

To modify the **clients** file on a Windows NT host, open the RADIUS Control Panel and choose **Clients...** from the Edit menu. The **clients** file is automatically opened in Notepad. Alternatively, you can use any text editor to edit the **clients** file.

1. **To add a client, enter the client’s IP address and the shared secret. To add a comment line, start the line with the number sign (#).**

Shared secrets must consist of 15 or fewer printable, nonspace, ASCII characters. There is no limit to the number of clients that you can add to this file.

Here are some examples of client names and shared secrets:

#Client Name	Shared Secret
#-----	-----
portmaster1	wP40cQ0
portmaster2	A3X445A
192.168.1.2	wer369st



Note – Lucent Remote Access recommends that you use IP addresses to avoid the DNS lookup time entailed by using client names.

2. **Go to one of the following sections to configure the PortMaster as a RADIUS client:**
- “Configuring the PortMaster Using the Command Line Interface” in the next section.
 - “Configuring the PortMaster Using PMVision or PMconsole” on page 3-5

Configuring the PortMaster Using the Command Line Interface

To configure the PortMaster using the command line interface, complete the following steps.

1. **Enable port security on all ports using the following command:**

```
Command> set all security on
Command> save all
```

The PortMaster tries to authenticate each user attempting to log in to a port by looking up the user in its user table. The RADIUS server authenticates users when port security is enabled **and** the user is not found in the user table. When port security is disabled and the user is not found in the Portmaster user table, RADIUS is **not** used and the login attempt fails.

2. **Enter the IP address of the primary RADIUS server using the following command:**

```
Command> set authentic Ipaddress
```

3. **You can optionally specify a secondary or alternate RADIUS server:**

```
Command> set alternate Ipaddress
```

The PortMaster consults the primary RADIUS server first. If the server does not respond, it is queried a second time; then both servers are queried up to eight additional times at 3-second intervals.

4. **To log activity using RADIUS accounting, enter the IP address of the primary accounting server:**

```
Command> set accounting Ipaddress
```

You can optionally specify an alternate accounting server:

```
Command> set accounting 2 Ipaddress
```

Lucent Remote Access recommends the use of a secondary RADIUS accounting server. The PortMaster always sends accounting packets to the primary RADIUS accounting server first, and retries it once every 45 seconds. If the primary server

does not respond within 10 minutes, or if there are more than 50 accounting packets waiting to be sent, the PortMaster sends the accounting packets to the secondary RADIUS accounting server.

5. **Enter the secret shared by the PortMaster and RADIUS server using the set secret command:**

```
Command> set secret String
```

This is the same shared secret entered in the **clients** file on the RADIUS server (see page 3-3).



Note – The shared secret is a string of up to 15 printable, nonspace, ASCII characters. If a secret longer than 15 characters is specified, an error message is displayed. Secrets in the **clients** file and configured on the PortMaster are case-sensitive and must match exactly.

6. **Save your changes using the save all command; then reset all ports:**

```
Command> save all  
Command> reset all
```



Caution – Resetting all ports disconnects any user sessions in progress. Resetting is only necessary when changes have been made to serial ports.

7. **Continue to Chapter 4, “Configuring User Information.”**

Configuring the PortMaster Using PMVision or PMconsole

You can use the PMVision™ application, a Java GUI, instead of the command line, to configure your PortMaster clients. PMVision provides all configuration options available through the older PMconsole™ interface. In addition, PMVision enables you to copy configurations within a PortMaster or to other PortMaster products and provides debugging capabilities and a window for entering ComOS commands.

Some features of PMVision include the following:

- Capability to copy configurations within a PortMaster or to other PortMaster products
- Can connect to a PortMaster using RADIUS authenticated administrative logins—if the PortMaster is appropriately configured—in addition to connecting using a **!root** login
- Debug capabilities
- Window for entering ComOS commands
- More extensive monitoring capabilities than those afforded by PMconsole, including the ability to monitor diagnostic commands
- ComOS upgrade capabilities equivalent to PMconsole
- Capability to back up and restore PortMaster configuration as ASCII text commands

When controlling a PortMaster running a ComOS release earlier than 3.8, PMVision does not provide configuration for SNMP, the host table, or static routes. If you have earlier versions of ComOS installed, you can use the PMconsole GUI to configure your PortMaster products. However, Lucent Remote Access suggests that you upgrade to a later version of ComOS.

Refer to the online help for PMVision for instructions on using it to configure a PortMaster. Refer to the *PMconsole for Windows Administrator's Guide* for instructions on using it to configure a PortMaster.

After configuring the client using the GUI, go to Chapter 4, “Configuring User Information.”



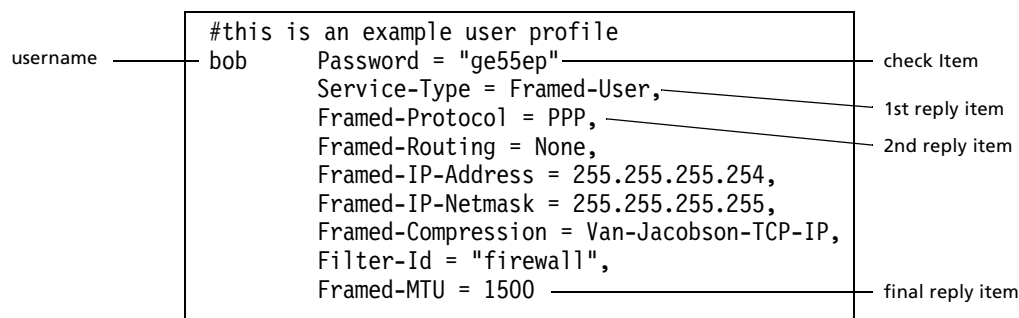
Note – Lucent Remote Access recommends that you create a single user profile and test RADIUS authentication and authorization for that user. If the test is successful, create and test profiles representative of other user types before proceeding to create all your user profiles. See Chapter 5, “Using RADIUS for NT Utilities,” for more information on testing RADIUS authentication.

This chapter includes the following topics:

- “User Profile Format” on page 4-2
- “Matching User Profiles” on page 4-4
- “Editing User Profiles” on page 4-4
- “Default User Profiles” on page 4-5
- “Check Items” on page 4-7
- “Reply Items” on page 4-16
- “Check and Reply Item Summary Table” on page 4-34
- “Using RADIUS with PAP and CHAP” on page 4-40
- “Configuring Database Caching of User Profiles” on page 4-42
- “Example PPP User Profile” on page 4-43

The RADIUS **users** file is a flat text file on the RADIUS server. The **users** file stores authentication and authorization information for all users authenticated with RADIUS. Each user must be represented by a **profile** or **entry** that consists of three parts: the username, a list of check items, and a list of reply items. Figure 4-1 displays an example.

Figure 4-1 User Profile



Note – Lucent Remote Access recommends that you create a single user profile and test RADIUS authentication and authorization for that user. If the test is successful, create and test profiles representative of other user types before proceeding to create all your user profiles.

User Profile Format

User profiles must be separated from each other by an empty line. The first line of a user profile consists of the username followed by the check items. This first line must not exceed 255 characters. All subsequent lines of the profile are individual reply items. Each reply item line, except for the final line in the profile, must end with a comma.

You can add comments to the **users** file by beginning comment lines with a number sign (#).



Caution – Do not place comments within a user profile. Comments in a user profile prevent the reply item following the comment from being processed and sent to the client. Place comments either before or after the user profile.

The contents of each user profile are case-sensitive. Definitions for all attributes and values are in the dictionary file and can be viewed with any text editor. You can also select **Edit→Dictionary...** on the RADIUS Control Panel to view the dictionary.



Caution – Modifying the contents of the dictionary file can cause RADIUS to fail to authenticate users correctly or cause other problems.

See “Default User Profiles” on page 4-5 for information on the special profile, DEFAULT. See “Example PPP User Profile” on page 4-43 for a typical user profile. All check items and reply items are summarized in “Check and Reply Item Summary Table” on page 4-34. Attributes and values used to create user profiles are defined in the dictionary.

Username. The username is the first part of each user profile and must start in the first column. Usernames consist of up to 63 printable, nonspace, ASCII characters. If SecurID or a system password file is used for authentication, the username must conform to any host username limitations.



Note – Usernames in access-requests are truncated at the first space encountered. Access-requests are rejected if the username includes a space or tab.

Check Items. Check items are listed on the first line of a user profile, following the username. The line in the user profile that contains the username and check items must not exceed 255 characters. Check items must be separated by commas. Do not place a comma after the final check item. For an access-request (see “How RADIUS Works” on page 1-2) to succeed, all check items in the user profile must be satisfied by information from the access-request or by related information from the local system, such as group membership in the access-request.

In Figure 4-1, *bob*’s password is the only check item. To successfully authenticate *bob*, the RADIUS server must receive this password in *bob*’s access-request.



Note – If no check items are included in the user profile, a user is authenticated if the username matches.

Reply Items. Reply items are placed one per line. Each line begins with a tab. Each line ends with a comma, except for the final reply item. Reply items give the PortMaster authorization information about the user’s connection—for example, whether PPP or SLIP is used or whether the user’s IP address is negotiated. In Figure 4-1, Framed-Protocol is a reply item. The value of Framed-Protocol is PPP, indicating that *bob* uses PPP for his connection.

If all check items in the user profile are satisfied by the access-request, the RADIUS server sends the reply items to the PortMaster to configure the connection.

Matching User Profiles

When a user logs in, the RADIUS server searches the **users** file for a matching profile. The following components of a profile must match the access-request for authentication to occur:

1. username
2. password
3. check items

The username matches if **any** of the following conditions are met:

- The username in the profile is identical to the login name.
- The username is identical to the login name after the prefix or suffix string specified in the profile is stripped away from the login name.
- The username in the profile is **DEFAULT** or **DEFAULT#**, where # is any integer.

The password matches if it is identical to that entered by the user. The password can be stored locally in the profile or remotely in a separate file. If you use an additional level of password security, you can specify the additional password authentication step in the profile.

All check items specified in a profile also must be present in the access-request packet for a match to occur.

Editing User Profiles

User profiles are maintained in the **users** file. On a Windows NT host, open the RADIUS Control Panel and choose **Users** from the Edit menu. The **users** file is automatically opened in Notepad.



Caution – Windows Notepad has a size limitation. For large **users** files you must use a different editor or risk losing any changes you make to the file.



Note – Windows Notepad saves files as type **.txt** by default. RADIUS NT cannot recognize or use files with the **.txt** extension. When saving the users file with Notepad, you must do a **File⇒Save As...** with no file type set.

Default User Profiles

When the RADIUS server receives a username from a PortMaster, the RADIUS server scans the users file for a matching username, starting from the top of the file. If a match is located, RADIUS attempts to authenticate the user with the information in that user profile. If a matching user profile is not found during the scan, but a DEFAULT profile is located, RADIUS attempts to use the DEFAULT profile for authentication. The DEFAULT profile is typically used when the Auth-Type is System or SecurID.



Caution – You must place DEFAULT profiles at the end of the **users** file. The RADIUS server stops scanning profiles when a matching DEFAULT profile is found and ignores any user profiles located after a DEFAULT user profile.

In the following example, user *bob*'s password is stored in a system password file. When he attempts to connect to the network, the RADIUS server scans the **users** file to determine whether it contains a matching user profile. If a matching profile is not found before the DEFAULT profile is found, the DEFAULT profile is used. Because the DEFAULT profile includes **Framed-Protocol = PPP** as a reply item, PPP is used for *bob*'s connection.

```
DEFAULT      Auth-Type = System
              Service-Type = Framed-User,
              Framed-Routing = None,
              Framed-Protocol = PPP,
              Framed-IP-Address = 255.255.255.254,
              Framed-MTU = 1500
```

RADIUS 2.0 and later permits multiple DEFAULT user profiles. In place of a username, the first line of DEFAULT profiles start as follows:

- **DEFAULT**, with all capital letters. You can use this for multiple DEFAULT profiles if the profiles include different check items.

- If there are multiple default profiles you can append a number to the end of the profile name—for example, **DEFAULT1**, **DEFAULT2**, and so on:

```
DEFAULT1    Auth-Type = System, Called-Station-ID = 9255551234
              (reply items)

DEFAULT2    Auth-Type = System, Called-Station-ID = 9255554971
              (reply items)
```

In the following example, the **Prefix** and **Suffix** check items distinguish between the DEFAULT profiles. When users add the prefix or suffix to their username, the RADIUS server matches them to the corresponding example DEFAULT profile.

```
DEFAULT     Auth-Type = System, Prefix = "P"
              Service-Type = Framed-User,
              Framed-Routing = None,
              Framed-Protocol = PPP,
              Framed-IP-Address = 255.255.255.254,
              Framed-MTU = 1500

DEFAULT     Auth-Type = System, Suffix = "%S"
              Service-Type = Framed-User,
              Framed-Routing = None,
              Framed-Protocol = SLIP,
              Framed-IP-Address = 255.255.255.254,
              Framed-Compression = None,
              Framed-MTU = 1006

DEFAULT     Auth-Type = System
              Service-Type = Login-User,
              Login-IP-Host = 172.16.1.4
              Login-Service = Telnet
```

In this example, assume that user *bob*'s password is stored in a system password file and that there is no profile with a username of **bob** in the RADIUS **users** file

Suppose *bob* logs in as **Pbob**. When the first DEFAULT profile is found by RADIUS, the server strips the initial **P** from **Pbob** and looks in the system password file for a password associated with **bob**. If the password matches the one user *bob* entered, then he is authenticated as a PPP user.

If *bob* logs in as **bob%S**, the first DEFAULT profile is not used because there is no initial **P** present in the login name. When the second DEFAULT profile is found by RADIUS, the server strips the ending **%S** from **bob%S** and looks in the system password file for a password associated with **bob**. If the password matches the one user *bob* entered, then he is authenticated as a SLIP user.

If *bob* logs in as **bob**, the first two DEFAULT profiles are not used because the Prefix and Suffix check items do not match. When the third DEFAULT profile is found by RADIUS, the server looks in the system password file for a password associated with **bob**. If the password matches the one user *bob* entered, then he is authenticated as a Telnet user.

Check Items

Check items can consist of any of the following attributes: password information—location, expiration, and encryption; client information; username prefixes and suffixes; group membership; connection rate; number called; number calling from; PPP autodetection; and type of service requested.

Connect-Rate, Called-Station-Id, and Calling-Station-Id can be used as check items only if the RADIUS client is capable of sending them in an access-request. Connect-Rate is supported only on a PortMaster 3 running ComOS 3.7 or later. Called-Station-Id and Calling-Station-Id are supported over an ISDN Primary Rate Interface (PRI) on a PortMaster 3 running ComOS 3.7 or later, and over an ISDN Basic Rate Interface (BRI) on other PortMasters running ComOS 3.7 or later.

Passwords

If you are using ComOS 3.5 or later, the user's local password can be up to 48 printable, nonspace, ASCII characters. If you are using an earlier version of ComOS, the password must not exceed 16 characters. The password check item must be contained within double quotation marks. In addition to the password itself, you can specify two different password characteristics in a user profile: the password's location and its expiration date.

Password Locations

Use the Auth-Type check item to specify the type of authentication to use for a particular user. Auth-Type can be set to one of the following: Local, System, Reject, or SecurID. If this check item is omitted from the user profile, Local is used.

- Local

To indicate that a user's password is stored in the RADIUS **users** file, use the Local Auth-Type.

To set the user's password, use the Password check item as shown in the following example line from a user profile:

```
bob    Auth-Type = Local, Password = "ge55ep"
```



Note – If no Auth-Type is specified in a profile, then the RADIUS server assumes Auth-Type = Local. Typically, you include the Password check item. If you do not include the Password item—that is, if no check items are specified in the profile—then a user is authenticated on the basis of username match alone.

- System

To indicate that a user's password is stored in a system password file or user table, use the System Auth-Type:

```
bob    Auth-Type = System
```

For example, you can use Auth-Type = System to authenticate users whose profiles are stored in the Windows NT User Manager. From the RADIUS Control Panel, you access these profiles by selecting **Tools**⇒**User Manager Utility**. Select a username, then select **User**⇒**Properties...**⇒**Profile**.

When the RADIUS server receives a username-password pair from the client and the Auth-Type = System, the server queries the operating system to determine whether there is a matching username-password pair.

- SecurID

To specify that the user's password is to be authenticated by a SecurID ACE/Server, use the SecurID Auth-Type:

```
bob    Auth-Type = SecurID
```

To use a SecurID passcode, the RADIUS server must be configured as an ACE/Client and you must have an ACE/Server configured—either on the same or a different host. See Chapter 7, “Installing and Configuring SecurID,” for instructions.

- Reject

To reject the user's authentication attempt without having to delete the user profile from the **users** file, use the Reject Auth-Type:

```
bob    Auth-Type = Reject
```

This feature enables you to disable the user account temporarily or to force authentication through DEFAULT profiles rather than through the individual user profile.

Password Expiration Date

To disable logins after a particular date, complete the following steps:

1. **Specify the date of expiration using the Expiration check item.**

The date must be specified in “*Mmm dd yyyy*” format, as in the following example:

```
bob    Password = "ge55gep", Expiration = "Dec 04 1996"
```

2. **Edit the Password-Expiration and Password-Warning values in the dictionary to meet your security needs.**

For example:

VALUE	Server-Config	Password-Expiration 30
VALUE	Server-Config	Password-Warning 5

The first parameter, Password-Expiration, turns on expiration if the value is greater than 0 (zero), but has no other effect.

Password-Warning controls when users are notified that their accounts are about to expire. In this example, users receive warning messages when they log in, starting 5 days before their password expiration date.



Note – A mechanism to permit users to change their passwords is outside the scope of RADIUS.

3. **If you modified the dictionary file, stop and restart the RADIUS NT service to activate the changes.**

Password Encryption

- Use the Crypt-Password check item if you store the user's password in encrypted format:

```
bob    Crypt-Password = "ijFYncSnctBY"
```

The PortMaster RADIUS client encrypts the password that the user enters at login and sends the encrypted password to the RADIUS server. The server compares this password with the encrypted password stored in one of the following locations:

- The user profile in **/etc/raddb/users**, if Auth-Type = Local
- A system password file, such as **/etc/passwd** or **/etc/shadow**, if Auth-Type = System

The encrypted password in this example corresponds to a password of *abcdefgh*.

If you are migrating from a UNIX platform to Windows NT, you can cut and paste the encrypted user passwords from the UNIX password file to the **users** file on the Windows NT server.



Note – Crypt-Password can be used with scripted logins or with PAP. It cannot be used with CHAP.

Username Prefixes and Suffixes

Use the **Prefix** and **Suffix** check items to allow a network user to access multiple services by adding a series of characters to the beginning or end of his username. Prefix and suffix strings must consist of 16 or fewer printable, nonspace, ASCII characters. The prefix and suffix strings must be contained within double quotation marks.

When a user logs in, the RADIUS server searches through the **users** file for a profile that matches the login. If a profile has a Prefix or Suffix check item, the server strips away the specified prefix or suffix character(s) from the login name and determines whether the result matches the username specified in the profile. If the server does not find a profile that matches the login exactly, or that matches with a prefix or suffix stripped away, RADIUS tries to match the login against a DEFAULT user profile.

Consider the following example **users** file:

```

bob      Auth-Type = System, Prefix = "P"
         Framed-Protocol = PPP,
         Service-Type = Framed-User,
         Framed-Routing = None,
         Framed-IP-Address = 255.255.255.254,
         Filter-Id = "firewall",
         Framed-MTU = 1500

DEFAULT  Auth-Type = System, Suffix = "%slip"
         Framed-Protocol = SLIP,
         Service-Type = Framed-User,
         Framed-Routing = None,
         Framed-IP-Address = 255.255.255.254,
         Filter-Id = "firewall",
         Framed-MTU = 1500

```

In this example, *bob*'s username and password are stored in a system password file. If *bob* specifies a username of **Pbob** when attempting to connect to the PortMaster, the RADIUS server looks up the username. When the profile for **bob** is found, the Prefix check item matches because the login name begins with a **P**. This cues the server to strip away the specified prefix character to see if there is a match. The username in the profile—*bob*—matches the stripped login name, so the server checks the system password file for *bob*'s password. If a password match is found, *bob* is connected as a PPP user.

If *bob* specifies a username of **bob%slip** when he logs in, the RADIUS server finds no match until it gets to the DEFAULT entry. The Suffix check item matches because the login name ends with **%slip**. This cues the server to strip away the specified suffix characters to see if there is a match. The **DEFAULT** username in the profile matches all login names, so the server next checks the system password file for *bob*'s password. The server next checks the system password for *bob*. If a password match is found, *bob* is connected as a SLIP user.

The following example **users** file has no provision for username prefixes:

bob	Auth-Type = System Framed-Protocol = PPP, Service-Type = Framed-User, Framed-Routing = None, Framed-IP-Address = 255.255.255.254, Filter-Id = "firewall", Framed-MTU = 1500
DEFAULT	Auth-Type = System, Suffix = "%slip" Framed-Protocol = SLIP, Service-Type = Framed-User, Framed-Routing = None, Framed-IP-Address = 255.255.255.254, Filter-Id = "firewall", Framed-MTU = 1500

Again, *bob*'s username and password are stored in a system password file. Suppose *bob* logs in as **Pbob**. There are no profiles with a username of **Pbob** or a Prefix check item specifying **P**. The RADIUS server cannot find a matching user profile and rejects the connection attempt.

Prefixes and suffixes are most useful when defined in a DEFAULT user profile. See “Default User Profiles” on page 4-5 for information on using prefixes and suffixes in a DEFAULT profile.

Called-Station-Id

You can use the number that the user is **calling** as a check item. Suppose user *mario* calls in using your toll-free access number, 1-800-555-4973. With the user profile shown in the following example, *mario* fails authentication. He can only be authenticated if he calls in to 510-555-1234.

```
mario Password = "ge55gep", Called-Station-ID = 5105551234
Service-Type = Framed-User,
Framed-Routing = None,
Framed-Protocol = PPP
```



Note – Use of the Called-Station-ID check item requires that the Called-Station-ID attribute be included in the access-request. The PortMaster 3 running ComOS 3.7 or later sends this attribute as part of the access-request over the PRI, if available. Other PortMaster products running ComOS 3.7 or later send this information as part of the access-request over ISDN Basic Rate Interfaces (BRIs). If the Called-Station-ID attribute is not sent, the Called-Station-ID check item is ignored.

Calling-Station-Id

You can use the number that the user is **calling from** as a check item. In the following example, *cissy* is authenticated if she calls from 209-555-5678. If she calls from any other number, she fails authentication.

```
cissy Password = "ge55gep", Calling-Station-ID = 2095555678
Service-Type = Framed-User,
Framed-Routing = None,
Framed-Protocol = PPP
```



Note – Use of the Calling-Station-ID check item requires that the Calling-Station-ID attribute be included in the access-request. The PortMaster 3 running ComOS 3.7 or later sends this attribute as part of the access-request over the PRI, if available. Other

PortMaster products running ComOS 3.7 or later send this information as part of the access-request over ISDN BRIs. If the Calling-Station-ID attribute is not sent, the Calling-Station-ID check item is ignored.

Client Information

Use the NAS-IP-Address check item to specify the IP address of a particular PortMaster. When this setting is used as a check item in a user profile, the user must attempt to start a connection on the specified PortMaster for the connection to succeed.

Use the NAS-Port check item to specify a particular PortMaster port. To be successfully authenticated, the user must attempt to log in to this port:

```
bob Password = "ge55gep", NAS-Port = 23
```

Use the NAS-Port-Type check item to specify the type of port. Options for the NAS-Port-Type are as follows: **Analog**, **Async**, **Sync**, **ISDN**, **ISDN-V120**, or **ISDN-V110**. The PortMaster must run ComOS release 3.3.1 or later to support NAS-Port-Type.

The following example displays a user profile containing the NAS-IP-Address and NAS-Port-Type settings:

```
bob Password = "ge55gep", NAS-IP-Address = 192.168.1.54, NAS-Port-Type = ISDN
Service-Type = Framed-User,
Framed-Routing = None,
Framed-Protocol = PPP
```

Connect-Rate

The Connect-Rate check item can be used with PortMaster 3 clients. Use this to specify the maximum connection rate permitted for a user.

In the following example, with a connection rate of 28800bps, *bob* fails authentication if he attempts to connect to the PortMaster 3 at a higher rate—for example, 33600bps or 56000bps:

```
bob  Auth-Type = System, Connect-Rate = 28800
     Service-Type = Framed-User,
     Framed-Routing = None,
     Framed-Protocol = PPP
```



Note – Use of the Connect-Rate check item requires that the Connect-Info attribute be included in the access-request. The PortMaster 3 running ComOS 3.7 or later sends the Connect-Info attribute as part of the access-request. If Connect-Info is not sent, the Connect-Rate check item is ignored.

Framed-Protocol

Framed-Protocol is primarily used as a reply item, but you can also use the Framed-Protocol check item in the user profile for PPP autodetection by the PortMaster:

```
bob  Auth-Type = System, Framed-Protocol = PPP
```

See “Framed-Protocol” on page 4-24 for more information.

Group

You can define a **group** of users to restrict authentication when specifying Auth-Type = System. If a user profile contains the Group check item, only users that are defined as members of the specified group are authenticated.

The Group string consists of up to 63 printable, nonspace, ASCII characters. The group must be contained within double quotation marks.

If you specify multiple groups in a user profile, the user must be a member of each group to be authenticated. In the following example, user *bob* is authenticated only if *bob* is a member of both the Engineering group and the Hardware group:

```
bob  Auth-Type = System, Group = "engineering", Group = "hardware"
```

On Windows NT hosts, groups are defined with the User Manager in the Administration Tools (Common) menu. You can define only local groups on hosts running the Windows NT Workstation software. However, you can define either local or global groups on hosts running the Windows NT Server software. Refer to your system documentation for instructions on creating groups and adding members to groups.

Service-Type

Service-Type is generally used as a reply item, but it can be used with either of the following values as a check item. See “Service-Type” on page 4-16 for more information on the Service-Type reply item.

Framed-User

You can use the Service-Type = Framed-User check item to authenticate users who make their connections via PPP or SLIP.

Outbound-User

Use the Service-Type = Outbound-User check item to restrict a user to outbound accesses to network device ports. You must use the same attribute and value—Service-Type = Outbound-User—as a reply item in the user profile. See “Outbound-User” on page 4-21 for more information.

Reply Items

Reply items can authorize or apply any of the following: type of service provided, callback information, routing information, connection protocol, timeouts, port limits, menus, maximum MTU, filters, remote login information, and termination menus.

Service-Type

You must specify the type of service authorized to the user, by specifying the Service-Type attribute in each user profile. Service-Type must be set to one of the values shown in Table 4-1.

Table 4-1 Service-Type

Service-Type	Explanation
Administrative-User	<p>The PortMaster grants the user a full administrative login—as if the user had logged in using !root. The user has full configuration ability and access to all PortMaster commands.</p> <p>This Service-Type is available only with ComOS 3.5 or later versions.</p>
Callback-Framed-User	<p>The PortMaster verifies the user’s identity by disconnecting the port and dialing the user back using a specified location table entry. When the user’s identity is verified, PPP or SLIP is used for the connection.</p> <p>To specify the callback location, see “Callback-Framed-User” on page 4-19.</p>
Callback-Login-User	<p>The PortMaster verifies the user’s identity by disconnecting the port and dialing the user back at a specified number. The user’s identity must be verified before the connection is permitted.</p> <p>To specify the callback location, see “Callback-Login-User” on page 4-19.</p>
Framed-User	<p>The user makes a connection via PPP or SLIP.</p>
Login-User	<p>The user connects via the Telnet, rlogin, or PortMaster service (in.pmd), or via TCP-Clear (netdata).</p>

Table 4-1 Service-Type (Continued)

Service-Type	Explanation
NAS-Prompt-User	<p>The PortMaster grants the user a limited administrative login. The user can use the following commands: ifconfig, ping, ptrace, reboot, reset, set console, set debug, show, traceroute, and any nonconfiguration commands.</p> <p>The following commands are not permitted: add, delete, erase, save, tftp, and any set commands other than set console or set debug.</p> <p>This Service-Type is available only with ComOS 3.5 or later versions.</p>
Outbound-User	The user uses Telnet for outbound connections.



Note – If the RADIUS server is used with non-Lucent products, the Administrative-User and NAS-Prompt-User Service-Types must not be used unless the other vendor's implementation of these types is compatible with Lucent's implementation.

Administrative-User

You can grant a user full PortMaster administrative ability by using the Service-Type = Administrative-User reply item. The user can configure the PortMaster client and can use **all** PortMaster commands. For example:

```
bob Password = "ge55gep"  
Service-Type = Administrative-User
```

This Service-Type requires ComOS 3.5 or later. Compare it with the NAS-Prompt-User Service-Type on page 4-21.

Callback-Framed-User

You can use the Service Type = Callback-Framed-User reply item to connect to a user by callback. When a user's service type is Callback-Framed-User, you must specify a location using the Callback-Id reply item. The location must be contained within double quotation marks. For example:

```
bob Password = "ge55gep"  
Service-Type = Callback-Framed-User,  
Callback-Id = "bobhome"
```

After the RADIUS server verifies the password for user *bob*, it includes the Callback-Id in the access-accept message it sends to the PortMaster. The PortMaster checks its local location table; if there is a matching location name, it makes the connection using that location's settings.



Note – To create location table entries, see the information on configuring dial-out locations in the *Configuration Guide for PortMaster Products*.

Callback-Login-User

You can use the Service Type = Callback-Login-User reply item to authenticate a user by callback. When a user's Service-Type is Callback-Login-User, specify a telephone number using the Callback-Number reply item. The number must be contained within double quotation marks. For example:

```
bob Password = "ge55gep"  
Service-Type = Callback-Login-User,  
Callback-Number = "9,1-800-555-1234"
```

After the RADIUS server verifies the password for user *bob*, it includes the Callback-Number in the access-accept message it sends to the PortMaster. The PortMaster calls the user back at the specified number; if the user is reached successfully, the PortMaster prompts the user to reenter his password and then sets up the connection.

When a user's Service-Type is Callback-Login-User, you can supply additional information: the service used to connect to the host, the name or IP address of the remote host, and a TCP port number.

- To specify the login service, use the Login-Service reply item; see "Login-Service" on page 4-30.
- To specify the remote host, use the reply item; see "Login-IP-Host" on page 4-31.
- To specify the TCP port number, use the Login-TCP-Port reply item; see "Login-TCP-Port" on page 4-32.

Framed-User

In the following example, user *bob*'s Service-Type is Framed-User, indicating that the user is making the connection via PPP or SLIP:

```
bob  Auth-Type = System
      Service-Type = Framed-User,
      Framed-Routing = None,
      Framed-Protocol = SLIP
```

When the Service-Type is Framed-User, you must include the Framed-Protocol reply item in the user profile to indicate whether PPP or SLIP is used.

Login-User

In the following example, user *bob*'s Service-Type is Login-User.

```
bob  Auth-Type = System
      Service-Type = Login-User
```

When a user's Service-Type is Login-User, you can supply additional information: the service used to connect to the host, the name or IP address of the remote host, and a TCP port number.

- To specify the login service, use the Login-Service reply item; see "Login-Service" on page 4-30.

- To specify the remote host, use the reply item; see “Login-IP-Host” on page 4-31.
- To specify the TCP port number, use the Login-TCP-Port reply item; see “Login-TCP-Port” on page 4-32.

NAS-Prompt-User

You can grant a user limited PortMaster administrative ability by using the Service-Type = NAS-Prompt-User reply item. The user can use the following commands: **ifconfig**, **ping**, **ptrace**, **reboot**, **reset**, **set console**, **set debug**, **show**, and **traceroute**. For example:

```
bob Password = "ge55gep"
    Service-Type = NAS-Prompt-User
```

The user cannot configure the PortMaster client and cannot use these commands: **add**, **delete**, **erase**, **save**, **tftp**, and any **set** commands other than **set console** or **set debug**.

This Service-Type requires ComOS 3.5 or later. Compare it with the Administrative-User Service-Type on page 4-18.



Note – If you use PMVision to control your PortMaster client, note that PMVision does not treat the RADIUS NAS-Prompt-User administrative user any differently from the RADIUS Administrative-User until the ComOS denies access to a function. For example, a NAS-Prompt-User level administrative user can use PMVision to create a user or location record, but creation of that record is denied when the command is sent to the PortMaster.

Outbound-User

Setting the Service-Type reply item to Outbound-User allows a user to gain outbound access to network device ports using Telnet. This feature is supported in ComOS version 3.3.2 or later and RADIUS 2.0 or later. To use this feature, you must set the relevant asynchronous ports on your PortMaster as either host-controlled devices, using the command **set S0 device Device network Mode**, or as devices capable of two-way operation, using the command **set S0 twoway Device network Mode**. See the *Command Line Administrator's Guide* for more information on setting the PortMaster port type.

To restrict users to outbound access, the user profile must include this same attribute and value—Service-Type = Outbound-User—as a check item. The Login-TCP-Port setting can be used to specify the TCP port for the connection; the port number must not be less than 10000 nor greater than 10100. For example:

```
bob    Password = "ge55gep", Service-Type = Outbound-User
       Service-Type = Outbound-User,
       Login-Service = Telnet,
       Login-TCP-Port = 10000
```

In this example, when user *bob* is attempting an outbound connection, the PortMaster client checks its local user table for an entry for *bob*. If *bob* is not found in the table, the PortMaster sends an access-request to the RADIUS server indicating that *bob* is an Outbound-User.

The RADIUS server examines *bob*'s profile in the **users** file. If Outbound-User is included as a reply item, the server notifies the PortMaster to permit the connection.

Configure the PortMaster as shown in the following example. The example configures port **s1**; however, you can configure multiple ports to listen at different TCP port numbers or at the same TCP port number to create a pool of devices:

```
Command> set s1 device /dev/network
Command> set s1 service_device telnet 10000
Command> set s1 modem off
```

Callback-Id

You must use the Callback-Id reply item to specify a location at which to call a user back when the user's Service-Type is specified as Callback-Framed-User. See "Callback-Login-User" on page 4-19.

Callback-Number

You must use the Callback-Number reply item to specify a telephone number at which to call a user back when the user's Service-Type is specified as Callback-Login-User. See "Callback-Framed-User" on page 4-19.

Compression

Van Jacobson TCP/IP header compression is enabled by default. To disable compression, set the Framed-Compression reply item value to **None**:

```
Framed-Compression = None
```

To enable compression, set the Framed-Compression reply item value to **Van-Jacobson-TCP-IP**:

```
Framed-Compression = Van-Jacobson-TCP-IP
```

Framed-IP-Address

Use the Framed-IP-Address reply item to specify the user's IP address, as shown in the following example:

```
bob  Auth-Type = System
      Service-Type = Framed-User,
      Framed-Routing = None,
      Framed-Protocol = PPP,
      Framed-IP-Address = 172.28.1.1
```

When Framed-IP-Address is set to 255.255.255.255, the PortMaster **negotiates** the address with the end-node (dial-in user). When it is set to 255.255.255.254 (or omitted), the PortMaster **assigns** an IP address to the dial-in user from the assigned address pool. All other IP address specifications are used each time the user logs in and constitute the user's **static** address.



Note – To create an assigned address pool for the PortMaster, use the **set assigned_address** *Ipaddress* command on the PortMaster, where *Ipaddress* is the first or base IP address in the address pool. See the *Configuration Guide for PortMaster Products* for more information on assigned address pools.

Framed-IP-Netmask

Use the Framed-IP-Netmask reply item to specify a variable-length subnet mask (VLSM). The VLSM is applied to the address specified for the user with the Framed-IP-Address reply item. The PortMaster uses the specified value to update its routing table when the user logs in:

```
bob  Auth-Type = System
      Service-Type = Framed-User,
      Framed-Routing = None,
      Framed-Protocol = PPP,
      Framed-IP-Address = 192.168.10.232,
      Framed-IP-Netmask = 255.255.255.192
```

In this example, a netmask of 255.255.255.192 is used. The user can be routed to a 62-host subnet. The user can access hosts with addresses from 192.168.10.193 through 192.168.10.255.

If this reply item is omitted or if you are using a version of ComOS earlier than 3.5, the default subnet mask is 255.255.255.255. Use the Framed-IP-Netmask reply item with caution because it affects both routing and proxy Address Resolution Protocol (ARP) on the PortMaster.



Note – This reply item requires ComOS 3.5 or later. You must use the **set user-netmask on** command to enable the PortMaster to use the netmask value. Before using this reply item, read about the **set user-netmask** command in the *Configuration Guide for PortMaster Products* or the *Command Line Administrator's Guide*.

Framed-Protocol

When the Service-Type is Framed-User, you must include the Framed-Protocol reply item in the user profile to indicate whether PPP or SLIP is used. For example, user *bob* is a PPP user. His user profile includes the following lines:

```
bob  Auth-Type = System
      Service-Type = Framed-User,
      Framed-Routing = None,
      Framed-Protocol = PPP
```


Framed-Protocol can also be used as a check item for PPP autodetection by the PortMaster. See “Framed-Protocol” on page 4-15 for more information on the Framed-Protocol check item.

Framed-Route

Use the Framed-Route reply item to add a route to the PortMaster routing table when service to the user begins. Three pieces of information are required: the destination IP address, gateway IP address, and metric. For example:

```
bob  Auth-Type = System
      Service-Type = Framed-User,
      Framed-Routing = None,
      Framed-Protocol = PPP,
      Framed-IP-Address = 172.28.1.1,
      Framed-Route = "172.28.1.0 172.28.1.1 1"
```

In this example, 172.28.1.0 is the IP address of a destination network. 172.28.1.1 is the IP address of the gateway for this network, and 1 is the metric (hop count).

If 0.0.0.0 is specified as the gateway IP address, the user’s IP address is substituted for the gateway.

In ComOS 3.5 or later, you can use the variable-length subnet mask (VLSM) format for the Framed-Route, which identifies the number of high-order bits in the destination IP address, as follows:

```
bob  Auth-Type = System
      Service-Type = Framed-User,
      Framed-Routing = None,
      Framed-Protocol = PPP,
      Framed-IP-Address = 172.28.1.1,
      Framed-Route = "172.28.1.0/28 172.28.1.1 1"
```

See the *Routing Guide for PortMaster Products* for more information on VLSM.

Framed-Routing

Use the Framed-Routing reply item to control how RIP is used on the user's interface. RIP options are explained in Table 4-2.

Table 4-2 Framed-Routing Options

Option	Explanation
None	Disables RIP on the interface.
Broadcast	The interface sends RIP updates.
Listen	The interface listens for RIP updates.
Broadcast-Listen	The interface sends and listens for RIP updates.

The following example displays user *bob*'s user profile. Framed-Routing is set to **None**; *bob*'s interface neither sends nor listens for RIP updates.

```
bob Password = "ge55gep"  
    Service-Type = Framed-User,  
    Framed-Routing = None,  
    Framed-Protocol = PPP
```

Typically, Framed-Routing is set to **Broadcast-Listen** for connections to other routers, and set to **None** for user connections. See the *Routing Guide for PortMaster Products* and the *Command Line Administrator's Guide* for more information.

Filter-Id

You can use the Filter-Id reply item with packet filters or access filters. For the Filter-Id attribute to initiate filtering, the filter must be previously defined and be specified in at least one rule in the filter. If you specify a Filter-Id in the user profile, but do not define the filter, then no filtering is performed. If you define the filter, but do not define any rules in the filter, then no filtering is performed.



Note – To configure filters on a PortMaster, see the information on configuring filters in the *Configuration Guide for PortMaster Products*. Filters specified in RADIUS can also be dynamically loaded using ChoiceNet. For more information see the *ChoiceNet Administrator's Guide*.

Packet Filters

Use the Filter-Id reply item to associate packet filters with each PPP or SLIP user authenticated with RADIUS. In the following example, the **firewall** filter is used during *bob's* connection:

```
bob Password = "ge55gep"  
Service-Type = Framed-User,  
Framed-Routing = None,  
Framed-Protocol = PPP,  
Filter-Id = "firewall"
```

You must define filters on each PortMaster that the user accesses, unless you are using ChoiceNet. See the *ChoiceNet Administrator's Guide* for information on ChoiceNet and how it provides storage for filters in a central site.

To control whether the filter restricts incoming or outgoing traffic, the filter defined on the PortMaster must have an **.in** or **.out** suffix attached to its name. In the previous example, the filter **firewall.in** is used as a filter for packets entering the PortMaster via the interface, and **firewall.out** is used as an output filter for packets leaving the PortMaster via the interface.

Do not specify the **.in** and **.out** suffixes in the user profile. When a user dials in to the PortMaster, the **.in** or **.out** suffix is automatically appended to the filter name provided by RADIUS.

Access Filters

An access filter is a filter associated with a login user. Use the Filter-Id reply item to associate an access filter with a host prompt login user authenticated with RADIUS. In the following example, the **engineering** filter is used to restrict the hosts that *bob* can access during a connection:

```
bob Password = "ge55gep"
    Service-Type = Login-User,
    Login-IP-Host = 255.255.255.255,
    Login-Service = Telnet,
    Login-TCP-Port = 23,
    Filter-Id = "engineering"
```

You must define access filters on each PortMaster the user accesses, using the same name as the Filter-Id. The access filter name defined in the user record must be exactly the same as the filter name defined on the PortMaster. The PortMaster does not append anything to the name of an access filter, unlike packet filters.



Note – ChoiceNet can be used with access filters only with PortMasters running ComOS 3.7.1 or higher.

Idle-Timeout

Use Idle-Timeout, as shown in the following example, to specify the number of seconds a session can be idle before it is disconnected. Idle-Timeout can range from 2 seconds to 14400 seconds (4 hours) and is rounded down to a multiple of 60 if greater than 240.

```
bob Password = "ge55gep"
    Service-Type = Framed-User,
    Framed-Routing = None,
    Framed-Protocol = PPP,
    Idle-Timeout = 600
```

In this example, if the session is inactive longer than 600 seconds (10 minutes), user *bob* is disconnected.



Note – Idle-Timeout and Session-Timeout values are specified in **seconds** in the RADIUS **users** file. If you set these timeout values using the PortMaster command line interface, PMVision, or PMconsole, you specify them in **minutes** by default.

IPX Network

When an IPX network is used for a particular user's connection, you must include the Framed-PX-Network reply item in the user profile. The PortMaster supports IPX over PPP.

Specify Framed-IPX-Network in dotted decimal notation (*xx.xx.xx.xx*). For example, the hexadecimal network number 123456 must be expressed as 0.18.52.86.

```
bob Password = "testing"
    Service-Type = Framed-User,
    Framed-Routing = None,
    Framed-Protocol = PPP,
    Framed-IPX-Network = 0.18.52.86
```



Note – If you set **Framed-IPX-Network = 255.255.255.254**, a dynamic IP address is used and converted to hexadecimal for the IPX network number.

On a Windows NT system, you can use the built-in calculator accessory in scientific mode to convert numbers between hexadecimal and decimal.

The following Perl script converts an IPX hexadecimal network number to dotted decimal notation:

```
#!/usr/local/bin/perl
# hex - convert ip addresses to hexadecimal and vice versa
for (@ARGV) {
    if (/\.\/) {                # convert . to hex
        @octets = split(/\.\/,$_);
        for $octet (@octets) {
            printf "%02X",$octet;
        }
        print "\n";
    } else {                    # convert hex to .
        $buf = '';
        while (s/\w\\w//) {
            $buf .= hex($&).'.';
        }
        $buf =~ s/\.$/\n/;
        print $buf;
    }
}
```

Login-Service

When a user's Service-Type is Login-User or Callback-Login-User, you can use the Login-Service reply item to specify the service used to connect to the host.

If you do not use this reply item, the PortMaster login service is used by default.

All Login-Service values are described in Table 4-2.

Table 4-3 Login-Service

Login-Service	Description
Telnet	Establishes a Telnet connection to the remote host. Port 23 is the default.
Rlogin	Establishes an rlogin connection to the remote host.

Table 4-3 Login-Service (Continued)

Login-Service	Description
TCP-Clear	Establishes a TCP clear connection to the remote host. 8-bit data is passed through this connection without interpretation. This option is the equivalent of the netdata login service on the PortMaster. Port 6000 is the default.
PortMaster	Establishes a connection to the remote host using the PortMaster login service. To use this setting with UNIX versions of RADIUS, you must install the in.pmd daemon on the remote host.

Login-IP-Host

When a user's Service-Type is Login-User or Callback-Login-User, you can use the Login-IP-Host reply item to specify the name or IP address of the remote host.

If you do not use this reply item to specify a remote host, the default host for the port is used. See the *Command Line Administrator's Guide* for information on setting the default host.

Consider the following example. In this profile, user *bob* is authenticated and then called back at the number specified by Callback-Number. If *bob* is successfully authenticated, a Telnet connection to host 192.168.1.76 is established.

```
bob Password = "ge55gep"
    Service-Type = Callback-Login-User,
    Login-IP-Host = 192.168.1.76,
    Login-Service = Telnet,
    Callback-Number = "9,1-800-555-1234"
```

If Login-IP-Host is set to 0.0.0.0 or omitted, the host defined for the port in the PortMaster is used. If Login-IP-Host is set to 255.255.255.255, the user is presented with a **host:** prompt where he enters the hostname or the host's IP address.

If the user is to log in to a particular TCP port on the remote host, specify the port number with the Login-TCP-Port reply item; see "Login-TCP-Port" on page 4-32.

Login-TCP-Port

When a user's Service-Type is Login-User or Callback-Login-User, you can use the Login-TCP-Port reply item to specify the port number if the user is to log in to a particular TCP port on the remote host. This reply item is often used with the Outbound-User reply item (see "Outbound-User" on page 4-21) and the Login-IP-Host reply item (see "Login-IP-Host" on page 4-31).

Consider the following example. In this profile, user *bob* is authenticated, then called back at the Callback-Number. If successfully authenticated, a Telnet connection to port 23 on host 192.168.1.76 is established.

```
bob    Password = "ge55gep"
       Service-Type = Callback-Login-User,
       Login-IP-Host = 192.168.1.76,
       Login-Service = Telnet,
       Login-TCP-Port = 23,
       Callback-Number = "9,1-800-555-1234"
```

If Login-TCP-Port is omitted, the port defined for Telnet service on the PortMaster is used.

Menu

Use the Menu reply item to call a menu by reference. The menu must be contained within double quotation marks. The Menu reply item is the only reply item in the user profile when a menu is referenced:

```
DEFAULT    Auth-Type = System
           Menu = "menu1"
```

In this example, after user *bob* is authenticated, the **menu1** menu is displayed and he is prompted to make a selection. When *bob* selects a menu option, the corresponding service is provided. See Chapter 6, "Configuring RADIUS Menus," for more information on menus.

MTU

Use the Framed-MTU reply item to configure the number of bytes in the maximum transmission unit (MTU) for a user's connection:

```
Framed-MTU = 1500
```

Framed-MTU is used only for PPP and SLIP connections. For PPP connections, Framed-MTU can be between 100 and 1520 bytes. SLIP connections can have an MTU between 100 and 1006 bytes. On IPX networks, set Framed-MTU to at least 600 bytes.



Note – If PPP negotiates an MTU for the connection, the Framed-MTU setting is ignored.

Port-Limit

Use the Port-Limit reply item to control the maximum number of ports available for a Multilink PPP or Multilink V.120 connection. Port-Limit applies only to ISDN connections; other connection types are not affected.

The Port-Limit value can be as high as the maximum number of B channels available for the ISDN ports. For example, if a PortMaster has 15 ISDN BRI ports, the Port-Limit value can be as high as 30.

In the following example, user *bob*'s connection can use only one B channel:

```
bob Password = "ge55gep", NAS-Port-Type = ISDN
    Service-Type = Framed-User,
    Framed-Routing = None,
    Framed-Protocol = PPP,
    Port-Limit = 1
```

Session-Timeout

Use Session-Timeout to specify the time limit for a session. If this reply item appears in a user profile, the user is disconnected when the time limit is reached.

Session-Timeout is specified as a particular number of seconds, up to a maximum of 31536000 (1 year).

In the following example, user *bob* is automatically disconnected after 7200 seconds (2 hours).:

```
bob Password = "ge55gep"
    Service-Type = Framed-User,
    Framed-Routing = None,
    Framed-Protocol = PPP,
    Session-Timeout = 7200
```

Termination-Menu

Use Termination-Menu to present a menu to the user when the service ends. If a Termination-Menu is not included in the reply items, the user is disconnected immediately after a SLIP, PPP, or login session.



If you want to disconnect the line when the service ends, do not use Termination-Menu.

See "Termination Menus" on page 6-4 for more information about termination menus.

Check and Reply Item Summary Table

Table 4-4 summarizes all user profile check and reply items.



Note – Although it is not considered a check item, be sure that the username appears as the first item on the first, or check item, line of the user profile.

Table 4-4 User Profile Check and Reply Items

Item	Options	Explanation	Used as Check Item?	Used as Reply Item?
Auth-Type	Local	User's password is stored in the RADIUS users file. Default.	Yes	No
	System	User's password is stored in a system password file.	Yes	No
	SecurID	User is authenticated via ACE/Server software.	Yes	No
	Reject	User always fails authentication.	Yes	No
Callback-Id	Location name in double quotation marks (" ")	Specify only for Service-Type = Callback-Framed-User . Location must be in PortMaster location table.	No	Yes
Callback-Number	Phone number in double quotation marks (" ")	Specify only for Service-Type = Callback-Login-User .	No	Yes
Called-Station-Id	String of numerals	Telephone number called by user. Available in ComOS 3.7 for ISDN BRI and PortMaster 3 ISDN PRI.	Yes	No
Calling-Station-Id	String of numerals	Telephone number user is calling from. Available in ComOS 3.7 for ISDN BRI and PortMaster 3 ISDN PRI.	Yes	No

Table 4-4 User Profile Check and Reply Items (Continued)

Item	Options	Explanation	Used as Check Item?	Used as Reply Item?
Connect-Rate	String of numerals	Maximum connection rate permitted, in bps. Available only for PortMaster 3 products running ComOS 3.7 or later.	Yes	No
Crypt-Password	User's password	User's password is stored in UNIX crypt format. CHAP authentication attempts fail if Crypt-Password is used, even if the password is correct.	Yes	No
Expiration	Must be specified in "Mmm dd yyyy" format	Date that user's password expires.	Yes	No
Filter-Id	Filter name	Filter name to be used for packet or access filtering on the interface.	No	Yes
Framed-Compression	None	If this reply item is omitted, Van Jacobson TCP/IP header compression is used.	No	Yes
	Van-Jacobson-TCP-IP	Van Jacobson TCP/IP header compression is used for the connection. Default.	No	Yes
Framed-IP-Address	IP Address	The user's IP address.	No	Yes
Framed-IP-Netmask	Netmask	The user's netmask.	No	Yes
Framed-IPX-Network	Dotted decimal IPX network number	IPX network number.	No	Yes

Table 4-4 User Profile Check and Reply Items (Continued)

Item	Options	Explanation	Used as Check Item?	Used as Reply Item?
Framed-MTU	Number	Number of bytes in maximum transmission unit (MTU).	No	Yes
Framed-Protocol	PPP	PPP is used for the connection.	Yes	Yes
	SLIP	SLIP is used for the connection.	No	Yes
Framed-Route	Destination IP address	The IP address of the destination network.	No	Yes
	Gateway IP address	The IP address of the gateway to the destination network.	No	Yes
	Metric	The number of routing hops to the destination network. Also known as the hop count.	No	Yes
Framed-Routing	None	Disables RIP on the interface.	No	Yes
	Broadcast	The interface sends RIP updates.	No	Yes
	Listen	The interface listens for RIP updates.	No	Yes
	Broadcast-Listen	The interface sends and listens for RIP updates.	No	Yes
Group	String of characters in double quotation marks (" ")	List of groups that users belong to.	Yes	No

Table 4-4 User Profile Check and Reply Items (Continued)

Item	Options	Explanation	Used as Check Item?	Used as Reply Item?
Idle-Timeout	In seconds	Specifies the idle time limit for a session.	No	Yes
Login-IP-Host	IP address	Address of the remote host.	No	Yes
Login-Service	Telnet	Establishes a Telnet connection to the remote host.	No	Yes
	Rlogin	Establishes an rlogin connection to the remote host.	No	Yes
	TCP-Clear	Establishes a TCP clear connection to the remote host.	No	Yes
	PortMaster	Establishes a connection to the remote host using the PortMaster login service.	No	Yes
Login-TCP-Port	TCP port number	TCP port number of the Login-Service.	No	Yes
Menu	Menu name in double quotation marks (" ")	Defines a menu in a user record. See Chapter 6, "Configuring RADIUS Menus."	No	Yes
NAS-IP-Address	IP address	PortMaster IP address.	Yes	No
NAS-Port	Number	The PortMaster port number that the user is dialed in to (for example, NAS-Port = S2).	Yes	No
NAS-Port-Type	ISDN	ISDN port.	Yes	No

Table 4-4 User Profile Check and Reply Items (Continued)

Item	Options	Explanation	Used as Check Item?	Used as Reply Item?
	Async	Asynchronous port.	Yes	No
	Sync	Synchronous port.	Yes	No
	ISDN-V120	ISDN in V.120 mode.	Yes	No
	ISDN-V110	ISDN in V.110 mode.	Yes	No
Password	User's password		Yes	No
Port-Limit	Number of B channels for ISDN Multilink PPP or Multilink V.120	Specifies the maximum number of B channels a user can use.	No	Yes
Prefix	String of characters in double quotation marks (" ")	Prepended to username to match a user to a particular user profile. Used primarily for DEFAULT profiles.	Yes	No
Session-Timeout	In seconds	Specifies the time limit for a session.	No	Yes
Service-Type	Login-User	User connects via Telnet, rlogin, PortMaster, or TCP-Clear login service.	Yes	Yes
	Framed-User	User uses PPP or SLIP for the connection.	Yes	Yes
	Outbound-User	User uses Telnet for outbound connections.	Yes	Yes
	Callback-Login-User	Calls user back and connects via Telnet, rlogin, PortMaster, or TCP-Clear login service.	No	Yes

Table 4-4 User Profile Check and Reply Items (Continued)

Item	Options	Explanation	Used as Check Item?	Used as Reply Item?
Suffix	Callback-Framed-User	Calls user back and establishes a framed connection (PPP or SLIP). Location must be specified in PortMaster location table.	No	Yes
	Administrative-User	Grants user full access to all configuration commands.	No	Yes
	NAS-Prompt-User	Grants user limited access to commands (nonconfiguration only).	No	Yes
	String of characters in double quotation marks (" ")	Appended to username to match a user to a particular user profile. Used primarily for DEFAULT profiles.	Yes	No
	Termination-Menu	Menu name in double quotation marks (" ")	No	Yes

Using RADIUS with PAP and CHAP

You can use RADIUS with Password Authentication Protocol (PAP) or Challenge Handshake Authentication Protocol (CHAP).

PAP

The PortMaster sends the PAP ID and password to the RADIUS server in an Access-Request packet as the User-Name and User-Password. The PortMaster includes the Service-Type = Framed-User and Framed-Protocol = PPP attributes in the request as a hint to the RADIUS server that PPP service is expected.

To authenticate a user with PAP, user profiles can include Auth-Type = Local, Auth-Type = System, or Auth-Type = SecurID.

CHAP

For CHAP, the PortMaster generates a random challenge and sends it to the user. The user returns a CHAP response, CHAP ID, and CHAP username. The PortMaster then sends an Access-Request packet to the RADIUS server with the CHAP username as the User-Name and with the CHAP ID and CHAP response as the CHAP-Password. The random challenge can either be included in the CHAP-Challenge attribute or, if it is 16 octets long, it can be placed in the Request Authenticator field of the Access-Request packet. The PortMaster includes the Attributes Service-Type = Framed-User and Framed-Protocol = PPP as a hint to the RADIUS server that PPP service is expected.

The RADIUS server does the following:

1. **Looks up a password based on the User-Name.**
2. **Uses MD5 to encrypt the password, the CHAP ID octet, and the CHAP challenge.**
3. **Compares the result to the CHAP-Password.**

If they match, the server sends an Access-Accept packet to the PortMaster. If there is no match, the server sends back an Access-Reject packet.

CHAP requires that the user's password be available on the server in unencrypted (clear text) format so that the server can encrypt the CHAP challenge and compare the result to the CHAP response. If the password is not available in clear text server sends an Access-Reject to the client.

To force all authentication over PPP to CHAP, do the following:

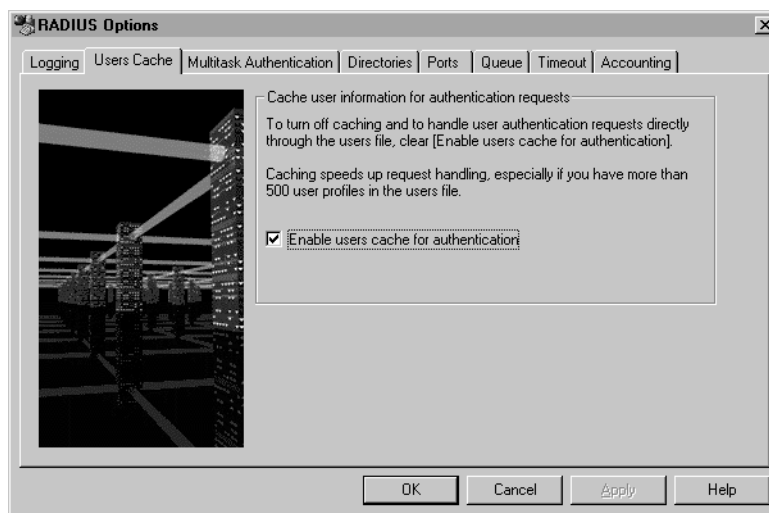
1. **Set the Auth-Type = Local.**
2. **Set passwords in clear text; they must not be encrypted.**
3. **Turn off PAP and turn on CHAP by using the following commands on the PortMaster:**

```
Command> set pap off
Command> set chap on
```

Configuring Database Caching of User Profiles

RADIUS offers database support for caching user profiles to increase the speed and efficiency of user lookups. Lucent Remote Access recommends caching user profiles when the users file contains more than 500 users.

To configure the database cache options, choose **Users Cache** from the Options menu. Alternatively, click the **Options** button, and then click the **Users Cache** tab.



12740013

To use the database to cache user requests, ensure that the **Enable users cache for authentication** option is selected.

If caching is used, you must update the database each time the users file is updated. To update the database, click the **Update Users Cache** button on the RADIUS Control Panel, or choose **Update Users Cache** from the File menu. A pop-up window displays the number of user and DEFAULT profiles in the **users** file. If the **Enable users cache for authentication** option is not selected, the **Update Users Cache** button is disabled and you cannot update the users cache.

You can also update the database from the DOS command line by entering the following command:

```
C:\program files\lucent\RADIUS\radsvc.exe" -builddb
```

The number of users in the **users** file is also logged into the event log. Use the Event Viewer in the Administrator Tools menu to display the event log.

Example PPP User Profile

User profiles can be configured in a number of ways to fit network security requirements. The following example illustrates a typical RADIUS profile for a PPP user:

```
bob Password = "ge55gep"
    Service-Type = Framed-User,
    Framed-Routing = None,
    Framed-Protocol = PPP,
    Framed-IP-Address = 255.255.255.254,
    Framed-Compression = Van-Jacobson-TCP-IP,
    Framed-MTU = 1500,
    Filter-Id = "firewall"
```

In this example, user *bob* has password **ge55gep**. He is a Framed-User, which indicates that he uses SLIP or PPP for his connections. In the following line, Framed-Protocol is specified as PPP.

An IP address of 255.255.255.254 is specified, indicating that an IP address is assigned to *bob* from the PortMaster assigned address pool.



Note – To create an assigned address pool, see the *Configuration Guide for PortMaster Products*.

Framed-Routing is set to **None**, which disables RIP for *bob*'s interface. RIP packets are not sent or listened for. Van Jacobson TCP/IP compression is used for the connection, and the MTU is set to 1500 bytes.

The Filter-Id identifies the packet filter(s) used for the connection if any are defined on the PortMaster or in ChoiceNet; **firewall.in** is used as an input filter and **firewall.out** is used as an output filter.

This chapter describes the utilities included with RADIUS for Windows NT. The RADIUS Control Panel provides the following utilities:

- **Authentication Test Utility**—enables you to test RADIUS authentication request packets to verify authentication is working and to troubleshoot some user problems.
- **Data Source/Table Copy Utility**—enables you to copy the schema for one or more data source tables into a new table.
- **User Manager Utility**—provides a convenient way to bring up the Windows NT User Manager window from within the application.
- **System Diagnostics Utility**—provides a convenient way to bring up the Windows NT Diagnostics window from within the application.

Testing RADIUS Authentication

You can quickly test whether the RADIUS server can successfully authenticate a user by performing the following steps:

1. **On the RADIUS Control Panel, select Tools**➡Authentication Test Utility.

The RADIUS Authentication Tester dialog box appears.

Radius Authentication Tester

Authentication

Server: localhost

Secret: xxxxxx

User Name: mary

Password: xxxxxxxx

Repeat: 200

Attempt: 0

Latency (ms): 0

Avg Latency (ms): 0

Logon

Quit

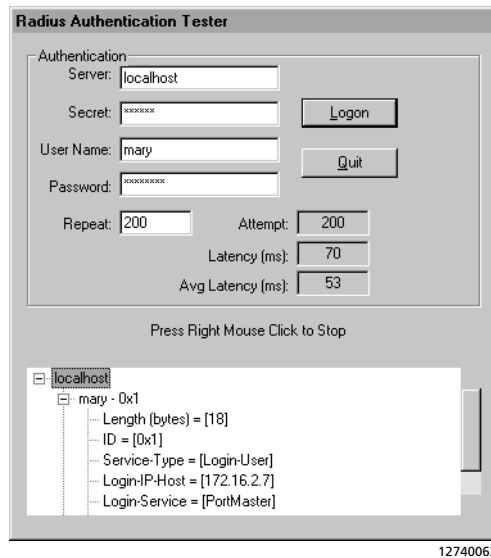
Press Right Mouse Click to Stop

12740062

Values for user, password, server name, secret, and number of test cycles are provided by default. You can alter any of these as you need.

For example, you can point to any RADIUS server—rather than using the default **localhost**—as long as the server recognizes your computer as a client. You must update the **clients** file on the RADIUS server you are pointing to with the IP address of your computer and provide a shared secret in the **clients** file and the test window.

2. Click Logon to test authentication with the default values.



You can click the right mouse button to halt a test in progress. Click **Quit** to close the test window.

The test does the following:

- Sends authentication request packets to the RADIUS server
- Receives the response
- Measures the latency of the authentication response for each test packet
- Calculates the average latency over the set of test packets
- Parses the attributes and displays them in the browser below the test fields

You can use the utility to test usernames that are causing problems to help you pinpoint the error. Use the test with prefixed or suffixed usernames to verify the default results of such user logins.

Copying Database Tables

You can use the **Data Source/Table Copy** utility to copy your RADIUS database tables. Reasons for copying the tables include the following:

- Archiving your accounting or authentication data
- Moving your tables to another location
- Backing up your data to secondary tables when you modify your primary tables

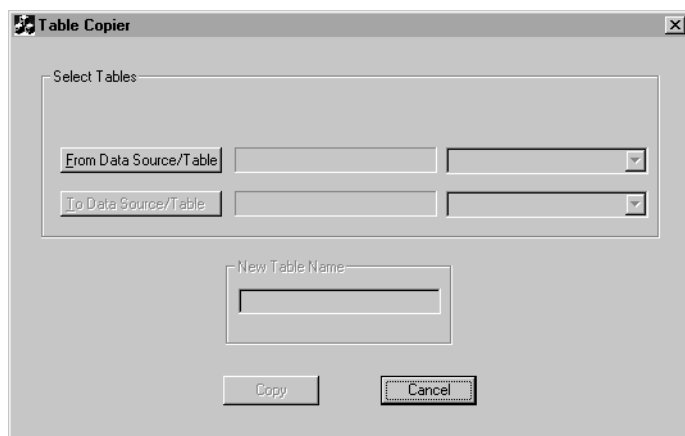
The utility creates a new table that you specify and associate with a data source. The new table uses the schema from the data source and table that you specify. The data from the specified table is then copied into the new table.

The example shown in this section copies a RADIUS accounting database table.

To copy a database table, perform the following steps:

1. **On the RADIUS Control Panel, select Tools**➔Data Source/Table Copy Utility.

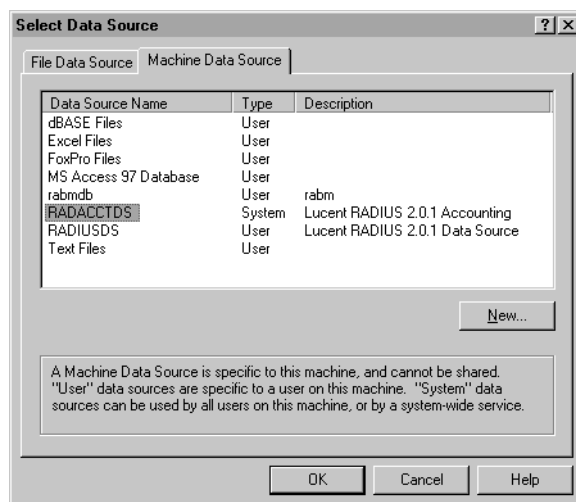
The Table Copier dialog box appears.



12740064

2. **Click From Data Source/Table.**

The Select Data Source dialog box appears.



12740019

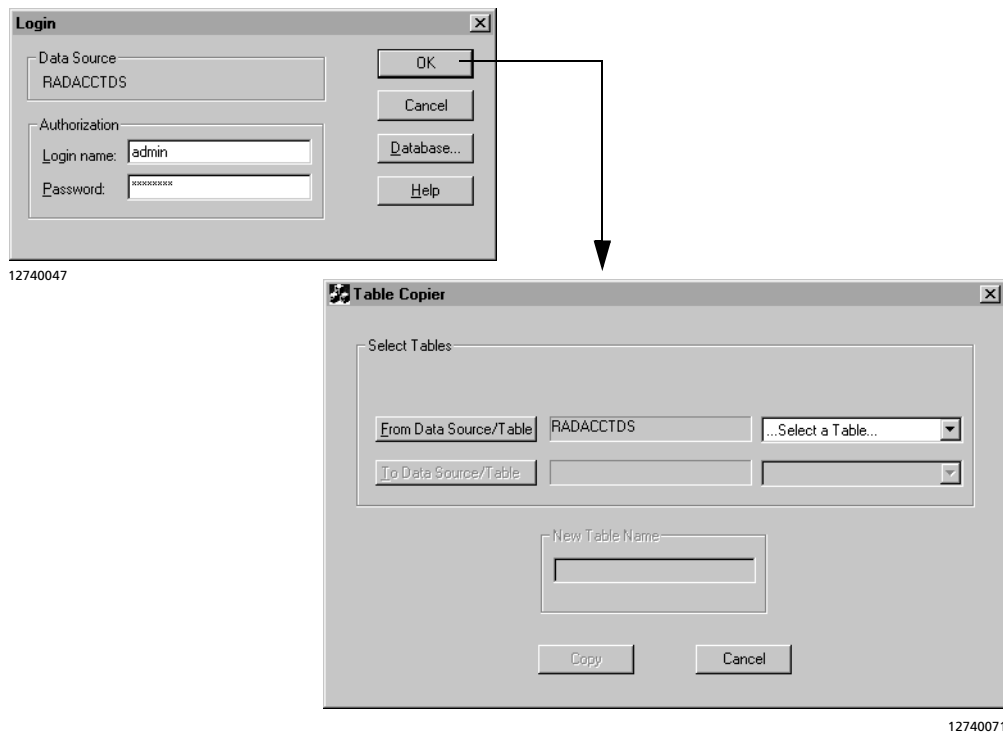
3. **Select the Machine Data Source tab.**
4. **Select the desired Data Source Name and click OK.**

The Login dialog box appears.



12740070

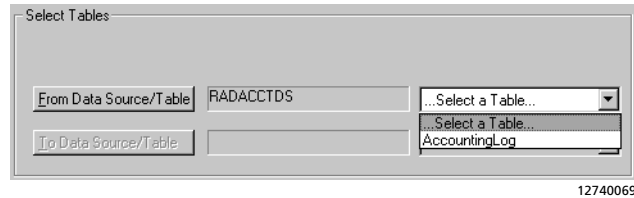
5. Enter your Login Name and Password and click OK to return to the Table Copier.



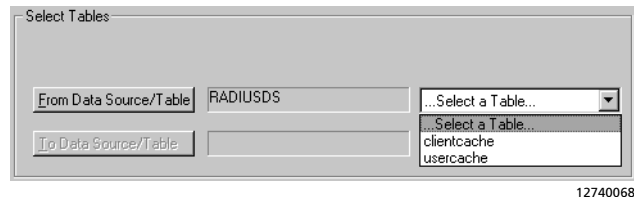
You associated the data source with a RADIUS for NT database when you configured the server. Typically, you maintain that association when copying tables, but you can choose to make a new association. If you want a new association, click **Database...** in the Login dialog box, then navigate to and select the desired database in the Select Database dialog. This is illustrated in Step 7 through Step 9 on page 2-22.

6. Select a table from the drop-down list.

- If you are copying the **RADACCTDS** data source, the only table choice is **AccountingLog**.



- If you are copying the **RADIUSDS** data source, select either **clientcache** or **usercache**.



7. Click To Data Source/Table.

The Select Data Source dialog box appears.

8. Select the Machine Data Source tab.

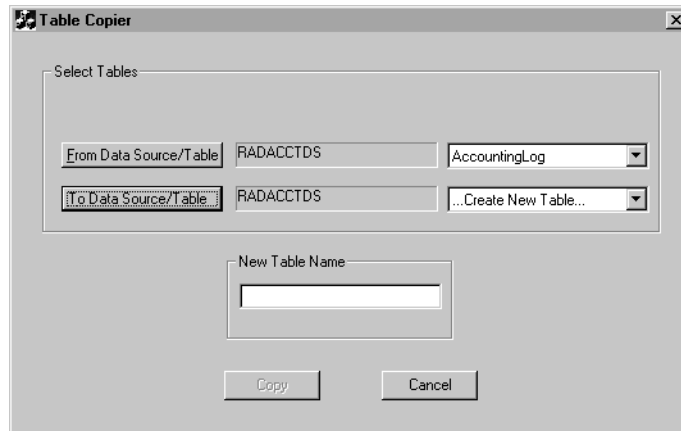
9. Select the desired Data Source Name and click OK.

10. Select an option from the drop-down list.

You can choose one of the following:

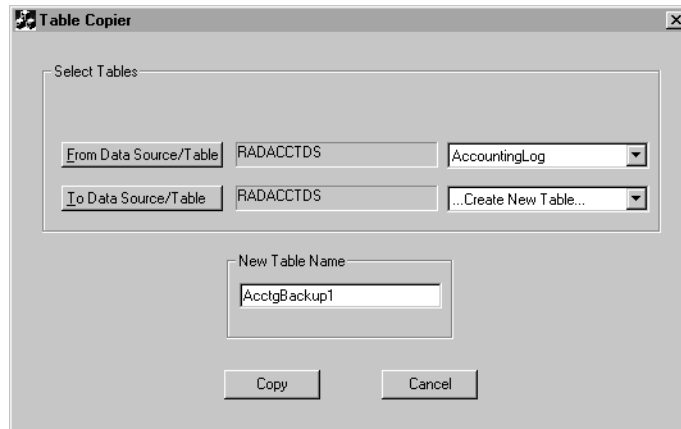
- Create a new table if you want a new table name. This is the usual choice.
- Use a preexisting table. The tables listed are the same as those in the *From* drop-down list. Because this can overwrite your current database table, you typically choose this option only if you have selected a different data source or a different location for the database.

This example shows the results of choosing to create a new table.



12740073

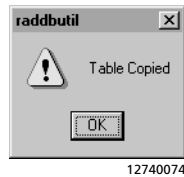
11. Enter the name of the new table.



12740074

12. Click Copy.

An Alert dialog notifies you when the copying process is completed.



Operating System Utilities

For your convenience, RADIUS for NT provides a quick way to access two Windows NT utilities.

You can manage security and access for Windows NT groups and group members by selecting **Tools⇒User Manager Utility** on the RADIUS Control Panel.

You can display and manage many operating system resources and variables by selecting **Tools⇒System Diagnostics Utility** on the RADIUS Control Panel.

For more information on using these operating system utilities, see your Windows NT documentation.

RADIUS menus enable a user to select different login options after being authenticated. The user only needs a single username for all options rather than a different username for each connection option. A menu is displayed if the Menu reply item is present in the user profile.

RADIUS menus are implemented as text files located in the **menus** subdirectory on the RADIUS server, typically **C:\winnt\system32\drivers\etc\raddb\menus**. The number of menu files under the **menus** directory is unlimited. A menu file can accommodate up to 2KB of display data plus menu selection entries. Menus can refer to other menus.

Menu File Format

A menu file consists of the following elements:

- An initial line containing only the keyword **menu**
- Additional lines of text to be displayed to the user
- A line containing only the keyword **end**
- One or more menu selection entries
- The DEFAULT menu selection entry

The **menu** and **end** keywords indicate the start and end of the text displayed to the user. Text between the **menu** and **end** keywords can be any printable ASCII characters up to a maximum of 2Kb. The text in the menu file is case-sensitive.

Each menu selection entry consists of the menu choice shown at the beginning of a line, followed by one or more lines of reply items—one per line—starting with spaces or tabs. You can enter comments among the menu selection entries by starting each comment line with a number sign (#).

The special menu choice DEFAULT must be the last menu selection entry. The DEFAULT menu is called when the user enters no choice or a choice that does not match a menu selection entry in the menu file.

Use the special menu choice EXIT for a menu selection—such as “Quit”—that disconnects the user.

Single-Level Menu

A single-level menu does not refer to other menus. The following example shows a file named **/etc/raddb/menus/menu1** for a single-level menu:

```
menu
    *** Welcome to EDU OnLine ***
    Please select an option:

        1.  Start SLIP session
        2.  Start PPP Session
        3.  Quit

    Option:
end
# This is a single-level menu called Menu1
1
    Service-Type = Framed-User,
    Framed-Protocol = SLIP,
    Framed-IP-Address = 255.255.255.254,
    Framed-Routing = None,
    Framed-MTU = 1006,
    Termination-Menu = "menu1"
#
2
    Service-Type = Framed-User,
    Framed-Protocol = PPP,
    Framed-IP-Address = 255.255.255.254,
    Framed-Routing = None,
    Termination-Menu = "menu1"
#
3
    Menu = "EXIT"
#
DEFAULT
    Menu = "menu1"
```

In the single-level menu example, after RADIUS authenticates the user, **menu1** is displayed and the user is prompted to select a service from this menu. Once the user has finished the selected SLIP or PPP session, the termination menu—also menu1 in this

case—is displayed and the user is prompted to select a new service. If you do not include a Termination-Menu reply item in the list of reply items corresponding to the user's menu selection, the user is disconnected immediately after the session completes.

Nested Menus

Nested menus refer to other menus. In the following example menu file, the menu that the user sees has an **other** option; if selected, this option displays a second menu:

```
menu
*** Welcome to the Internet Service ***
Please enter an option:
    ppp - Start PPP session
    telnet - Begin login session with a host
    other - Display a second menu
Option:
end
# This is a nested menu called Menu2
ppp
    Service-Type = Framed-User,
    Framed-Protocol = PPP,
    Framed-IP-Address = 255.255.255.254,
    Framed-Routing = None,
    Framed-MTU = 1500
#
telnet
    Service-Type = Login-User,
    Login-IP-Host = 172.16.1.81,
    Login-Service = Telnet,
    Login-TCP-Port = 23
#
other
    Menu = "menu3"
#
DEFAULT
    Menu = "menu2"
```

Termination Menus

Termination menus are presented to users when their service ends. The termination menu must be contained within double quotation marks. The Termination-Menu reply item in the user's profile calls the menu.

With the user profile shown in the following example, user *bob* sees **menu1** when he finishes his PPP session. When *bob* selects a menu option, the corresponding service is provided.

```
bob    Password = "ge55gep"
       Service-Type = Framed-User,
       Framed-Protocol = PPP
       Framed-IP-Address = 255.255.255.254,
       Framed-Routing = None,
       Termination-Menu = "menu1"
```

Menus Called by Reference

Any user profile in the **users** file—including the DEFAULT profile—can call a menu by reference. The Menu reply item is the only reply item in the user profile when a menu is referenced.

```
DEFAULT    Auth-Type = System
           Menu = "menu1"
```

In this example, after user *bob* is authenticated, the **menu1** menu is displayed and he is prompted to make a selection. When *bob* selects a menu option, the corresponding service is provided.

Menu Filenames

You must create the menu filename in the **menus** subdirectory of the RADIUS server, described on page 6-1. Menu names can consist of up to 120 printable, nonspace, ASCII characters; in the **users** file the menu name must be enclosed in double quotation marks (" ").

Security Dynamics provides an additional level of security in user identification and authentication by using SecurID tokens to generate codes and ACE/Server software to process the codes. This software and hardware authentication system is often referred to as **SecurID**.

This chapter is an overview of the installation and basic configuration of ACE/Server and ACE/Client software when used with RADIUS. This chapter includes the following topics:

- “Overview of SecurID Components” on page 7-2
- “How SecurID Works with RADIUS” on page 7-3
- “ACE/Server Installation on a Windows NT Host” on page 7-3
- “RADIUS Configuration for SecurID” on page 7-14
- “Troubleshooting SecurID” on page 7-18

This information is intended to serve as a quick reference guide for the ACE/Server and ACE/Client software. Refer to the Security Dynamics manual set for detailed features of SecurID and future ACE/Server software releases.



Note – Lucent Remote Access Technical Support does not provide support for the ACE/Server and ACE/Client installation and configuration. Contact Security Dynamics Technical Support at 800-995-5095 from within the United States, or +44-118-936-2699 from outside the United States. Lucent Remote Access Technical Support provides support for RADIUS when used with ACE/Server and SecurID only after you have verified that the ACE/Server is working properly.

The ACE/Server and ACE/Client software version 2.3 is supported on the following platforms:

- Windows NT Workstation 4.0
- Windows NT Server 4.0

Additionally, this software is supported on several UNIX platforms.

Overview of SecurID Components

The Security Dynamics authentication system (generally referred to as *SecurID*) consists of the following components:

- ACE/Server master

Stores usernames and serial numbers of tokens and performs calculations to verify the identity of users.

- ACE/Server slave

Functions as a secondary server to the ACE/Server master.

- ACE/Client

A computer or other device protected by ACE/Server. ACE/Client software must be installed on these systems.

- Token

A device that generates a random number known as a **tokencode** (the software might show this as two words: **token code**). A new number is generated and displayed every 60 seconds. Five types of tokens are supported in SecurID: the standard SecurID card, the SecurID Key Fob, SecurID PINPAD card, SecurID Modem, and SoftID. The first three tokens are small, handheld devices.

RADIUS has been tested with the standard SecurID card, the SecurID Key Fob, and the SecurID PINPAD card.

- PASSCODE

A two-part password, consisting of a memorized personal identification number (PIN) followed by the current tokencode displayed on the token.



Note – To use RADIUS with SecurID, you typically run the ACE/Server software on the same host as the RADIUS server. If you install the ACE/Server software on a different machine, then you must install the SecurID ACE/Server slave component on the RADIUS server host. The ACE/Server slave must then reference the ACE/Server master.

How SecurID Works with RADIUS

When SecurID is used with RADIUS, a connection proceeds as follows:

1. A remote user initiates a connection by dialing in to the PortMaster.
2. The PortMaster prompts for the user's username and password.
3. The user enters a username. At the password prompt, the user enters a PASSCODE (PIN followed by the currently displayed number on the token).
4. The PortMaster forwards this information to the RADIUS server for authentication.
5. The RADIUS server examines the **users** file, scanning for the appropriate username. When the profile is located, it is examined to determine the user's authentication method.
6. When the RADIUS server discovers that the authentication method is SecurID, it forwards the username and PASSCODE to the ACE/Server for authentication.
7. The ACE/Server examines its database for the username and serial number of the user's token. It uses the serial number to verify the PASSCODE entered by the user. It also verifies that the time on the token is synchronized with the ACE/Server.
8. The ACE/Server sends the result of the database lookup (identity verified or not verified) to the RADIUS server.
9. If the user's identity was verified by the ACE/Server, the RADIUS server sends an access-accept message to the PortMaster along with the additional information from the RADIUS user profile. If the ACE/Server rejected the user's PASSCODE, the RADIUS server sends an access-reject message to the PortMaster.

ACE/Server Installation on a Windows NT Host

RADIUS for Windows NT is compatible with ACE/Server version 2.3 or higher. This section provides guidelines for the installation and use of ACE/Server and ACE/Client version 2.3. Refer to the appropriate Security Dynamics documentation for information on other versions of ACE software.

The master ACE/Server handles the authentication requests passed on to it by the RADIUS server configured as an ACE/Client. The master and client software can be installed on the same host.

You can increase the reliability of the authentication process if you configure the ACE/Client and an ACE/Server slave on a separate host or hosts from the ACE/Server master. In the event the host for the ACE/Server master goes down, the ACE/Server slave handles the authentication requests from the ACE/Client.

These instructions cover the following:

- “Installing a Master Server” on page 7-6
- “Installing a Master Server and a Slave Server” on page 7-7
- “Configuring the Master Server” on page 7-8
- “Installing ACE/Client on the Server” on page 7-11
- “Starting the ACE/Server” on page 7-12
- “Testing SecurID Server-to-Client Communication” on page 7-13

This is not a complete explanation of all SecurID requirements or procedures. If you are upgrading a previous ACE/Server installation to version 2.3, you must read the *ACE/Server v 2.3 for Windows NT Administration Manual* from Security Dynamics for instructions.



Note – Read the *ACE/Server v 2.3 for Windows NT Administration Manual* before beginning installation.

SecurID software is not shipped with the PortMaster. This software must be ordered directly from Security Dynamics at 800-995-5095 from within the United States or +1-617-687-7700 from outside the United States.

Getting Started

SecurID installation requires a host that meets the following requisites. See the *ACE/Server v 2.3 for Windows NT Administration Manual* for more information. These requirements are for SecurID alone, and do not reflect the requirements for RADIUS.

Platform

SecurID requires an Intel Pentium 166 or higher processor running Microsoft Windows NT Server or Workstation version 4.0 with Service Pack 2 or higher—RADIUS for NT requires Service Pack 3. The host must have a local CD-ROM drive, a monitor set to a minimum of 800 x 600 pixels, and NTFS File system.

Physical Memory

SecurID requires a minimum 32MB of physical memory.

Disk Space

SecurID requires

- 200MB for ACE/Server software
- 10MB for ACE/Server databases
- 20MB for ACE/Server Remote Administration software
- 1MB for ACE/Client for Windows NT

Refer to the *ACE/Server v 2.3 for Windows NT Administration Manual* for disk requirements for ACE database management.

ACE/Server Service Names and Port Numbers

Authentication Service. The installer places the default name—**securid**—and port number—**5500**—for the SecurID authentication service in the **C:\winnt\system32\drivers\etc\services** file. If the installer is successful, the Configuration Management window displays this information.

If some other process is using this port, a message appears telling you to change the authentication port. To change the port number from 5500, follow these steps:

1. **Use any text editor to modify the C:\winnt\system32\drivers\etc\services file.**
2. **Use the ACE/Server Configuration Management window to change the port number expected by the authentication service process.**

Master/Slave Communication Service. The default name—**securidprop**—and port number—**5510**—for the SecurID master/slave communication service is placed in the **C:\winnt\system32\drivers\etc\services** file when you enable the slave and enter the name of the slave computer using Configuration Management. If the installer is successful, the Configuration Management window displays this information.

If some other process is using this port, a message appears telling you to change the port on the slave computer that is used by the authentication service. To change the port number from 5510, follow these steps:

1. Use any text editor to modify the C:\winnt\system32\drivers\etc\services file.
2. Use the ACE/Server Configuration Management window to change the port number expected by the authentication service process on the slave computer.

Installing a Master Server

Use this procedure if you are installing **only** a master server without a slave server.

To install a new master server, complete the following steps:

1. Insert the ACE/Server CD-ROM into the host CD drive.
2. Insert the floppy diskette ACE/Server License File into your diskette drive.
3. Click the Windows NT Start button and select Run.
4. Enter D:\ACESERV\NT_I386\Setup.exe and click OK.

Substitute the appropriate drive letter of your CD-ROM drive for D.

5. Click OK.

The Setup window appears.

6. Follow the instructions on the screen to complete the installation process.

A setup wizard guides you through the ACE/Server installation. The following steps are particularly important:

- a. In the Installation Type dialog box, do the following:
 - Select **Master ACE/Server**.
 - Enter the **Destination** where you want the server installed—for example, **C:\ACE**. The partition containing the destination directory must be formatted for Windows NT File System (NTFS) rather than File Allocation Table File System (FATFS), which is used by Windows 95.
 - Click **Next**.
- b. In the Encryption Type window, check **SDI**; then click **Next**.
- c. In the Start Copying Files window, click **Next**.

The wizard copies the ACE/Server files from the CD-ROM to your system. When the Setup Complete window appears, remove the floppy from your diskette drive, check **Yes**, **Restart My Computer**, and click **Finish**.

7. **Use any text editor to add the hostname for the ACE/Server to the C:\winnt\system32\drivers\etc\hosts file.**
8. **From a DOS prompt, copy C:\ace\data\sdconf.rec to the C:\winnt\system32 directory.**

The ACE/Server software is typically installed on the same machine as the RADIUS server. To run ACE/Server on a different machine, you must configure the RADIUS server as an ACE/Server slave. See “Installing a Master Server and a Slave Server” in the next section.

9. **Click the Windows NT Start button and then select Settings➔Control Panel to verify ACE/Server is present.**
10. **Go to “Configuring the Master Server” on page 7-8.”**

Installing a Master Server and a Slave Server

Use this procedure if you are installing a master server and a slave server.

To install a new master server and a slave server, complete the following steps:

1. **Insert the ACE/Server CD-ROM into the host CD drive.**
2. **Insert the floppy diskette ACE/Server License File into your diskette drive.**
3. **Click the Windows NT Start button and select Run.**
4. **Enter D:\ACESERV\NT_I386\setup.**
Substitute the appropriate drive letter of your CD-ROM drive for *D*.
5. **Click OK.**
6. **Follow the instructions on the screen to complete the installation process.**
7. **Click the Windows NT Start button and then select Programs➔ACE Server➔Configuration Management.**
The Configuration Management window appears.
8. **Click Edit, enable the slave server, and enter the name of the slave server.**

The software fills in the IP address of the slave server as well as the default port and services information for communication with the master server.

- 9. Click OK to save the new configuration.**
- 10. Copy \ace\data\sdconf.rec to the C:\winnt\system32 directory.**
- 11. Go to “Configuring the Master Server.”**

Configuring the Master Server

Configuring the master server consists of the following procedures:

- “Adding the Site and Client” on page 7-8.
- “Importing Tokens to the ACE/Server Database” on page 7-9.
- “Adding a User” on page 7-9.
- “Synchronizing the Token” on page 7-11.

After the master server is configured, you must install the ACE/Client, start the ACE/Server, and test the communication between server and client.

Adding the Site and Client

- 1. Click the Windows NT Start button and select Programs⇒ACE Server⇒Database Administration.**

The ACE/Server Database Administration window appears.

- 2. Select Site⇒Add Site.**

The Add Site dialog box appears.

- 3. Enter a site name and click OK.**

- 4. Select Client⇒Add Client.**

The Add Client dialog box appears.

- 5. Enter a client name and click OK.**

The client name must match the hostname entered in the C:\winnt\system32\drivers\etc\hosts file.

6. **Select the Site added in Step 2.**
7. **Select Net OS client type and click OK.**
8. **Go to “Importing Tokens to the ACE/Server Database.”**

Importing Tokens to the ACE/Server Database

You must put token records in your database before you can use it. These records might be in a file that you brought over from another system acting as an ACE/Server, or might have been shipped to you when you ordered the ACE/Server software.

To import tokens to the ACE/Server Database for Windows NT on the master server, complete the following steps:

1. **On the master server, click the Windows NT Start button and then select Programs⇒ACE Server⇒Database Administration.**

The Database Administration window appears.

2. **Select Token⇒Import Tokens.**

The **Filename** dialog box appears.

3. **Select the token record file.**

Enter the path and filename of the token record file, or browse your system for the token record filename, which ends in **.asc**.

4. **Click OK to add the token records to the database and close the Filename dialog box.**

5. **Select Token⇒List Tokens to verify that you successfully imported the token records.**

6. **If you intend to run the database administration application from machines other than the master server, you must refer to the *ACE/Server for Windows NT Administration* manual for additional installation instructions.**

7. **Go to “Adding a User.”**

Adding a User

You must create a user record for each SecurID user. Perform the following steps:

1. Create an NT user.

2. On the master server, click the Windows NT Start button and then select Programs⇒ACE Server⇒Database Administration.

The Database Administration window appears.

3. Select User⇒Add User.

The **Add User** dialog box appears.

4. Enter the first name and last name of the user.

5. Enter a Default shell, such as /bin/csh.

6. Click Assign Token.

The Confirmation dialog box appears.

7. Click Yes.

The Select Token dialog box appears.

8. Click Tokens and select the token you want to assign to this user; then click OK.

You return to the ACE/Server Database Administration window.

9. Select User⇒Edit User.

The **Edit User** dialog box appears.

10. Click Client Activation.

The Client Activation dialog box appears.

11. Select the client and click Activate On Client.

The Activate User dialog box appears.

12. Click OK.

You return to the Client Activation dialog box.

13. Click Exit.

You return to the Edit User dialog box.

14. Click OK.

15. Go to “Synchronizing the Token.”

Synchronizing the Token

1. **On the master server, click the Windows NT Start button and then select Programs→ACE Server→Database Administration.**

The Database Administration window appears.

2. **Select Token→Edit Token.**

The **Edit Token** dialog box appears.

3. **Select the token.**

4. **Click Resynchronize tokens.**

5. **Enter the current token code displayed on the token and click OK.**

6. **Wait until the token code changes on the token, then enter that number and click OK.**

A message appears stating “Token successfully resynchronized.”

7. **Go to “Installing ACE/Client on the Server.”**

Installing ACE/Client on the Server

The RADIUS server acts as the client to the ACE/Server. Before installing the ACE/Client software, you must first complete the steps in “Installing a Master Server” on page 7-6 or “Installing a Master Server and a Slave Server” on page 7-7.



Note – Read *ACE/Client for Windows NT v4.0* from Security Dynamics before beginning installation.

To install the ACE/Client for Windows NT on the master server, complete the following steps:

1. **Insert the ACE/Server CD-ROM into the host CD drive.**
2. **Insert the floppy diskette ACE/Server License File into your diskette drive.**
3. **Click the Windows NT Start button and select Run.**
4. **Enter D:\ACECLNT\NT_I386\Setup.exe and click OK.**

Substitute the appropriate drive letter of your CD-ROM drive for *D*.

5. **Click OK.**
6. **Follow the instructions on the screen to complete the installation process.**

A setup wizard guides you through the ACE/Client installation. The following steps are particularly important.

- a. In the Setup window, click **Next**.
- b. In the License Agreement dialog box, click **Accept**.

The wizard copies the ACE/Client files from the CD-ROM to your system. When this is completed, the message “!ACE/Client for Windows NT v. 4.0 has been successfully installed.” appears in the Setup window

- c. Remove the floppy from your diskette drive and click **Finish**.
- d. Restart your computer.
- e. Click the Windows NT **Start** button and then select **Settings⇒Control Panel** to verify ACE/Client is present.

See the *ACE/Client for Windows NT v4.0* manual for further information on how to set up and administer the ACE/Client.

7. **Go to “Starting the ACE/Server.”**

Starting the ACE/Server

1. **On the master server, click the Windows NT Start button and then select Settings⇒Control Panel⇒ACE/Server.**

The Ace/Server window appears.

2. **Check Automated ACE/Server startup.**

This causes the ACE/Server to start up whenever the system reboots.

3. **Click Start.**

A message box appears stating “ACE/Server Started.”

4. **Click OK to return to the ACE/Server window.**
5. **Click OK to close the ACE/Server window.**

6. Go to “Testing SecurID Server-to-Client Communication” in the next section.

Testing SecurID Server-to-Client Communication

Before you configure RADIUS for Windows NT to work with ACE/Server, test the communication between the ACE/Server and the ACE/Client. If the test is successful, you have eliminated the ACE/Server installation and configuration as a cause of any subsequent problems.

1. **On the master server, click the Windows NT Start button and then select Settings⇒Control Panel⇒ACE/Client.**

The Ace/Client window appears.

2. **Click Test Authentication with ACE/Server.**

The Test Authentication dialog box appears.

3. **Enter a username.**

This must be a name for a valid SecurId user that has been added to the database. See “Adding a User” on page 7-9.

4. **Enter the token code displayed on the token.**

If the ACE/Server accepts the request, a dialog box appears asking you to choose between entering a PIN or accepting a system-generated PIN. At this point, you know that the client has successfully communicated with the server.

If the test authentication fails and you get a “Node Validation Failure” message, do the following:

- a. Go to a DOS prompt.
- b. Enter **attrib -r C:\winnt\system32\securid.**
- c. Enter **del C:\winnt\system32\securid.**
- d. View the activity log on the ACE/Server panel to determine the cause of the failure.

Installing Other ACE/Server Features

For any other ACE/Server installation and configuration options, refer to the ACE/Server documentation.



Note – Lucent Remote Access Technical Support does not provide support for the ACE/Server and ACE/Client installation and configuration problems. Contact Security Dynamics Technical Support at 800-595-5095 from within the United States, or +44-118-936-2699 from outside the United States. Lucent Remote Access Technical Support provides support for RADIUS when used in conjunction with SecurID only after you have verified that the ACE/Server is working properly.

RADIUS Configuration for SecurID

Each SecurID user must have a profile in the RADIUS **users** file or must use a DEFAULT profile. In the profile, the Auth-Type check item must be **SecurID**, as shown in the following example:

```
DEFAULT    Auth-Type = SecurID
           Service-Type = Framed-User,
           Framed-Protocol = PPP,
           Framed-Address = 255.255.255.254,
           Framed-Routing = None,
           Framed-MTU = 1500
```

To activate and assign tokens to users authenticated with this DEFAULT profile, do the following:

1. **Select** Start➔Programs➔ACE Server➔Database Administration **to display the Database Administration window.**
2. **Select** User➔Edit User **to activate a user.**
3. **Select** Token➔Edit Token **to assign and enable a token.**

When user *bob* dials in to the PortMaster, the following prompts are displayed:

```
login: <enter username>
Password: <enter PIN number followed by a token code>
```


PIN Assignment

When a new user is added to the ACE/Server database, a token is assigned to the user. How the authentication is completed depends on how you have specified PIN generation. You can require the ACE/Server to generate PINs for all users, you can force all users to provide their own PINs, or you can enable specified users to choose the generation method.

Users must provide their PINs in New PIN mode. You can also force other users into New PIN mode if they have forgotten their PINs or if an attacker has learned their PINs.

A user in New PIN mode can create the PIN using RADIUS when dialing in to the network. Refer to information on PIN administration in the *ACE/Server v 2.3 for UNIX Administration Manual* or *ACE/Server v 2.3 for Windows NT Administration Manual* for more information on New PIN mode.

User-Created PIN

When a user in New PIN mode is forced to create a PIN via RADIUS, the user is prompted to enter a new PIN:

```
login: bob
Password: xxxxx
Enter PASSCODE: <token code>
    Enter your new PIN, containing 4 to 8 digits,
    or
    <Ctrl d> to cancel the new PIN procedure:
```

In this example, when user *bob* dials in to the network, he logs in with his username and UNIX password. When prompted for the PASSCODE—a PIN followed by the token code—*bob* enters the token code displayed on his SecurID device. The PortMaster sends an access-request to the RADIUS server. The ACE/Server searches its database and recognizes user *bob* as a New PIN mode user. It sends an access-challenge to the PortMaster, and *bob* is prompted to enter a new PIN.

After *bob* enters his new PIN, the RADIUS server responds with the following message:

```
Please re-enter new PIN:
Wait for the code on your token to change, then log in with the new PIN
Enter PASSCODE:
PASSCODE accepted
```

User *bob* re-enters the new PIN. After a few seconds, the token code on his SecurID device changes. User *bob* enters the PIN and the token code, and is authenticated. For subsequent logins, *bob* enters his PIN followed by the currently displayed token code when prompted for the PASSCODE.

System-Generated PIN

When you specify that the PIN is generated by the system, the user is prompted to initiate PIN generation. The new PIN is displayed on the screen for the user to memorize.



Note – The system-generated PIN appears for only 10 seconds. After the PIN disappears, it cannot be viewed again.

In the following example, *keiko* logs in with her username and UNIX password for the first time. When prompted for the PASSCODE—a PIN followed by the token code—*keiko* enters the token code displayed on her SecurID device.

```
login: keiko
Password:
Enter PASSCODE: <token code>
    Press <Return> to generate a new PIN and display it on the screen,
    or
    <Ctrl d> to leave your token in New PIN mode:
ARE YOU PREPARED TO HAVE THE SYSTEM GENERATE A PIN? (y or n) (n): y
```

When prompted, *keiko* indicates that she wants the system to generate her PIN. As shown in the following example, the PIN is displayed, and *keiko* is prompted to enter the new PASSCODE.

```
Your screen will automatically clear in 10 seconds.  
Your new PIN: NNNNN  
Wait for the code on your token to change, then log in with the new PIN  
Enter PASSCODE:  
PASSCODE Accepted.
```

For subsequent logins, *keiko* enters her system-generated PIN followed by the currently displayed token code when prompted for the PASSCODE.

Entering an Invalid Token Code

If a user enters a valid PIN and an invalid token code, the token goes into Next Tokencode mode. The user is prompted to enter the next code from the token. This prompt also appears if the user's token is not synchronized with the ACE/Server.

The user must wait until the token code changes and then enter the new token code number at the prompt. After the system verifies the second token code, the user is authenticated.

If an unauthorized user enters a stolen PIN followed by a guessed token code, he is given three opportunities to enter the correct token code. If three invalid token codes are entered, the unauthorized user is disconnected.

In the following example, *paolo* has entered a valid PIN followed by an invalid token code. The prompt appears, indicating that *paolo's* token is not synchronized with the ACE/Server, or that *paolo* has entered an invalid token code. User *paolo* must wait for 60 seconds for a new token code and then must enter this code at the prompt. In this example, *paolo* has entered the next code and it has been accepted.

```
login: paolo  
Password: <PIN number followed by invalid token code>  
Please Enter the Next Code from Your Token:  
PASSCODE Accepted
```

Troubleshooting SecurID

Refer to your SecurID manuals for information on troubleshooting SecurID. If you still have problems after trying these solutions, contact Security Dynamics Technical Support at 800-995-5095 from within the United States or +44-118-936-2699 from outside the United States

RADIUS accounting logs information about dial-in connections. This information is often used for billing purposes. RADIUS accounting consists of a client/server format. On a Windows NT host, transactions are recorded as they occur either in an SQL database, in the **C:\usr\adm\radacct\portmastername\detail** file, or both.

This chapter includes the following topics:

- “How RADIUS Accounting Works” on page 8-1
- “Getting Started” on page 8-3
- “Client Configuration” on page 8-4
- “Accounting Server Configuration” on page 8-4
- “Accounting Attributes” on page 8-10
- “Examples” on page 8-15

How RADIUS Accounting Works

RADIUS accounting consists of an accounting server and accounting clients (PortMaster products). RADIUS accounting starts automatically when the RADIUS server starts.

RADIUS uses the UDP protocol. The RADIUS accounting server listens for UDP packets on port 1646 by default.

RADIUS accounting consists of the following steps:

1. The PortMaster (accounting client) sends an **accounting-request** packet containing the record of an event to the accounting server. The record is described by the values of RADIUS attributes included in the packet.

For example, when a user is authenticated and connected, the Acct-Status-Type attribute has a value indicating that the request marks the beginning of user service. The RADIUS accounting server records this event as a Start accounting record. The records are recorded in a file called **C:\usr\adm\radacct\portmastername\detail** on a Windows NT server.



Note – RADIUS automatically creates the *portmastername* directory and the **detail** file. If the IP address of a PortMaster client cannot be resolved to a hostname, then the name of the directory is the IP address of the PortMaster rather than its name

When the user's connection ends, the Acct-Status-Type attribute has a value indicating that the request marks the end of user service. The RADIUS accounting server records this as a Stop accounting record. The Stop record contains the same information as the Start record; however, it also includes Acct-Session-Time, which records the time (in seconds) of a user's session.

2. The accounting server sends an **accounting-response** packet back to the PortMaster to acknowledge receipt of the request. The server must send back an acknowledgment when it records the request.
3. If the PortMaster does not receive a response, it continues to send accounting-requests until it receives a response.

A backoff algorithm is used to determine the delay between accounting-requests if an accounting-response is not received.

4. The PortMaster records the number of seconds that have passed between the event and the current attempt to send the record; this number is the Acct-Delay-Time value. As additional time passes before an accounting-response is received, the Acct-Delay-Time is updated.

Table 8-1 lists all possible attributes that might be found in an accounting record.

Table 8-1 Possible Attributes in **detail** File

User-Name	Called-Station-Id
NAS-IP-Address	Calling-Station-Id
NAS-Port	Acct-Status-Type
Service-Type	Acct-Delay-Time
Framed-Protocol	Acct-Input-Octets
Framed-IP-Address	Acct-Output-Octets
Filter-Id	Acct-Session-Id
Login-IP-Host	Acct-Authentic
Login-Service	Acct-Session-Time
Login-TCP-Port	Acct-Terminate-Cause
Framed-IPX-Network	NAS-Port-Type
Session-Timeout	Connect-Info
Idle-Timeout	Request-Authenticator
Datestamp	Acct-Timestamp

Getting Started

Select a host to use as the RADIUS accounting server. This host can be either the same host as the RADIUS server used for authentication or a separate host.

Choose a host with the following characteristics:

- Secure physical location
- Root access limited to the security officer or system administrator
- Limited number of user accounts—preferably none
- Basic memory

- Enough disk space to store the RADIUS accounting **detail** files

For typical installations, allocate 50MB per 1000 users if the logs are rotated monthly. Keep in mind that allocating too much space is preferable to allocating too little; your usage can vary.

For example, if you have 1000 users, one port for every 10 users, an average connection time per user of 1 hour, and all ports in use around the clock, one month of logs would require 50MB of disk space:

$$700 \text{ bytes/session} * 1000 \text{ users} * 1 \text{ port}/10 \text{ users} * 1 \text{ session/hour} * 24 \text{ hours/day} * 31 \text{ days/month}$$

The use of a secondary RADIUS accounting server is recommended. The primary accounting server is always used first; if this server is unavailable, the secondary server is used.

The PortMaster always sends accounting packets to the primary RADIUS accounting server first and retries it once every 45 seconds. If the primary server does not respond within 10 minutes, or if there are more than 50 accounting packets waiting to be sent, the PortMaster sends the accounting packets to the secondary RADIUS accounting server.

Client Configuration

To configure RADIUS accounting information on a PortMaster, see Chapter 3, “Adding a RADIUS Client.”

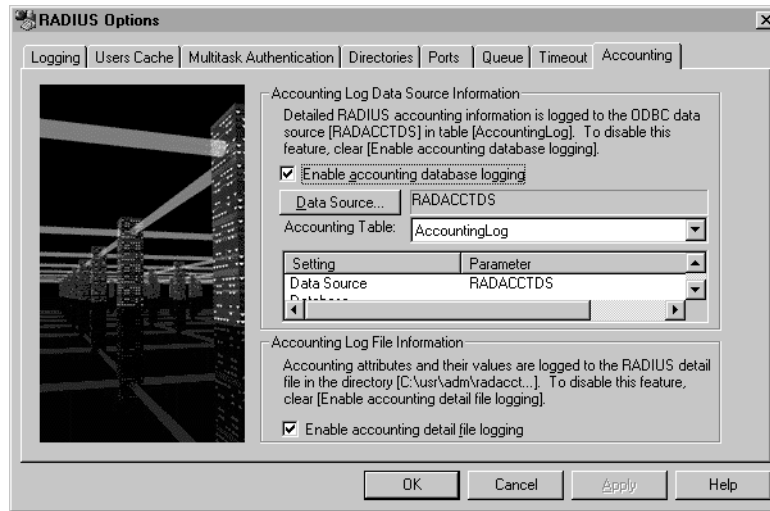
Accounting Server Configuration

The RADIUS for Windows NT installation program automatically creates the **C:\usr\adm\radacct** directory for the RADIUS accounting server. See Chapter 2, “Configuring a RADIUS Server,” for information on installing the RADIUS accounting and authentication servers.

Configuring Accounting Database Logging

When accounting database logging is on, RADIUS for Windows NT logs detailed RADIUS accounting information to the ODBC data source in the specified table.

To configure database logging, navigate to the Accounting tab.

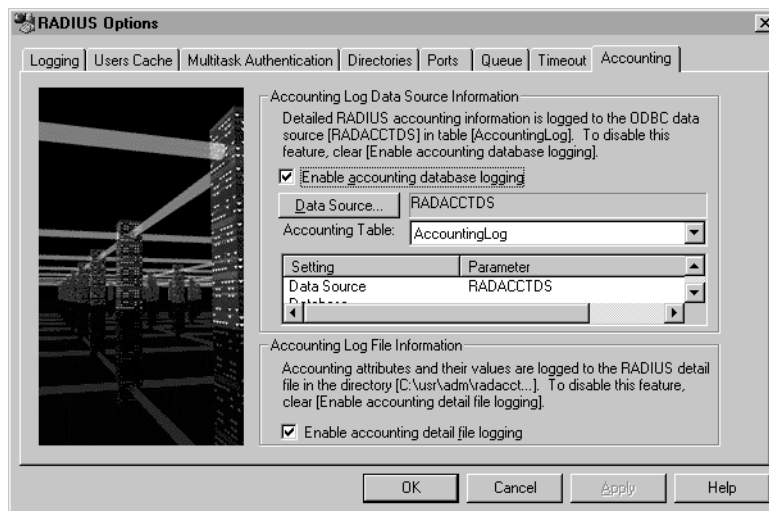


12740018

To use the accounting database logging feature, ensure that the **Enable accounting database logging** option is selected. To turn off accounting database logging, clear the **Enable accounting database logging** option. Click **Apply** or **OK** to save your changes.

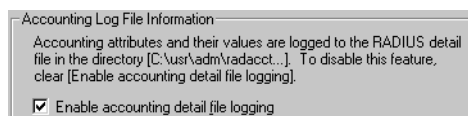
Configuring Accounting Detail File Logging

When accounting detail file logging is selected, RADIUS for Windows NT logs detailed RADIUS accounting information into the **detail** file in the **C:\usr\adm\radacct\portmastername** directory. To configure detail file logging, navigate to the Accounting tab.

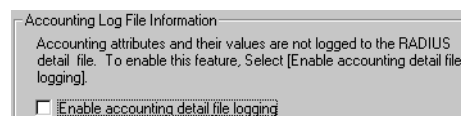


12740018

To enable detail file logging, select the **Enable accounting detail file logging** option. To disable this feature, clear the **Enable accounting detail file logging** option.



12740027



12740028

Click **Apply** or **OK** to save your changes.

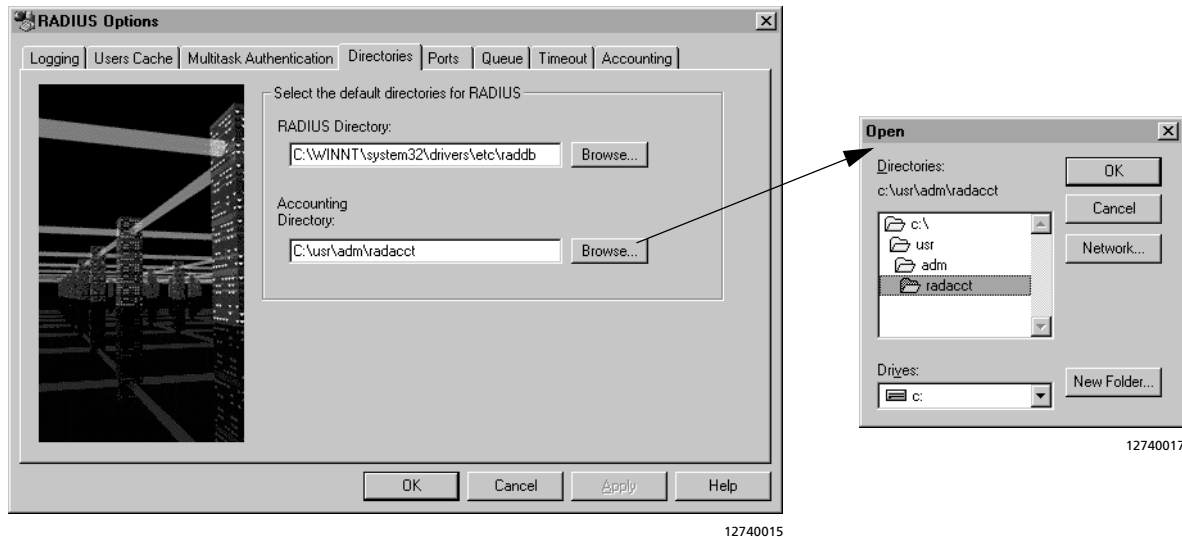
Determining the Server Version

The version number of the software is the same for the RADIUS accounting and authentication servers. You can determine the version number by selecting **Help**→**About RADIUS** on the RADIUS Control Panel.

Changing the Accounting Directory Location

RADIUS for Windows NT automatically creates a subdirectory within the **C:\usr\adm\radacct** directory for each PortMaster serving as a PortMaster accounting client.

To change the default accounting directory for the RADIUS accounting server, navigate to the Directories tab. Enter the desired location manually in the Accounting Directory: text box, or click **Browse...** and select the desired directory location. Click **Apply** or **OK** to save your changes.



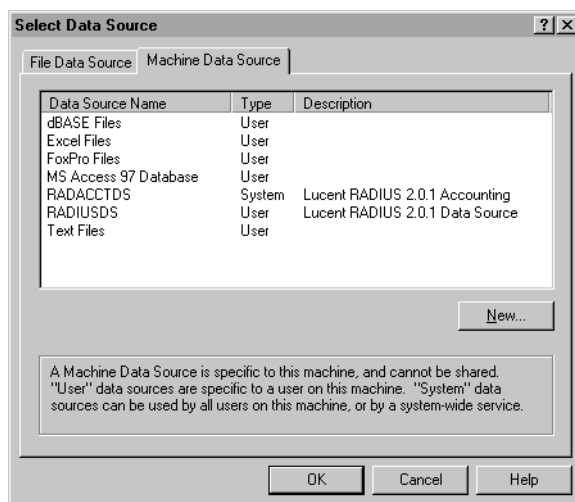
Specifying an ODBC Data Source

You can use ODBC-compliant databases other than Microsoft Access. You can create another accounting database for RADIUS to use while you are working on the original database. To specify a new ODBC data source different from the one you configured during installation, navigate to the Accounting tab. Perform the following steps:

1. **Click** Data Source....

The Select Data Source dialog box appears.

2. Select the Machine Data Source tab.

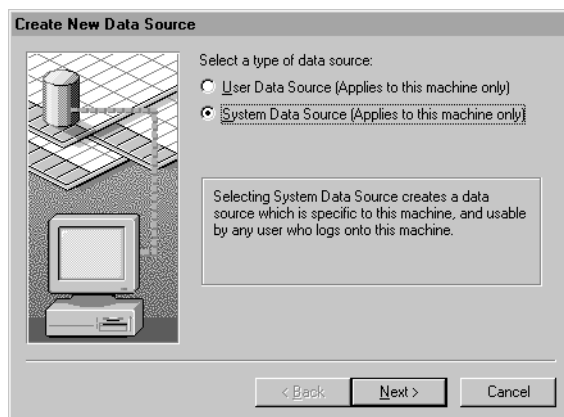


12740044



Note – The machine data source is specific to your server and cannot be shared. If you have selected a file data source, RADIUS might not appear to the system as a service. Selecting a file data source generates an error window and the data source is rejected.

3. Click New... to display the Create New Data Source dialog box.



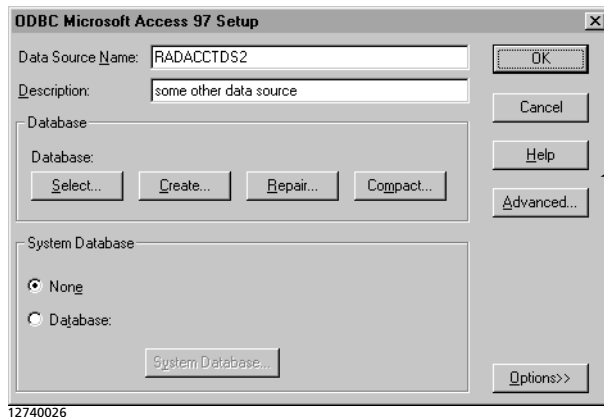
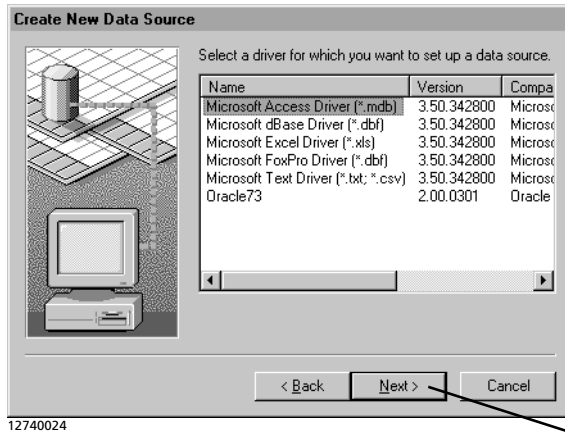
12740023

4. Select the *System* source type.



Note – Selecting the user source type generates an error window and the data source is rejected. When RADIUS is enabled as a Windows NT service, the server considers the system—rather than you, the logged-in user—to be running RADIUS.

5. Click Next and follow the directions in each dialog box.



6. Click Apply or OK to save your changes.

Accounting Attributes

For RADIUS accounting to function, a series of accounting attributes are defined in the **dictionary** file on the RADIUS server and appear in the Start and Stop accounting records. Use the following descriptions to help you interpret Start and Stop records.

Acct-Authentic

Acct-Authentic records whether the user was authenticated via RADIUS or by the PortMaster user table. Accounting records are not generated for passthrough users, because those users are authenticated by the destination host.

Acct-Delay-Time

The PortMaster records the number of seconds that have passed between the event and the current attempt to send the record; this number is the Acct-Delay-Time value.

You can determine the approximate time of an event by subtracting the Acct-Delay-Time value from the time of the record's arrival on the RADIUS accounting server.

Acct-Input-Octets and Acct-Output-Octets

Acct-Input-Octets records the number of bytes received and Acct-Output-Octets records the number sent during a session. These values appear only in Stop records.

Acct-Session-Id

Acct-Session-Id is a unique number assigned to each Start and Stop record to make it easy to match the Start and Stop records in a **detail** file, and to eliminate duplicate records.

The Acct-Session-Id is a string consisting of eight uppercase hexadecimal digits. The first two digits increment each time the PortMaster is rebooted. The next six digits begin at 0—*nn*000000 for the record sent on reboot, *nn*000001 for the first user login after a reboot—and increment up to approximately 16 million logins. This value equals the number of logins a user can make in one year if she logs in once a minute to every port of a 30-port PortMaster.

Acct-Session-Time

Acct-Session-Time records the user's connection time in seconds. This information is included only in Stop records.

Acct-Status-Type

Acct-Status-Type has two values: **Start** and **Stop**. A Start record is created when a user session begins. A Stop record is recorded when the session ends.

Acct-Terminate-Cause

The values returned by Acct-Terminate-Cause, which are shown in Table 8-2, indicate the cause of a session's termination. This information appears only in Stop records.

Table 8-2 Session Termination Causes

Termination Cause	Meaning
Admin-Reboot	System administrator is ending service on the NAS—for example, prior to rebooting the NAS.
Admin-Reset	Port was reset by an administrator.
Callback	Callback user was disconnected so port can be used to call the user back.
Host-Request	Session was disconnected or logged out by the Login-IP-Host. This attribute value can indicate normal termination of a login session, or that the remote host has failed or become unreachable.
Idle-Timeout	Idle timer expired for user or port.

Table 8-2 Session Termination Causes (*Continued*)

Termination Cause	Meaning
Lost-Carrier	<p>Session terminated when the modem dropped the Data Carrier Detect (DCD) signal. This value can indicate any of the following:</p> <ul style="list-style-type: none">• The user or his modem hung up the telephone from their end; no problem exists.• The line was dropped.• The modem was unable to recover from severe line noise.• The local modem dropped DCD for some other reason.
Lost-Service	<p>Service can no longer be provided—for example, the user's connection to a host was interrupted.</p>
NAS-Error	<p>NAS detected some error other than on the port, which required ending the session.</p>
NAS-Reboot	<p>NAS ended the session to perform a nonadministrative reboot—a system crash.</p>
NAS-Request	<p>NAS ended the session for a nonerror reason not otherwise listed here.</p>
Port-Error	<p>PortMaster had to reset the port. This error commonly occurs when a device attached to the port causes too many interrupts.</p>
Port-Preempted	<p>NAS ended the session in order to allocate the port to a higher priority use.</p>
Port-Suspended	<p>NAS ended the session to suspend a virtual session.</p>
Port-Unneeded	<p>NAS ended the session because resource usage fell below low-water mark—for example, if a bandwidth-on-demand algorithm decided that the port was no longer needed.</p>
Service-Unavailable	<p>NAS was unable to provide the requested service.</p>

Table 8-2 Session Termination Causes (Continued)

Termination Cause	Meaning
Session-Timeout	Session timer expired for the user.
User-Error	Because the PortMaster received a PPP configuration request or acknowledgment when a session was already established, it terminated the session. This error is caused by a PPP implementation error in the dial-in client.
User-Request	Dial-in PPP client requested that the PortMaster terminate the connection. This message is expected from a proper PPP client termination.

Acct-Timestamp

Acct-Timestamp records the time of arrival on the RADIUS accounting host measured in seconds since the epoch (00:00 January 1, 1970). This attribute provides a machine-friendly version of the logging time at the beginning of the accounting record. To find the actual time of the event, subtract Acct-Delay-Time from Acct-Timestamp.

Called-Station-Id and Calling-Station-Id

Called-Station-Id records the telephone number called by the user. Calling-Station-Id records the number the user is called from. This information is recorded when the NAS-Port-Type is ISDN, ISDN-V120, or ISDN-V110 where supported by the local telephone company. On the PortMaster 3, this information is available for asynchronous calls as well, where supported by the local telephone company.

Datestamp

Datestamp records the full date and time of arrival on the RADIUS accounting host. It does not record milliseconds. This attribute provides a human-friendly version of the logging time at the beginning of the accounting record.

NAS-Port-Type

NAS-Port-Type records the type of port used in the connection. The port type can be any of the following: Async, Sync, ISDN, ISDN-V120, or ISDN-V110.

Request-Authenticator

The Request-Authenticator attribute appears in an accounting record only when the RADIUS 2.0-or-later server detects a problem with the accounting request's digital signature. A Request-Authenticator of **None** means that the accounting request was not digitally signed and was probably sent by a PortMaster running a version of ComOS that did not sign accounting packets. If the Request-Authenticator value is **Unverified**, the accounting request signature did not match the expected value. Ensure that the shared secret on the PortMaster matches the shared secret in the **/etc/raddb/clients** (UNIX) or **C:\winnt\system32\drivers\etc\raddb\clients** (Windows NT) file.

Examples

Use a text editor such as Notepad or WordPad to view the RADIUS **detail** file. Figure 8-1 displays Start and Stop accounting records in a PortMaster **detail** file on a Windows NT host:

Figure 8-1 Example Detail File: **rlogin**

```
detail.txt - Notepad
File Edit Search Help

Wed Aug 12 09:32:34 1998
  Acct-Session-Id = "15000003"
  User-Name = "jaime"
  NAS-IP-Address = 172.16.64.91
  NAS-Port = 2
  NAS-Port-Type = Async
  Acct-Status-Type = Start
  Acct-Authentic = RADIUS
  Service-Type = Login-User
  Login-Service = Rlogin
  Login-IP-Host = 172.16.64.25
  Acct-Delay-Time = 0
  Timestamp = 902939554

Wed Aug 12 09:33:34 1998
  Acct-Session-Id = "15000003"
  User-Name = "jaime"
  NAS-IP-Address = 172.16.64.91
  NAS-Port = 2
  NAS-Port-Type = Async
  Acct-Status-Type = Stop
  Acct-Session-Time = 60
  Acct-Authentic = RADIUS
  Acct-Input-Octets = 10
  Acct-Output-Octets = 131
  Acct-Terminate-Cause = Host-Request
  Service-Type = Login-User
  Login-Service = Rlogin
  Login-IP-Host = 172.16.64.25
  Acct-Delay-Time = 0
  Timestamp = 902939614
```

The Acct-Status-Type attribute in the record indicates whether the record was sent when the connection began (Start) or when it ended (Stop). The Acct-Session-Id is listed at the beginning of the record. Note that this value matches the Acct-Session-Id of the Stop record, indicating that these records correspond to the same session.

User-Name specifies the username, in this case, *jaime*. NAS-IP-Address specifies the IP address of the PortMaster. NAS-Port indicates the port on which the connection is made. NAS-Port-Type specifies that this is an asynchronous connection. Acct-Authentic specifies that *jaime* is authenticated via RADIUS. Service-Type and Login-Service specify that *jaime* is a login user using **rlogin**. Login-IP-Host specifies the host that user *jaime* logged in to.

In the Stop accounting record, Acct-Session-Time specifies that *jaime's* connection lasted 60 seconds. Acct-Input-Octets indicates that 10 bytes of incoming traffic were received; Acct-Output-Octets indicates that 131 bytes of outgoing traffic were sent.

The Acct-Terminate-Cause indicates that a Host-Request terminated the session, meaning that *jaime* logged off the host or that the host logged him off. The Acct-Delay-Time is 0 seconds, indicating that the RADIUS accounting server received the accounting-request on the first try.



For more information on accounting attributes, see “Accounting Attributes” on page 8-10.

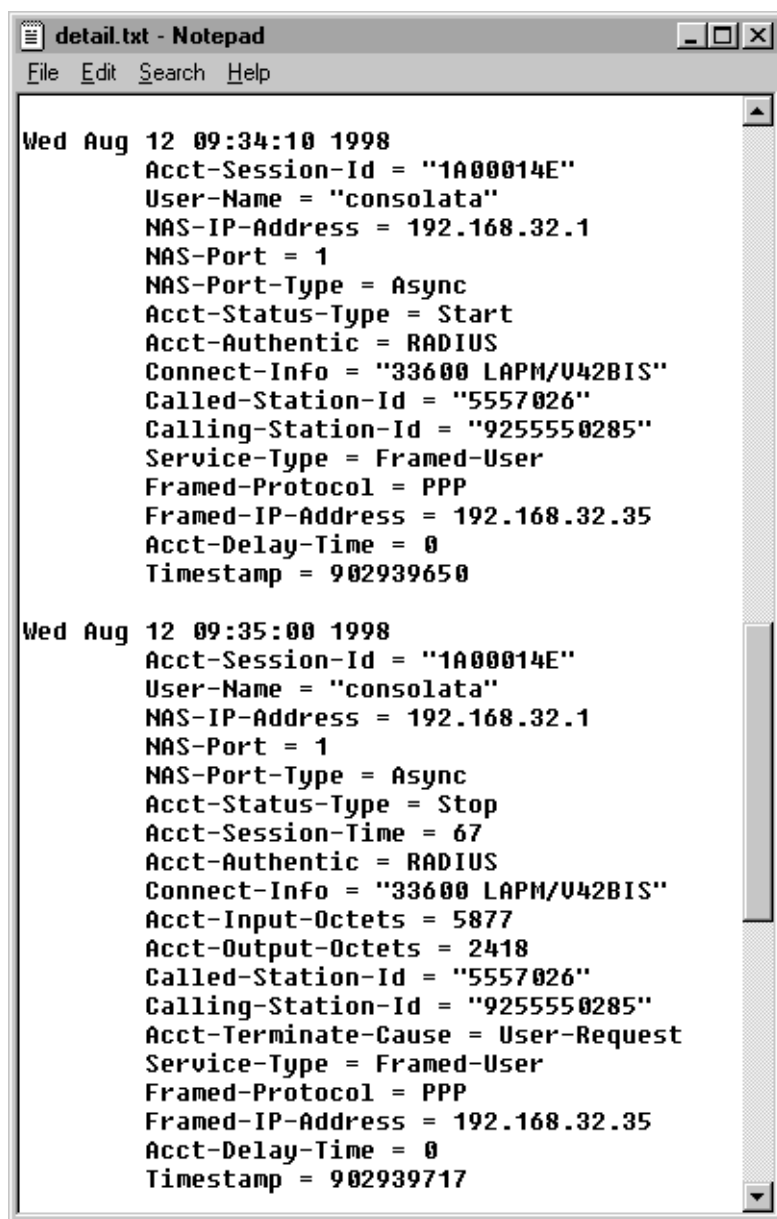
Figure 8-2 displays the Start and Stop accounting records for an ISDN PPP connection. In the Start record of this example, the NAS-Port-Type specifies that the user *consolata* is using Async for her connection. Called-Station-Id and Calling-Station-Id specify the source and destination of the Async call. Service-Type and Framed-Protocol indicate that user *consolata* is a framed user using PPP to establish the connection.

The Stop record in this example indicates that the login time for user *consolata* was 67 seconds. The Acct-Input-Octets and Acct-Output-Octets indicate that the incoming traffic for this session was 5877 bytes, and outgoing traffic was 2418 bytes.



Note – Examples of Perl scripts to process the RADIUS accounting logs are available at the Lucent Remote Access FTP site at **<ftp://ftp.livingston.com/pub/le/radius/>**.

Figure 8-2 Example Detail File: PPP



```
detail.txt - Notepad
File Edit Search Help

Wed Aug 12 09:34:10 1998
  Acct-Session-Id = "1A00014E"
  User-Name = "consolata"
  NAS-IP-Address = 192.168.32.1
  NAS-Port = 1
  NAS-Port-Type = Async
  Acct-Status-Type = Start
  Acct-Authentic = RADIUS
  Connect-Info = "33600 LAPM/V42BIS"
  Called-Station-Id = "5557026"
  Calling-Station-Id = "9255550285"
  Service-Type = Framed-User
  Framed-Protocol = PPP
  Framed-IP-Address = 192.168.32.35
  Acct-Delay-Time = 0
  Timestamp = 902939650

Wed Aug 12 09:35:00 1998
  Acct-Session-Id = "1A00014E"
  User-Name = "consolata"
  NAS-IP-Address = 192.168.32.1
  NAS-Port = 1
  NAS-Port-Type = Async
  Acct-Status-Type = Stop
  Acct-Session-Time = 67
  Acct-Authentic = RADIUS
  Connect-Info = "33600 LAPM/V42BIS"
  Acct-Input-Octets = 5877
  Acct-Output-Octets = 2418
  Called-Station-Id = "5557026"
  Calling-Station-Id = "9255550285"
  Acct-Terminate-Cause = User-Request
  Service-Type = Framed-User
  Framed-Protocol = PPP
  Framed-IP-Address = 192.168.32.35
  Acct-Delay-Time = 0
  Timestamp = 902939717
```

12740077

This appendix provides hints and tips for troubleshooting the RADIUS authentication server and the RADIUS accounting server.

Troubleshooting RADIUS Authentication

Most RADIUS authentication problems occur because the server or client was not configured correctly, or because a step was omitted during installation. Carefully check the instructions in Chapter 2, “Configuring a RADIUS Server,” and Chapter 3, “Adding a RADIUS Client,” to ensure that the authentication server was properly installed and configured.

If you have not solved the problem after reviewing the instructions in Chapter 2 and Chapter 3, read the troubleshooting suggestions in this section.

Testing for Successful Authentication

You can use the Authentication Test Utility to perform simple, repeated tests of RADIUS authentication. See Chapter 5, “Using RADIUS for NT Utilities,” for more information.

NIC Problems

The RADIUS host must have only a single NIC card installed. Additionally, there must not be more than a single IP address associated with the host’s NIC card.

Checking the RADIUS NT Service

- 1. Go to the Services applet and ensure that RADIUS for Windows NT has been installed and is started.**
- 2. Go to the RADIUS Control Panel and verify that it indicates that RADIUS for Windows NT is currently running.**

RADIUS is running if the **Stop RADIUS service** button is visible and the message in the status bar at the bottom of the panel indicates RADIUS activity.

3. Examine the Windows NT event log for records verifying RADIUS is running.

Click the Windows NT **Start** button and select
Programs⇒Administrative Tools (Common)⇒Event Viewer.

Dr. Watson Window

If a Dr. Watson window pops up, the RADIUS service has stopped running. In this case, perform the following steps:

1. Email the Dr. Watson log file and a complete description of the problem to Lucent Remote Access Technical Support at support@livingston.com.

Your email must include the following information:

- Version of Windows NT you are running on the Windows NT host
- Version of Windows NT Service Pack installed on the Windows NT host
- **All** applications present on the Windows NT host—not just those running
- Hot fixes or other patches installed, and their origins, for **all** applications present on the Windows NT host—not just for those running
- Version of all applications running on your host at the time of the problem

2. Restart the RADIUS service.

If RADIUS stops again, perform Step 3.

3. Reboot the Windows NT host.

This is not usually necessary.



Note – A Dr. Watson window can appear only if RADIUS is running as a nonservice or if you have changed the service properties to enable the service to interact with the desktop.

Checking the PortMaster

1. Make sure that security is on for each port:

```
Command> set all security on
Command> save all
Command> reset all
```

When security is on, the **show S0** command displays **(Security)** in the Port Type field of its output.

2. Use the show global command to verify the following:

- RADIUS server IP address is set on the PortMaster
- Secondary RADIUS server does not have the same IP address as the primary server

3. Make sure that the PortMaster can contact the RADIUS server:

```
Command> ping Ipaddress
```

4. Make sure the secret set on the PortMaster with the set secret password command matches the secret in the /etc/raddb/clients file on the RADIUS server.

The PortMaster will not display the shared secret; however, you can set the secret again if you are not sure that it is set properly. If you update the shared secret, make sure to use the **save all** command to save the shared secret in the PortMaster nonvolatile memory.

Checking /etc/raddb/users

1. Items in the user entries are case-sensitive. You must do the following:

- a. Verify the spelling and capitalization of each line of the **users** file.
- b. Compare keywords against the **/etc/raddb/dictionary** file to ensure that they are the same.

- c. Check the event log for “Can’t Parse” errors, which indicate an entry in the **users** file with a spelling or capitalization error. Correct the error in the **users** file.
2. **Verify that the user can authenticate with a clear text password before authenticating with** Auth-Type = System **or** Auth-Type = SecurID.

Host Unavailable

If a “Host Unavailable” message is displayed before a username is entered at the login prompt, then **both** of the following conditions exist:

- Autolog username was set on the port.
- Default host is not responding to the login service. The default host is either defined for the port or defined in the PortMaster user table for the user. The login service—**rlogin** or **telnet** or **in.pmd**—is either defined for the port or defined in the PortMaster user table for the user.

If a “Host Unavailable” message is displayed after a username is entered at the login prompt, but before a password is entered, **all** of the following conditions exist:

- Username exists in the local user table
- No password associated with the username
- Default host is not responding to the login service—**rlogin**, **telnet**, or **in.pmd**

If a “Host Unavailable” message is displayed after a username and password are entered at the login prompt, **either** of the following conditions might exist:

- Security for the port is disabled and default host is not responding to the login service—**rlogin**, **telnet**, or **in.pmd**
- Security for the port is enabled and default host is not responding to the login service—**rlogin**, **telnet**, or **in.pmd**

To verify that security is not enabled, enter the following command. If necessary, replace **s1** with the port that you are using.

```
Command> show s1
```

If (**Security**) is not displayed in the Port Type field, enter the following commands to enable security for the port:

```
Command> set s1 security on
Command> reset s1
Command> save all
```

Invalid Login after 30-Second Wait

If the PortMaster sends 10 access-requests at 3-second intervals and then displays an “Invalid Login” message, this message can indicate one of the following problems:

- RADIUS is not running on the server.

Verify **radsvc.exe** is running. Press CTRL+ALT+DEL to display the Task Manager window. If **radsvc.exe** is displayed in the window, it is running.

- The RADIUS server is not defined correctly on the PortMaster.

Check the RADIUS server information using the following commands:

```
Command> show global
Command> show netcon
```

Look for remote ports of 1645 or 1646 in the **netcon** output.

- No entry exists for the PortMaster in the **/etc/raddb/clients** file. Verify this condition by doing the following:

Choose **Clients...** from the Edit menu on the RADIUS Control Panel. Ensure that the PortMaster hostname or IP address is defined correctly in the **/etc/raddb/clients** file.

- RADIUS responses are not getting back to the PortMaster. Do the following:
 - Examine the routing table on the RADIUS server host.
 - Ping the PortMaster from this host.
 - Run **tracert** on the PortMaster address from this host.
 - Run **tracert** on the host from the PortMaster.

- The PortMaster is ignoring RADIUS responses. This results when the access-accept or access-reject source address does not match the destination of the access-request packet—the IP address of either the primary or secondary RADIUS server. This is usually caused by one of the following:
 - Multiple IP addresses are assigned to a single Ethernet interface on the RADIUS server host.
 - Multiple Ethernet interfaces are enabled, and the RADIUS server is replying to a request from the PortMaster on an interface different from the interface that received the request.

You can use the PortMaster packet tracing command to determine where packets are being routed. See the *PortMaster Troubleshooting Guide* for more information.

Result of Debug Output

If debug output shows more than one access-reject packet sent for the same ID, check the following:



Note – To display debugging output, choose **Logging** from the Options menu on the RADIUS Control Panel. Ensure that the **Enable log file for RADIUS messages** option is selected.

1. **Check the route back to the PortMaster; ensure that replies are getting to the PortMaster.**
2. **Check to see if the RADIUS server host has more than one Ethernet port or multiple IP addresses assigned to the same Ethernet interface.**
3. **Check for packet filters between the RADIUS server host and the PortMaster filtering out the RADIUS return packets.**
4. **On the PortMaster, use ptrace as follows to show packets returning from the host running radiusd.**

For ComOS versions below 3.7:

```
Command> add filter r
Command> set filter r 1 permit udp src eq 1645
Command> set filter r 2 permit icmp
Command> ptrace r
```



Note – ptrace on a PortMaster only shows UDP or ICMP packets generated on the PortMaster itself if the PortMaster is running ComOS version 3.7 or later. Outgoing RADIUS access requests are not shown; however, returning packets are displayed. To turn off tracing, use the **ptrace** command with no values. See the *Command Line Administrator's Guide* for more information.

For ComOS version 3.7 or higher:

```
Command> add filter r
Command> set filter r 1 permit udp src eq 1645
Command> set filter r 2 permit udp dst eq 1645
Command> set filter r 3 permit udp src eq 1646
Command> set filter r 4 permit udp dst eq 1646
Command> set filter r 5 permit icmp
Command> ptrace r ext
```

5. Check the source address of a packet during tracing.

A multihomed RADIUS host might be using the wrong source address when replying to access-request packets.

If debugging output shows an access-reject packet right away, check the following:

1. Check the spelling of the username and password.

The capitalization must match exactly.

2. Check the log file, C:\Temp\radius.log.

3. Use the show table user command to verify that the user is not in the PortMaster user table.

The local user table is always checked first during authentication attempts.

4. If Auth-Type = System is not working, attempt to use a clear text password in the user profile.

5. If Auth-Type = System is specified on a UNIX system that has shadow passwords, ensure that radiusd is run as root to access the shadow passwords.

6. If Auth-Type = System is specified on a Windows NT system, verify that the username is defined in the User Manager.

7. **Verify the spelling, capitalization, and syntax of the `/etc/raddb/users` file.**

If **radsvc.exe** finds any errors in the user profile, it sends an access-reject message and logs an error to **C:\Temp\radius.log**.

8. **Check that the shared secret in `/etc/raddb/clients` matches the one set on the PortMaster with the `set secret` command**

9. **If you are using PMconsole 3.5 or earlier, ensure that the secret was not inadvertently erased.**

Pressing the **Return** key with the cursor in the RADIUS Secret field of the RADIUS window erases the secret when the **Save** button is clicked.

Troubleshooting RADIUS Accounting

Most RADIUS accounting problems occur because a step was skipped during installation. Carefully check the instructions in Chapter 3, “Adding a RADIUS Client,” and Chapter 8, “Implementing RADIUS Accounting,” to ensure that the accounting server was properly installed and configured.

If you have not solved the problem after reviewing the instructions in Chapter 3 and Chapter 8, do the following:

1. **Verify the RADIUS accounting service directory, `\usr\adm\radacct` exists.**

2. **Verify that the account used to execute the RADIUS for Windows NT service has write permission to the RADIUS accounting service directory.**

3. **Check the RADIUS version number.**

Choose **About RADIUS** from the Help menu on the RADIUS Control Panel.

4. **Make sure that you do not have any other process bound to UDP ports 1645 or 1646.**

Stop RADIUS by closing the RADIUS Control Panel or by selecting **File⇒Exit** from the menu bar. Restart RADIUS by clicking the Windows NT **Start** button, then selecting **Programs⇒Lucent RADIUS 2.0.1⇒Lucent RADIUS NT**.

5. **Use the `show global` command to verify that the IP address of the accounting host has been configured on the PortMaster.**

If it has not been configured, set it using the **set accounting *Ipaddress*** command on the PortMaster, where *Ipaddress* is the IP address of the host running **radiusd**.

- 6. Check syslog (auth.warning) for error messages from radiusd.**

During normal use, very few error messages should appear.

- 7. Ping the PortMaster from the RADIUS server to check connectivity.**
- 8. If the previous suggestions do not solve the problem, run `radiusd -x` on the RADIUS server host and check to determine if accounting records are displayed.**

Table B-1 compares RADIUS actions on UNIX platforms versus Windows NT. It is helpful if you are familiar with RADIUS for UNIX. You issue the **radiusd** command with options to perform different actions in RADIUS for UNIX. In RADIUS for Windows NT, you usually perform the same actions through the GUI.

Table B-1 RADIUS Actions—UNIX versus Windows NT

RADIUS Action	UNIX Command	Windows NT Procedure
To specify an alternate directory for RADIUS accounting.	radiusd -a The default directory is /usr/adm/radacct .	From the Setup Options menu, select Directories... ; then enter the desired Accounting Directory path. The default directory is C:\usr\adm\radacct .
To use the .dbm version of the users file. See “Configuring Database Caching of User Profiles” on page 4-42 for more information.	radiusd -b	From the Setup Options menu, select Users Cache... ; then click Enable users cache for authentication .
To specify an alternate directory for RADIUS configuration files.	radius -d The default directory is /etc/raddb .	From the Setup Options menu, select Directories... ; then enter the desired path. The default directory is C:\winnt\system32\drivers\etc\raddb .
To specify a RADIUS logfile to use instead of syslog.	radiusd -l	From the Setup Options menu, select Logging... ; then enter the desired file path. The default log file is C:\Temp\radius.log .

Table B-1 RADIUS Actions—UNIX versus Windows NT (Continued)

RADIUS Action	UNIX Command	Windows NT Procedure
To specify the UDP ports used by the RADIUS authentication and accounting servers.	radiusd -p If you specify radiusd -p 6000 , the authentication server uses port 6000 and the accounting server uses port 6001. The default UDP ports are 1645 for authentication and 1646 for accounting.	Use a text editor to modify the C:\winnt\system32\drivers\etc\services . The RADIUS installer specifies UDP port 1645 for authentication and 1646 for accounting. Change these to the desired values.
To run RADIUS in single-threaded mode without spawning a child process to handle each authentication request.	radiusd -s	From the Setup Options menu, select Multitask Authentication... ; then click Enable simultaneous authentication request handling to deselect it.
To display the version of RADIUS without starting the radiusd daemon.	radiusd -v	From the Help menu, select About RADIUS .
To enable debug mode.	radiusd -x To send debug output to syslog, use -x -l syslog .	From the Setup Options menu, select Logging.... The default log file is C:\Temp\radius.log .

Index

Symbols

/etc/raddb/users, checking A-3

A

access-reject packet

 immediate reject A-7

 multiple packets A-6

 result of debug output A-6

accounting

 attributes 8-3, 8-10

 changing directory location 8-7

 changing the default directory 8-7

 configuring database logging 8-5

 configuring detail file logging 8-6

 configuring on Windows NT 2-20

 configuring server 8-4

 example records 8-15

 logged information 8-10

 overview 8-1

 primary and secondary server 2-2, 3-4

 server configuration 8-4

 server requirements 8-3

 server version 8-6

 specifying a new ODBC data source 8-7

 Start and Stop records 8-10

Acct-Authentic 8-10

Acct-Delay-Time 8-10

Acct-Input-Octets 8-10

Acct-Output-Octets 8-10

Acct-Session-Id 8-10

Acct-Session-Time 8-11

Acct-Status-Type 8-11

Acct-Terminate-Cause 8-11

Acct-timestamp 8-13

ACE/Client installation on Windows NT 7-11

ACE/Server

 adding a user on Windows NT 7-9

 importing tokens to the database 7-9

 installation on a Windows NT host 7-3

 installing other features 7-14

 port numbers 7-5

 requirements for Windows NT 7-4

 service names 7-5

 starting 7-12

additional references xi

Administrative-User value for Service-Type reply
 item 4-17, 4-18

Admin-Reboot session termination 8-11

Admin-Reset session termination 8-11

archiving the RADIUS databases 5-4

attributes, accounting

 Acct-Authentic 8-10

 Acct-Delay-Time 8-10

 Acct-Input-Octets 8-10

 Acct-Output-Octets 8-10

 Acct-Session-Id 8-10

 Acct-Session-Time 8-11

 Acct-Status-Type 8-11

 Acct-Terminate-Cause 8-11

 Acct-timestamp 8-13

 Called-Station-Id 8-13

 Calling-Station-Id 8-13

 Datestamp 8-13

 NAS-Port-Type 8-14

 overview 8-10

 Request-Authenticator 8-14

- authentication
 - configuring multitask authentication 2-15
 - overview 1-2
 - primary server 2-1, 3-4
 - restricting to a group of users 4-15
 - secondary server 2-2, 3-4
 - specifying type 4-8
 - test utility 5-1
 - troubleshooting A-1
- authorization, overview 1-4
- Auth-Type check item
 - Local value 4-8
 - Reject value 4-9
 - SecurID value 4-9
 - System value 4-8

B

- Broadcast-Listen value for Framed-Routing reply item 4-26
- Broadcast value for Framed-Routing reply item 4-26

C

- Callback-Framed-User value for Service-Type reply item 4-17, 4-19
- Callback-Id reply item 4-22
- Callback-Login-User value for Service-Type reply item 4-17, 4-19
- Callback-Number reply item 4-22
- Callback session termination 8-11
- Called-Station-Id
 - accounting attribute 8-13
 - check item 4-13
- Calling-Station-Id
 - accounting attribute 8-13
 - check item 4-13
- caution icon xiv
- check items
 - Auth-Type 4-8

- Called-Station-Id 4-13
- Calling-Station-Id 4-13
- Connect-Rate 4-14
- Crypt-Password 4-10
- definition 4-3
- Expiration 4-9
- Framed-Protocol 4-15
- Group 4-15
- NAS-IP-Address 4-14
- NAS-Port 4-14
- NAS-Port-Type 4-14
- overview 4-7
- Password 4-7
- Prefix 4-11
- Service-Type 4-16
- Suffix 4-11

- clients
 - configuring PortMaster 3-1
 - configuring with command line 3-3
 - configuring with PMconsole 3-5
 - configuring with PMVision 3-5
 - NAS-IP-Address 4-14
 - NAS-Port 4-14
 - NAS-Port-Type 4-14
- clients file
 - description 1-6
 - editing 3-3
- compression, TCP/IP 4-23
- configuring
 - accounting on Windows NT 2-20
 - caching on Windows NT hosts 4-42
 - multitask authentication 2-15
 - overview of RADIUS 1-7
 - RADIUS client using command line 3-3
 - RADIUS client using PMconsole 3-5
 - RADIUS client using PMVision 3-5
 - RADIUS menus 6-1
 - RADIUS options on Windows NT 2-10
 - user information 4-1
 - users cache 2-13
- connection rate, maximum 4-14
- Connect-Rate check item 4-14

contact information
 Europe, Middle East, and Africa xv
 Lucent Remote Access technical support xv
 North America, Latin America, and Asia
 Pacific xv
 technical support xiv
 users mailing lists xvi
conventions in this guide xiii
Crypt-Password check item 4-10

D

database
 administration and importing tokens 7-9
 associating with ODBC driver 2-26
 tables, copying 5-4
data source
 creating 2-23, 8-7
 file 2-21, 8-8
 machine 2-21, 8-8
 RADACCTDS 2-21
 specifying the ODBC 2-21, 8-7
 table copy utility 5-4
Datestamp 8-13
debug output
 immediate access-reject A-7
 multiple access-reject A-6
DEFAULT
 menu 6-1
 user profile 4-5
default directories, changing 2-16
detail file
 attributes, list of 8-3
 example 8-15
dictionary
 accounting attributes in 8-10
 definition 1-6
 troubleshooting with A-3
 viewing 4-2

directories
 changing the default accounting 8-7
 default on Windows NT 2-16
 structure in RADIUS 1-6
disconnecting users 4-34
document advisory xiv
documentation, related ix
document conventions xiii
Dr. Watson A-2

E

editing user profiles 4-4
encrypting passwords 4-10
event log 4-43
examples
 accounting detail file 8-15
 menus 6-2, 6-3, 6-4
 prefix in DEFAULT user profiles 4-6
 Start and Stop accounting records 8-15
 suffix in DEFAULT user profiles 4-6
 user profile 4-43
EXIT menu choice 6-1
Expiration check item 4-9

F

file data source 2-21, 8-8
Filter-Id reply item 4-26
filters
 access 4-28
 packet 4-27
flags, radiusd B-1
format
 menus 6-1
 user profile 4-2
Framed-Compression reply item 4-23
Framed-IP-Address reply item 4-23
Framed-IP-Netmask reply item 4-24

Framed-IPX-Network reply item 4-29
Framed-MTU reply item 4-33
Framed-Protocol
 check item 4-15
 reply item 4-24
Framed-Route reply item 4-25
Framed-Routing reply item 4-26
 Broadcast-Listen value 4-26
 Broadcast value 4-26
 Listen value 4-26
 None value 4-26
Framed-User value
 Service-Type check item 4-16
 Service-Type reply item 4-17, 4-20

G

Group check item 4-15

H

Host-Request session termination 8-11
host unavailable message A-4

I

Idle-Timeout
 reply item 4-28
 session termination 8-11
in.pmd daemon 4-31
installation
 ACE/Client on Windows NT 7-11
 ACE/Server on a Windows NT host 7-3
 on a Windows NT host 2-3
 other ACE/Server features 7-14
 overview of RADIUS installation and
 configuration 1-7
 SecurID master and slave servers on Windows
 NT 7-7
 SecurID master server on Windows NT 7-6
invalid login message A-5

IPX

 converting decimal to dotted decimal 4-29
 setting network information 4-29

L

Listen value for Framed-Routing reply item 4-26
Local value for Auth-Type check item 4-8
logging RADIUS messages to a file 2-11
login, invalid A-5
Login-IP-Host reply item 4-31
logins, matching user profiles with 4-4
Login-Service reply item 4-30
 PortMaster value 4-31
 Rlogin value 4-30
 TCP-Clear value 4-31
 Telnet value 4-30
Login-TCP-Port reply item 4-32
Login-User value for the Service-Type reply item
 4-17, 4-20
Lost-Carrier session termination 8-12
Lost-Service session termination 8-12

M

machine data source 2-21, 8-8
mailing lists, subscribing to users xvi
master server
 SecurID installation without slave server 7-6
 SecurID installation with slave server 7-7
maximum connection rate 4-14
maximum transmission unit 4-33
menu bar 2-30
Menu reply item 4-32
menus
 DEFAULT 6-1
 format 6-1
 nested 6-3
 reference 6-4

- single-level 6-2
 - subdirectory 1-6
 - termination 6-4
- moving databases 5-4
- MTU, setting 4-33
- multitask authentication, configuring 2-15

N

- NAS-Error session termination 8-12
- NAS information
 - NAS-IP-Address check item 4-14
 - NAS-Port check item 4-14
 - NAS-Port-Type accounting attribute 8-14
 - NAS-Port-Type check item 4-14
 - NAS-Prompt-User value for Service-Type
 - reply item 4-18, 4-21
- NAS-Reboot session termination 8-12
- NAS-Request session termination 8-12
- nested menus 6-3
- None value for Framed-Routing reply item 4-26
- note icon xiv

O

- ODBC driver, associating with database 2-26
- operating systems supported 1-2
- options
 - changing accounting directory location 8-7
 - configuring accounting database logging 8-5
 - configuring accounting detail file logging 8-6
 - configuring accounting server 8-4
 - radiusd B-1
 - specifying a new ODBC data source 8-7
- Outbound-User
 - value for Service-Type check item 4-16
 - value for Service-Type reply item 4-18, 4-21

P

- PASSCODE 7-2
- Password check item 4-7
- passwords
 - encryption 4-10
 - expiration date 4-9
 - location of 4-8
- Perl script 4-29
- PIN
 - assignment for SecurID 7-15
 - system-generated 7-16
 - user-created 7-15
- Port-Error session termination 8-12
- Port-Limit reply item 4-33
- PortMaster
 - checking A-3
 - configuring with command line 3-3
 - configuring with PMconsole 3-5
 - configuring with PMVision 3-5
 - value for Login-Service reply item 4-31
- port numbers
 - ACE/Server 7-5
 - changing from default 2-17
 - RADIUS 1-6
 - specifying for RADIUS B-2
 - specifying TCP for a remote host 4-32
 - specifying TCP for connection 4-22
- Port-Preempted session termination 8-12
- Port-Suspended session termination 8-12
- Port-Unneeded session termination 8-12
- PPP, example DEFAULT user profile for 4-11
- Prefix check item 4-11
 - in DEFAULT user profiles 4-6

R

RADACCTDS data source 2-21

RADIUS

accounting 8-1

actions in UNIX compared with Windows NT
B-1

authentication 1-2

authorization 1-4

checking Windows NT service A-1

client configuration 3-1

configuring for SecurID 7-14

configuring on a Windows NT host 2-10

directory structure 1-6

enhancements for version 2.0.1 1-4

features 1-1

for Windows NT, starting 2-6

functions 1-2

installation 2-6

installation and configuration overview 1-7

installation as a Windows NT nonservice 2-8

installation as a Windows NT service 2-7

logging messages to a file 2-11

primary accounting server 2-2

primary authentication server 2-1

removal as a service 2-10

secondary accounting server 2-2

secondary authentication server 2-2

server requirements 2-1

users file 4-1

utilities 5-1

Windows NT service versus nonservice 2-7

working with SecurID 7-3

radius.mdb file 1-6

radiusd, checking A-1

radiusd flags or options, complete list B-1

references xi

books xiii

RFCs xi

Reject value for Auth-Type check item 4-9

related documentation ix

removal of RADIUS service 2-10

reply items

Callback-Id 4-22

Callback-Number 4-22

definition 4-3

example 4-43

Filter-Id 4-26

Framed-Compression 4-23

Framed-IP-Address 4-23

Framed-IP-Netmask 4-24

Framed-IPX-Network 4-29

Framed-MTU 4-33

Framed-Protocol 4-24

Framed-Route 4-25

Framed-Routing 4-26

Idle-Timeout 4-28

Login-IP-Host 4-31

Login-Service 4-30

Login-TCP-Port 4-32

Menu 4-32

overview 4-16

Port-Limit 4-33

Service-Type 4-16

Session-Timeout 4-34

Termination-Menu 4-34

Request-Authenticator 8-14

request packet timeout 2-19

request queue, setting size of 2-18

RIP configuration 4-26

Rlogin value for Login-Service reply item 4-30

S

secret, shared 2-3, 3-5

SecurID

ACE/Server 7-3

ACE/Server installation on a Windows NT
host 7-3

ACE/Server requirements for a Windows NT
host 7-4

configuring RADIUS for 7-14

- master and slave server installation 7-7
 - master server installation 7-6
 - new users 7-15
 - PIN assignment 7-15
 - port numbers 7-5
 - service names 7-5
 - technical support 7-1
 - testing 7-13
 - troubleshooting 7-18
 - value for Auth-Type check item 4-9
 - working with RADIUS 7-3
 - server, RADIUS
 - accounting requirements 8-3
 - primary accounting 2-2
 - primary authentication 2-1
 - requirements 2-1
 - secondary accounting 2-2
 - secondary authentication 2-2
 - server, SecurID
 - master installation without slave server 7-6
 - master server installation with slave 7-7
 - Service-Type check item
 - Framed-User value 4-16
 - Outbound-User value 4-16
 - Service-Type reply item
 - Administrative-User value 4-17, 4-18
 - Callback-Framed-User value 4-17, 4-19
 - Callback-Login-User value 4-17, 4-19
 - Framed-User value 4-17, 4-20
 - Login-User value 4-17, 4-20
 - NAS-Prompt-User value 4-18, 4-21
 - Outbound-User value 4-18, 4-21
 - Service Unavailable session termination 8-12
 - session termination, reasons for
 - Admin-Reboot 8-11
 - Admin-Reset 8-11
 - Callback 8-11
 - Host-Request 8-11
 - Idle-Timeout 8-11
 - Lost-Carrier 8-12
 - Lost-Service 8-12
 - NAS-Error 8-12
 - NAS-Reboot 8-12
 - NAS-Request 8-12
 - Port-Error 8-12
 - Port-Preempted 8-12
 - Port-Suspended 8-12
 - Port-Unneeded 8-12
 - Service Unavailable 8-12
 - Session-Timeout 8-13
 - User-Error 8-13
 - User-Request 8-13
 - Session-Timeout
 - reply item 4-34
 - session termination 8-13
 - shared secret 2-3, 3-5
 - single-level menus 6-2
 - slave server, SecurID installation 7-7
 - SLIP, example DEFAULT user profile for 4-11
 - starting
 - ACE/Server 7-12
 - RADIUS for Windows NT 2-6
 - Suffix check item
 - in DEFAULT user profile 4-6
 - overview 4-11
 - support, technical xiv, xv
 - Security Dynamics 7-1
 - synchronization, token 7-11
 - System Diagnostics utility 5-9
 - system-generated PIN 7-16
 - System value for Auth-Type check item 4-8
- ## T
- TCP/IP header compression 4-23
 - TCP-Clear value for the Login-Service reply item 4-31
 - technical support xiv
 - Lucent Remote Access xv
 - Security Dynamics 7-1

- Telnet
 - example DEFAULT user profile for 4-11
 - value for Login-Service reply item 4-30
- termination causes. See session termination, reasons for
- Termination-Menu reply item 4-34
- Termination menus 6-4
- testing RADIUS authentication 5-1
- testing SecurID 7-13
- text files
 - clients 3-1
 - menu 6-1
 - users 4-1
- timeout
 - request packet 2-19
- token
 - definition 7-2
 - synchronizing 7-11
- tokencode
 - definition 7-2
 - invalid 7-17
- token records, importing ACE/Server 7-9
- troubleshooting
 - authentication A-1
 - SecurID 7-18
 - with the dictionary file A-3

U

- UNIX command equivalents to Windows options B-1
- user-created PIN 7-15
- User-Error session termination 8-13
- User Manager utility 5-9
- username
 - definition 4-3
 - prefix and suffix to 4-11
- user profile
 - components 4-2

- DEFAULT 4-5
- editing 4-4
- example 4-43
- format 4-2
- overview 4-1
- user profiles
 - matching logins with 4-4
- User-Request session termination 8-13
- users
 - cache, configuring the 2-13
 - disconnecting 4-28, 4-34
 - groups of 4-15
- users file 1-6, 4-1
 - checking A-3
- utility
 - data source table copy 5-4
 - System Diagnostics 5-9
 - to test RADIUS authentication 5-1
 - User Manager 5-9
 - using RADIUS for NT 5-1

V

- version
 - determining for accounting server 8-6

W

- warning icon xiv
- Windows NT configuration options B-1