



# ***RadiusNT & RadiusX***

**The Ultimate RADIUS Servers**  
For Windows NT, Linux, Solaris & Cobalt Appliances  
**Version 4.0**

**IEA Software, Inc.**

Administrative and Support Office  
516 W. Riverside, Suite 201  
Spokane, Washington 99201  
Phone: (509) 444-BILL

[Sales@iea-software.com](mailto:Sales@iea-software.com)  
[Support@iea-software.com](mailto:Support@iea-software.com)



## Software License Agreement

By purchasing or installing RadiusNT or RadiusX, you indicate your acceptance of the following License Agreement.

**Ownership of Software** You acknowledge and agree that the computer program(s) and associated documentation contained with RadiusNT or RadiusX (collectively, the Software) are owned exclusively by IEA Software, Inc. and/or its licensors. The Software contained in the package is protected under copyright laws and all copyright and other intellectual property rights relating to the Software are and remain the exclusive property of IEA Software, Inc. and/or its licensors. You may not rent or lease the Software, but you may transfer the Software and accompanying materials on a permanent basis provided you retain no copies and the recipient agrees to the terms of this Agreement.

**License** IEA Software, Inc. grants to you, and you accept, a limited, non-exclusive and revocable license to use the Software. You agree to use the Software in machine-readable object code form only as authorized in this License Agreement. This License Agreement does not convey any title or interest in the Software to you.

**Scope of License** You may not make any changes or modifications to the Software, and you may not de-compile, disassemble, or otherwise reverse engineer the Software. You may not lend, rent, lease or sublicense the Software or any copy to others for any purpose. RadiusNT or RadiusX may only be installed on a single WindowsNT, Solaris, Linux or Cobalt Networks workstation or server. Additional servers may be purchased separately. You agree to use reasonable efforts to protect the Software from unauthorized use, modifications, reproduction, distribution and publication. You are not permitted to make any uses or copies of the Software that are not specifically authorized by the terms of this License Agreement. Your adherence to this License Agreement will allow IEA Software, Inc. to continue developing innovative and useful products and providing a high level of customer service and support. If you do not comply with the terms of this License Agreement, your license will be revoked.

**Updates and Support** All software updates and fixes are available via the IEA Software, Inc. Web site. Major version upgrades are not included or covered as part of the basic purchase agreement. Technical support is currently available via methods listed on our Web site Support section at <http://www.iea-software.com/support>.

**Restricted Rights** The Software is provided with U.S. Governmental Restricted Rights. Use, duplication, or disclosure by the Government is subject to restrictions set forth in subparagraph ©(1)(ii) of The Rights in Technical Data and Computer Software clause at DFARS 252.227-7013 or subparagraphs ©(1) and (2) of the Commercial Computer Software - Restricted Rights at 48 CFR 52.227-19 as applicable. The Software is also protected by International Treaty Provisions. Manufacturer is IEA Software, Inc. 516 W. Riverside, Suite 201, Spokane, Washington 99201.

**Miscellaneous** This License Agreement shall be construed, interpreted and governed by the laws of the State of Washington. Should any term of this License Agreement be declared void or unenforceable by any

court of competent jurisdiction, enforcement of the remaining terms shall not be affected. Failure of either party to enforce any rights or to take action against the other party in the event of any breach of this Licensing Agreement shall not be deemed a waiver of any subsequent enforcement of rights.

**Limitations of Liability and Remedies** In no event shall IEA Software, Inc. or its licensors be liable for any loss of profit or any other commercial damage, including but not limited to special, incidental, consequential or other damage, even if IEA Software, Inc. or its licensors are advised, in advance, of the possibility of such damages. IEA Software, Inc. and its licensor's entire liability and your exclusive remedy shall be, at IEA Software's option, either (a) return of the price paid, or (b) repair or replacement of the Software. To the maximum extent permitted by applicable law, IEA Software, Inc. and its licensors disclaim all other warranties, either express or implied, including but not limited to, implied warranties with regard to the Software and the accompanying material. This Limited Warranty is void if failure of the Software has resulted from accident, abuse or misapplication. You may have other specific legal rights, which vary from state/jurisdiction to state/jurisdiction.

**Return Policy** It is our goal to provide customers with the highest level of satisfaction possible. In order to ensure that our products work well in your environment, IEA Software offers a 30-day FULL functioning software trial that includes documentation and support. If you require more than 30 days to evaluate the software, we are happy to work with you to extend the trial to a length that fits your timetable. This gives you, the user, an opportunity to ensure that the product fully meets your needs. (Please test the software in a non-production environment.) In light of the trial period and opportunity to fully test our software, IEA Software maintains the policy that no refunds will be offered. We will, however, address any problems with the software.

Should a software anomaly occur, our Development and Support Teams will work to correct the problem. Please note that you must be using the application normally, as defined, and you must ensure that the bug is not due to anomalies in other programs, the operating system, your hardware, or data.

In order to address any problems, please note that the bug must be able to be reproduced. Our Development and Support Teams will require full documentation of the steps taken by the user that caused the error in the software as well as necessary data and scenario files to reproduce the error.

**Contact** Should you have any questions concerning this license agreement, please contact IEA Software, Inc. at 516 W. Riverside, Suite 201, Spokane, Washington 99201 U.S.A. (509) 444-BILL (2455).

Information in this document is subject to change without notice. No part of this document may be reproduced or transmitted in any form or by any means, electronic or mechanical, without the express written consent of IEA Software, Inc.

## **Trademarks**

*Emerald Management Suite*, *RadiusNT* and *RadiusX* are trademarks of IEA Software, Inc. All images, photographs, animations, audio, video and text incorporated into the Software are owned by IEA Software, Inc., unless otherwise noted by Trademark. *Alpha AXP* is a registered trademark of Digital Equipment Corporation. *Intel* is a registered trademark of Intel Corporation. *Transact-SQL* is a registered trademark and *DB-Library* is a trademark of Sybase, Inc. *Cobalt*, *RAQ*, and *Solaris* are trademarks of Sun Microsystems. *Cisco* is a trademark of Cisco Systems. All other trademarks are the property of their respective owners.

© 1995-2001 IEA Software, Inc.  
All Rights Reserved, World Wide



# Table Of Contents

<b>SOFTWARE LICENSE AGREEMENT .....</b>	<b>1</b>
TRADEMARKS .....	2
<b>WELCOME.....</b>	<b>7</b>
<b>PREFACE.....</b>	<b>7</b>
ABOUT RADIUS .....	7
RADIUSNT AND RADIUSX EDITIONS .....	8
<b>CONVENTIONS .....</b>	<b>10</b>
<b>SYSTEM REQUIREMENTS.....</b>	<b>11</b>
RADIUSNT .....	11
RADIUSX.....	11
<b>TECHNICAL SUPPORT.....</b>	<b>12</b>
.....	<b>13</b>
INSTALLING RADIUSNT FOR WINDOWSNT/2000 .....	13
INSTALLING RADIUSX FOR COBALT (RAQ3+) .....	17
INSTALLING RADIUSX FOR SOLARIS & LINUX.....	18
UPGRADING FROM AN EARLIER VERSION OF RADIUSNT OR RADIUSX .....	21
THE RADIUSNT/X ADMINISTRATOR.....	22
CONFIGURATION OPTIONS FOR RADIUSNT/X ADMINISTRATOR .....	23
USERS AND CLIENTS FILES .....	39
.....	<b>46</b>
RADIUSNT/X USER AND CONFIGURATION MODE OPTIONS .....	46
TEXT MODE .....	46
ODBC MODE.....	48
BOTH MODE.....	51
.....	<b>52</b>
LIVINGSTON PORTMASTERS .....	52
ASCEND MAX AND PIPELINE.....	52
OTHER RADIUS COMPATIBLE NAS .....	53
.....	<b>54</b>
RADLOGIN.....	54
TROUBLESHOOTING .....	55
.....	<b>56</b>
INSTALLING RADIUSNT AS A SERVICE .....	56
REMOVING THE SERVICE.....	56
SERVICE CONSIDERATIONS.....	56

	<b>58</b>
UNIX PASSWD FILE.....	58
WINDOWS NT SAM SUPPORT.....	58
	<b>60</b>
COMMAND LINE AND REGISTRY/INI LISTINGS.....	60
	<b>69</b>
TABLE LAYOUT.....	69
INSIDE THE DATABASE.....	81
SUPPORTED DATABASE SYSTEMS.....	83
	<b>87</b>
CONCURRENCY CONTROL.....	87
TIME BANKING.....	87
SERVER ACCESS.....	88
DNIS ACCESS.....	88
REJECT LIST.....	88
LOGGING.....	88
SPECIAL USERS.....	90
IP POOLING.....	91
	<b>92</b>
PROXY AND ROAMING.....	92
SIMPLE NETWORK MANAGEMENT PROTOCOL (SNMP).....	94
SNMP CONCURRENCY CHECKING.....	97
SERVER TYPES.....	99
SMART CACHE.....	100
SYSLOG SUPPORT.....	101
LDAP AUTHENTICATION.....	101
	<b>103</b>
ACE SERVER.....	103
DEFENDER.....	103
SAFEWORD.....	103
TACACS+.....	103
EXTERNAL AUTHENTICATION API.....	103
EXTERNAL ATTRIBUTE-VALUE MAPPING.....	106
STORE & FORWARD PROXY.....	106
	<b>108</b>
INSTALLATION AND SETUP PROBLEMS.....	108
STARTUP PROBLEMS.....	108
OPERATION PROBLEMS.....	109
	<b>110</b>
GENERAL.....	110
TEXT MODE.....	112
ODBC MODE.....	112
VENDOR SUPPORT.....	113

	.....	<b>116</b>
RFC 2138	RADIUS .....	148
RFC 2139	RADIUS ACCOUNTING .....	149
	.....	<b>151</b>
UPDATE SCRIPT FOR EMERALD USERS.....		151
CONFIGURING ODBC.....		151
TABLES .....		152
STORED PROCEDURES .....		154
EMERALD INTEGRATION FAQs.....		158
	.....	<b>160</b>

## Welcome

IEA Software would like to thank you for selecting our RadiusNT or RadiusX product. These remote access authentication solutions support all RADIUS authentication and accounting features plus many more options. Our RADIUS server implementation lets you consolidate the authentication of all your remote users, as well as trace their remote access activity.

## Preface

The term RADIUS is an acronym for Remote Authentication Dial-in User Services. The RADIUS protocol is based on an Internet Standards Request For Comments (RFC) for Authentication and an Informational RFC for Accounting. IEA Software offers both RadiusNT and RadiusX, RADIUS based security servers that are used to handle user authentication and accounting from RADIUS supported Network Access Server(s) (NAS) or terminal servers.

This document is not intended to delve into the technical aspects of RADIUS. You will find that technical reference materials exist in a variety of places. For RFC information, please check out the World Wide Web. A good starting point is the Internet Engineering Task Force (IETF) Web site at <http://www.ietf.org>. Specific technical RADIUS documentation for your implementation is available from the RADIUS 'client' (or NAS) you are using with the RADIUS 'server' (RadiusNT/X). It is important to read through your client information before attempting to install RadiusNT/X, especially if you are unfamiliar with the RADIUS protocol.

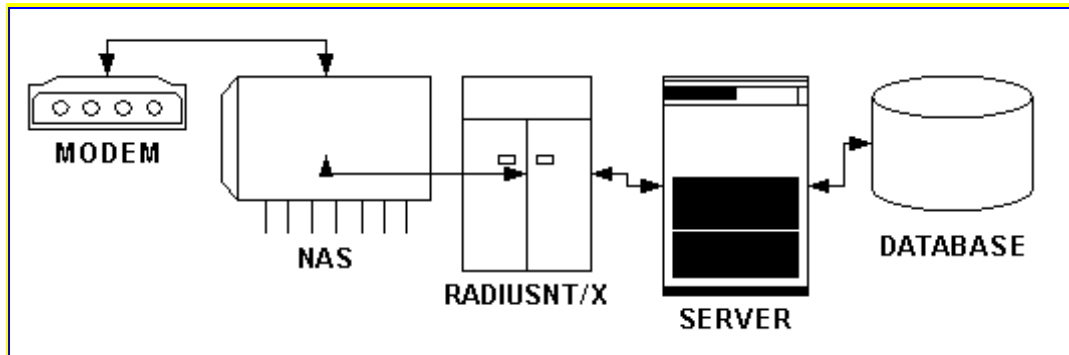
We offer a RADIUS server for the **Windows NT** platform (RadiusNT) and RADIUS servers for the UNIX **Linux**, **Solaris** and **Cobalt Networks RaQ and Qube** platforms (RadiusX). You will find that the most current RadiusNT/X files are available from our Download Center at <http://www.iea-software.com/download>. In addition, please watch our Web site at <http://www.iea-software.com> for update and release information, a searchable RadiusNT/X mailing list archive and more.

## About RADIUS

In our society, it is becoming increasingly common for users to dial into a public or private network to access information and to easily communicate with one another. Managing these sometimes widespread serial line and modem pools for large numbers of users can often create the need for a significant amount of administrative support. In addition, since many networks are linked to other networks around the world, there is an essential need for authentication, authorization and accounting (AAA). This can be best accomplished by administering a single database of users that will allow for authentication (the verification of a user's name and password) as well as detailed configuration information regarding the type of service to deliver to the user (for example: Point-to-Point Protocol (PPP), Telnet or ISDN). The RADIUS protocol was designed to solve the problem of centralized authentication and accounting from multiple, possibly heterogeneous, NASs.

The basic RADIUS design allows for a client such as a NAS or firewall to contact the RadiusNT/X server and send a message requesting authentication of a user who has requested access to a network. In response, RadiusNT/X searches its *clients* file for an entry that matches the request. If a match is found, RadiusNT/X searches the *users* file for a profile that matches the criteria (commonly a username and password). The server processes the request and replies to the client. The reply can either be an acknowledgment (ACK) or no acknowledgment (NACK). In either case, the RADIUS server can include a set of attributes, or qualifications, for the request. This may include user service information, messages or a myriad of other attributes of the calls or accounting information.





Most RADIUS clients can be configured to use an alternate RADIUS server in the event that the primary RADIUS server does not respond. This backup allows for fail-safe operations in larger networks, or the functionality may be used to create a group of RADIUS servers for a distributed implementation.

RadiusNT/X has very similar characteristics to most UNIX RADIUS servers, including basic authentication and accounting capabilities. RadiusNT/X stands out among RADIUS servers by providing a multitude of powerful features and enhanced options. The most striking feature of RadiusNT/X is the extensive Relational Database Management System (RDBMS) interface that is available via Open Database Connectivity (ODBC). By virtue of the power of the database, adding fields, tables and rules at any time can refine RadiusNT/X. For example, instead of RADIUS authentication based on a simple username and password, RadiusNT/X has the ability to authenticate based on username, password, time on-line, port access, or additional rules as configured by the RadiusNT/X Administrators.

### ***RadiusNT and RadiusX Editions***

There are two RadiusNT and RadiusX stand-alone editions: Professional and Enterprise. The RadiusNT/X application is also available as a bundled component of the [Emerald Management Suite](#), version 2.5 and above. The RadiusNT/X edition bundled with the Emerald Management Suite is dependent on the Emerald edition purchased.

The RadiusNT/X Professional edition includes advanced RADIUS server features such as Smart Cache and proxy (see below). The RadiusNT/X Enterprise edition includes all Professional edition features, plus it additionally supports Token cards, LDAP, and Tacacs+. The Enterprise edition also provides web-based access to RadiusNT/X user account management and configuration. Functional differences between the RadiusNT/X editions are noted throughout the documentation. The following charts describe the options that are available in the Professional and Enterprise editions. For more detailed information on each option, please see the [Features](#) chapter.

### **Professional and Enterprise Editions**

<b>Option</b>	<b>Description</b>
<b>RADIUS Proxy and Roaming</b>	To forward RADIUS client requests to other RADIUS servers
<b>SNMP Support</b>	Query real-time authentication and accounting request statistics
<b>Unlimited Smart Cache</b>	Unlimited number of smart cache entries for scaling
<b>Store and Forward Proxy</b>	Higher performance and reliability for large chains of proxy servers.

### **Enterprise Edition Only**

<b>Option</b>	<b>Description</b>
<b>Token Cards</b>	Support for SecurID, Safeword, Axent Defender token cards.
<b>LDAP Authentication</b>	Authenticate and configure a session from any LDAP-enabled directory system.
<b>Tacacs+</b>	RADIUS acts as a client for a Tacacs authentication server.
<b>Advanced State Management</b>	Store and recover authentication and accounting information
<b>Authentication API</b>	Allows authentication from custom databases

Note: Some advanced options listed are only available in ODBC mode. Other options may be restricted by limitations of the database system RadiusNT/X is using in ODBC mode.

You will find that the Windows NT (RadiusNT) and UNIX versions (RadiusX) are very similar. The main differences are:

- ?? RadiusX uses AgentX for Simple Network Management Protocol (SNMP) statistics, whereas RadiusNT uses the WindowsNT SNMP Service
- ?? RadiusX uses .INI configuration files versus using the Windows NT registry
- ?? RadiusX has a different installation process
- ?? RadiusX uses system password functions in place of a password file.
- ?? RadiusX does not support NT Authentication
- ?? RadiusX datasources are defined in the *odbc.ini* file versus the Windows ODBC Administrator

## Conventions

This User Guide has standard document and keyboard conventions to help you locate, interpret and identify information. They are provided to show consistent visual clues and a standard key combination format to assist you while learning and using RadiusNT/X.

Format	Representation
<b>Bold</b>	Menu option to be selected, icon or button to be clicked. Also used to identify key terms or to emphasize a word, term or concept
<b>RadiusNT/X</b>	Applies to both the Windows NT & UNIX versions of Radius
<b>RadiusNT</b>	Applies to the Windows NT version of Radius
<b>RadiusX</b>	Applies to the UNIX version of Radius
<b>Italic</b>	Directory or filename. Also used to emphasize a word, term or concept
<b>"quoted text"</b>	This is text that you need to type. Do not include the quotation marks in your entry, just the text within the quotation marks

## System Requirements

### ***RadiusNT***

RadiusNT runs on any Windows NT 4.0 or Windows 2000 workstation or server. It is administered from Windows NT, either remotely or locally. The system requirements on Windows systems are:

- ?? Windows NT 4.0 or Windows 2000
- ?? NT4 Service Pack 5 or higher
- ?? 128MB of RAM or greater
- ?? 30MB Disk space
- ?? Pentium 200 or greater
- ?? Web browser (Netscape 4.7+ or IE 5.0+)

RadiusNT runs with the relational databases listed below. You need to have a working knowledge of your database. Please use the following guidelines:

- ?? Microsoft SQL Server 7.0 or SQL Server 2000
- ?? Sybase SQL Server 11.9.2
- ?? Oracle Server 8.0
- ?? Microsoft Access 7.0

Service Packs for the Windows NT operating system can be obtained from Microsoft Corporation. For links to Microsoft's Drivers, Patches and Sample Files location on the World Wide Web, please see Microsoft's Web site at <http://www.microsoft.com/>.

### ***RadiusX***

RadiusX is built individually for Solaris and Linux installations. The system requirements for RadiusX are:

- ?? Solaris 2.6 or higher, RedHat Linux 6.2 or higher
- ?? 128MB of Ram or greater
- ?? 30MB Disk space
- ?? Perl 5.0 or higher (for installation purposes only)
- ?? Web browser (Netscape 4.7+ or IE 5.0+)

RadiusX for Cobalt runs on the RaQ3 and RaQ4 platforms (please contact [support@iea-software.com](mailto:support@iea-software.com) if you have questions regarding the current level of support for the Qube and XTR platforms). RadiusX is administered either remotely or locally. The system requirements for RadiusX for Cobalt are:

- ?? 128MB of RAM or greater
- ?? 30MB of disk space
- ?? Perl 5.0 or greater (for installation purposes only)

RadiusX can authenticate against a password file, users file, or an ODBC database. The supported relational databases for RadiusX are:

- ?? Microsoft SQL Server 7.0 or SQL Server 2000
- ?? Sybase SQL Server 11.9.2
- ?? Oracle Server 8.0

## Technical Support

Should you experience any trouble installing or using RadiusNT/X, please consider the following technical support options:

- ?? Please read the *readme.txt* file that is included within your distribution archive. This file contains up-to-date information on the software, noting any changes, feature enhancements or known problems.
- ?? This RadiusNT/X Administrator's manual contains much of the information that you will need to solve problems. Please read the pertinent section to ensure that something wasn't overlooked.
- ?? Please check out our Web site at <http://www.iea-software.com> for announcements, troubleshooting tips, Frequently Asked Questions (FAQ) and more.
- ?? IEA Software hosts mailing lists for RadiusNT/X. These are user-supported lists and are a great resource for conversing with others who own the products. You can learn more about the mailing lists at <http://www.iea-software.com/support/maillists/liststart>. We host a searchable archive of the lists on our Web site as well.
- ?? If you still require assistance, we have a variety of support contract options available via our Web site at <http://www.iea-software.com/support>.

## Chapter 1 – INSTALLATION

This chapter contains information on how to install and configure your RadiusNT and RadiusX servers. The instructions include information on configuration options that will differ depending on your organization's needs. It is strongly recommended that you read the *readme.txt* file included with your distribution for late-breaking and additional information before proceeding with your installation.

In addition, please read the licensing agreement when it is displayed during the installation process or near the beginning of this document. It is required that you agree with the terms of the agreement before proceeding.

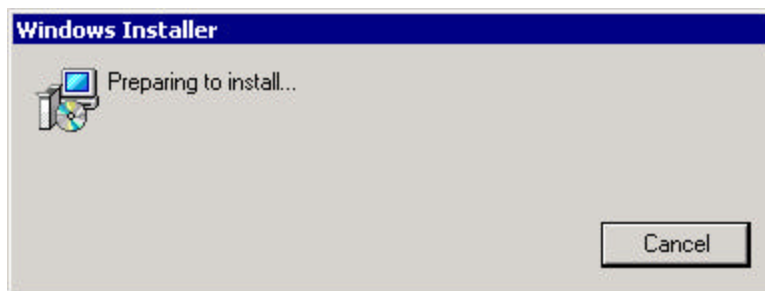
The installation of RadiusNT/X involves three main steps: the installation of the application, the creation and/or upgrade of the Radius database, and the configuration of the server. The following sections describe these installation steps by platform.

### *Installing RadiusNT for WindowsNT/2000*

Please follow the steps below to install RadiusNT on your system. Note: The logged in user must have Administrative privileges to perform the installation. It is recommended that you log into your system as the "Administrator" user.

1. Download the distribution archive for RadiusNT from the IEA Software Web site at <http://www.iea-software.com/download>, or insert the software distribution cd-rom.
2. Review and verify the RadiusNT system requirements listed earlier in this section.
3. Choose the **Run** option from the Windows **Start** Menu.
4. **Browse** to locate the *RadiusNT4.exe* file and then click **OK** to begin the installation process.

Please note that if some of your system files are out of date, the RadiusNT installation will update the files and require you to restart Windows NT in order to proceed.

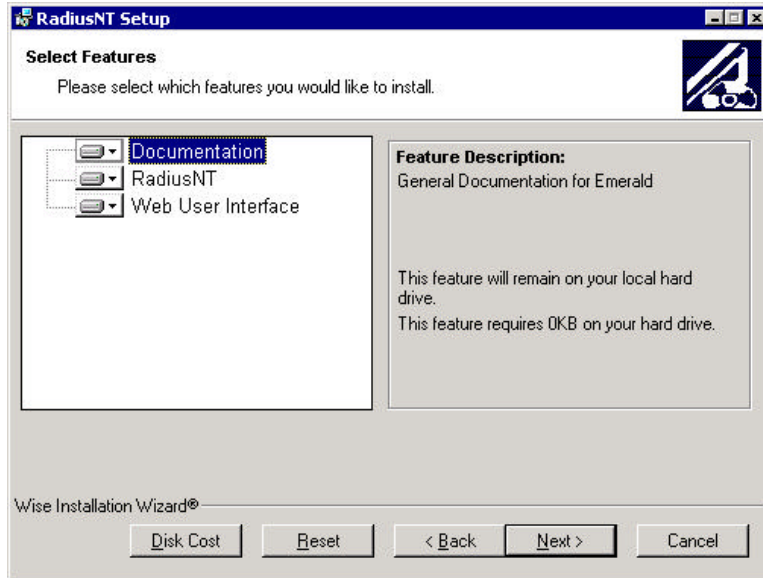


7. You will see the Welcome screen. Click **OK** to proceed.

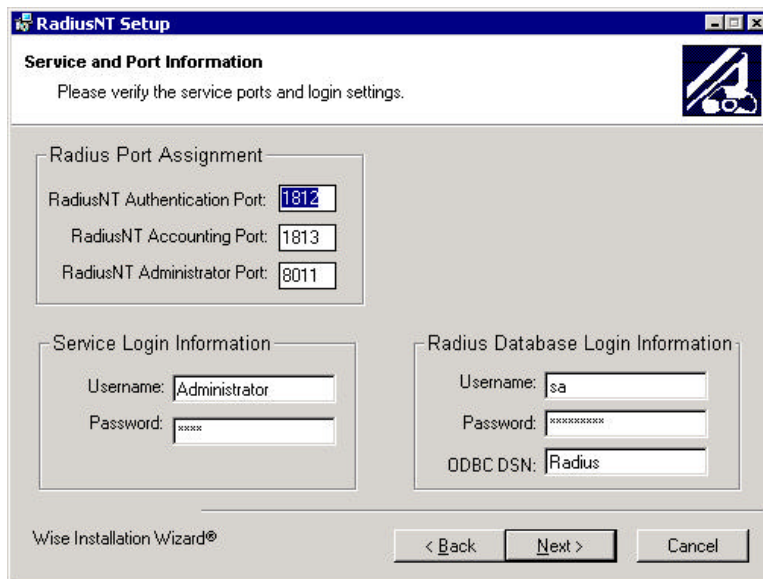
8. Next, you will see the User License Agreement. Before you proceed, make sure that you have read and agree with the terms of the license agreement. Click **I Accept the License Agreement** to continue.

- The Installation Wizard will assist you with installing RadiusNT into the **c:\radius** directory. We recommend using this directory for all first time installations of RadiusNT. Instances where you may choose another directory include when you have another Radius server installed in c:\radius, the c: drive being out of space, etc. Confirm your directory selection and click the **Installation** button to continue.

Select the features you want to install. Note: the Web User Interface is available on RadiusNT/X Enterprise Edition installations.

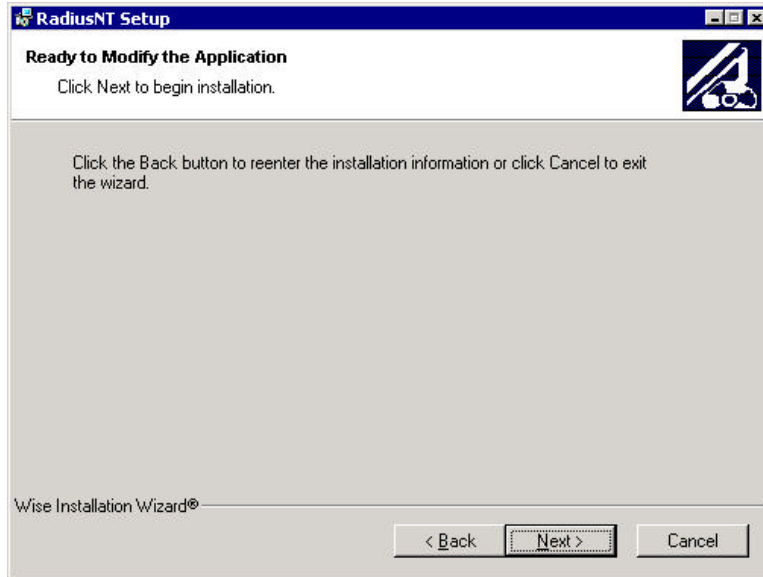


- Next, the Installer will ask to configure some initial options for you: port numbers, the NT Account RadiusNT should run as, and database connectivity. After RadiusNT is installed, these options can be changed using the Configuration Web Interface.





11. When the installation has completed, you will receive a final confirmation screen. Click **Next** to confirm the settings and finish.



12. If you would like to configure RadiusX to run in database mode, you will need to continue with the database installation steps, numbers 13 through 15 below.
13. Create a new (empty) Radius database on your database server.
14. Create the necessary RadiusX database structure by running the appropriate database installation script located in the `/usr/local/radius` directory, according to your selected database platform. Or, if you have an existing RadiusNT or Emerald database, locate it. Below is a list of the database installation scripts and their descriptions:

*emer25\_up.sql* – This script upgrades an existing Microsoft SQL Server Emerald 2.5 database to be compatible with Radius v4.

*radius4\_mssql.sql* - This script is used for a new RadiusX installation using Microsoft SQL Server 7.0+.

*radius4\_sybase.sql* - This script is used for a new RadiusX installation using Sybase Adaptive Server v11.9+.

*radius4\_oracle.sql* - This script is used for a new RadiusX installation using Oracle version 8.

Note: Please refer to your database documentation to learn how to run the SQL script file. For MS SQL, you can use the Enterprise Manager for Sybase you can use the SQL Server Manager or ISQL on either platform. For Oracle use SQLPlus to load the script.

15. To complete the database setup, an ODBC datasource will need to be created and the RadiusX server will need to be configured for ODBC mode. These steps are completed within the RadiusX Administrator (using the **ODBC Setup** and **Authentication** options) and are described in detail within the RadiusNT/X Administrator section of this document.

Once installation is complete, you must configure your RadiusNT server for your operating environment. Configuration is performed via the [RadiusNT Administrator](#). Please refer to the RadiusNT/X Administrator section of this document for information on configuring your RadiusNT server. Please note that for the product to function, you will need to enter your license information within the RadiusNT Administrator, or the RadiusNT/X User Manager, if you have the RadiusNT Enterprise edition.

Additional RadiusNT for Windows General information:

The RadiusNT Administrator is accessed by entering `http://computername:8011/`. Use the login: "Administrator" and password: "password" to initially log in when prompted. It is strongly recommended that you change the default access password immediately for security reasons. RadiusNT configuration via the RadiusNT Administrator is described in detail in the RadiusNT/X Administrator section of this document.

Once the application has been installed, the database created (if running in ODBC mode), and the RadiusNT application configured, start the RadiusNT server by choosing the **RadiusNT Debug Mode** option under the Programs /RadiusNT Start menu option. Alternatively, execute the following command from the command prompt from within the RadiusNT install directory:  
"Radius -x15".

### ***Installing RadiusX for Cobalt (Raq3+)***

Please follow the steps below to install RadiusX for Cobalt on your system. It is strongly recommended that you read the *readme.txt* file that came with your RadiusX distribution prior to beginning installation. This file contains pertinent information to your installation.

1. Download the distribution archive for RadiusX for Cobalt from the IEA Software Web site at <http://www.iea-software.com/download>, or insert the software distribution cd-rom.
2. Review and verify the RadiusX for Cobalt system requirements listed earlier in this section.
3. From the Cobalt server admin interface, select **Maintenance**.
4. Select the **Install Software** option.
5. Upload your RadiusX for Raq3 package (.pkg) file. RadiusX for Cobalt will be installed in the */usr/local/radius* directory.
6. If you would like to configure RadiusX for Cobalt to run in database mode, you will need to continue with the database installation steps, numbers 7 through 9 below.
7. Create a new (empty) Radius database on your database server.
8. Create the necessary RadiusX database structure by running the appropriate database installation script located in the */usr/local/radius* directory, according to your selected database platform. Or, if

you have an existing RadiusNT or Emerald database, locate it. Below is a list of the database installation scripts and their descriptions:

*emer25\_up.sql* – This script upgrades an existing Microsoft SQL Server Emerald 2.5 database to be compatible with Radius v4.

*radius4\_mssql.sql* - This script is used for a new RadiusX installation using Microsoft SQL Server 7.0+.

*radius4\_sybase.sql* - This script is used for a new RadiusX installation using Sybase Adaptive Server v11.9+.

*radius4\_oracle.sql* - This script is used for a new RadiusX installation using Oracle version 8.

Note: Please refer to your database documentation to learn how to run the SQL script file. For MS SQL, you can use the Enterprise Manager for Sybase you can use the SQL Server Manager or ISQL on either platform. For Oracle use SQLPlus to load the script.

9. To complete the database setup, an ODBC datasource will need to be created and the RadiusX server will need to be configured for ODBC mode. These steps are completed within the RadiusX Administrator (using the **ODBC Setup** and **Authentication** options) and are described in detail within the RadiusNT/X Administrator section of this document.

Once installation is complete, you must configure your RadiusX server for your operating environment. Configuration is performed via the [RadiusX Administrator](#). Please refer to the RadiusNT/X Administrator section of this document for information on configuring your RadiusX server. Please note that for the product to function, you will need to enter your license information within the RadiusX Administrator, or the RadiusNT/X User Manager, if you have the RadiusX Enterprise edition.

Additional RadiusX for Cobalt General information:

The RadiusX Administrator for Cobalt is accessed by entering <http://mycobaltserver:8011/>. Use the login: "Administrator" and password: "password" to initially log in when prompted. It is strongly recommended that you change the default access password immediately for security reasons. RadiusX configuration via the RadiusX Administrator is described in detail in the RadiusNT/X Administrator section of this document.

Once the application has been installed, the database created (if running in ODBC mode), and the RadiusX application configured, start the RadiusX server by executing the following command:  
"/usr/local/radius/radiusd -x15"

## ***Installing RadiusX for Solaris & Linux***

Please follow the steps below to install RadiusX on your Solaris or Linux system. It is strongly recommended that you read the *readme.txt* file that came with your RadiusX distribution prior to beginning installation. This file contains pertinent information to your installation. Note: The logged in user must have root/installation privileges to perform the installation. It is recommended that you log into your system as the "root" user.

1. Download the distribution archive for RadiusX from the IEA Software Web site at <http://www.iea-software.com/download>, or insert the software distribution cd-rom.
2. Review and verify the RadiusX system requirements listed earlier in this section.
3. Next, you will need to install Perl5 or higher on your system, if it is not already installed.

Perl is an Open Source interpreted high-level programming language that is often included with your operating system as an installation option. To learn more about Perl, please check out O'Reilly's Web site at <http://www.perl.com>. You can also download a free copy of Perl from O'Reilly's Web site at <http://www.perl.com/pub/language/info/software.html>.

4. Next, un-tar the distribution (***radiusx4\_solaris.tar.gz*** or ***radiusx4\_linux.tar.gz***) into a temporary directory. This can be done by typing the following commands:

```
On Linux:      "tar -xzf ../radiusx4_linux.tar.gz"
On Solaris:    "gzip -d radiusx4_solaris.tar.gz"
               "tar -xf radiusx4_solaris.tar"
```

5. If you would like to configure RadiusX to run in database mode, you will need to continue with the database installation steps, numbers 6 through 8 below. Otherwise, skip to step number 9.
6. Create a new (empty) Radius database on your database server.
7. Create the necessary RadiusX database structure by running the appropriate database installation script located in the `/usr/local/radius` directory, according to your selected database platform. Below is a list of the database installation scripts and their descriptions:

*radius4\_mssql.sql* - This script is used for a new RadiusX installation using Microsoft SQL Server 7.0+.

*radius4\_sybase.sql* - This script is used for a new RadiusX installation using Sybase Adaptive Server v11.9+.

*radius4\_oracle.sql* - This script is used for a new RadiusX installation using Oracle version 8.

Note: Please refer to your database documentation to learn how to run the SQL script file. For MS SQL, you can use the Enterprise Manager for Sybase you can use the SQL Server Manager or ISQL on either platform. For Oracle use SQLPlus to load the script.

8. To complete the database setup, an ODBC datasource will need to be created and the RadiusX server will need to be configured for ODBC mode. These steps are completed within the RadiusX Administrator (using the **ODBC Setup** and **Authentication** options) and are described in detail within the RadiusNT/X Administrator section of this document.
9. Continue with the installation by starting the RadiusX package installer. Use the **"cd"** command to change to the directory where the files were expanded.
10. Run the Install application by typing **"perl install.pl"**. The RadiusX Installer is displayed.

```
Welcome to IEA Software, Inc. UNIX Installer v4.0

Select optional components to install from the list
by selecting the number of the option below.
Press 'C' to continue with the Installation or 'Q' to abort.

1.  [Setup]                Configure Microsoft SQL Server 7.0, 2000
2.  [Do not Setup]        Configure Sybase 11
3.  [Do not Setup]        Configure Oracle 8
4.  [Install]             RadiusX (4.0.3)
5.  [Do not Install]      RadiusX User Interface (4.0.3)

: |
```

You will be presented with three options. Select the component you want from the install list by typing the corresponding number (e.g., 1 for Microsoft SQL Server 7.0, 2000, Sybase 11 and Oracle 8 ODBC drivers). Once you have selected an option, you will note that the indicator changes from "Do not Setup", to "Setup". Please note that, if you make a mistake, you can simply type the corresponding option number again and this will **toggle** the "Setup" or "Do not Setup" option.

11. Type "C" to continue, or "Q" to abort the install process.
12. Next, you will be prompted to enter your database server **network address, port number** (e.g., the port that is used to communicate between RadiusX and the SQL or Sybase server), **database login, database name** and **database password**. You will also need to confirm your password to ensure that it is correct. An example is shown below. Press the **Return** key when you have completed entering the information. You will be returned to the command prompt.

```
Welcome to IEA Software, Inc. UNIX Installer v4.0

The following questions set default values in:
ODBC configuration file (/usr/local/iea/odbc.ini)
IEA configuration file (/usr/local/iea/common.ini)

      SQL Server address (IP Address only for MSSQL):
```

Please note that the default values you set are stored in the ODBC configuration file (*/usr/local/radius/odbc.ini*) and RadiusX configuration file (*/usr/local/radius/radiusd.ini*). These settings can be changed later by using the RadiusNT/X Administrator.

Once Installer program has finished and installation is complete, you must configure your RadiusX server for your operating environment. Configuration is performed via the [RadiusX Administrator](#). Please refer to the RadiusNT/X Administrator section of this document for information on configuring your RadiusX server. Please note that for the product to function, you will need to enter your license information within the RadiusX Administrator, or the RadiusNT/X User Manager, if you have the RadiusX Enterprise edition.

<b>Quick Tip!</b>	If you experience any trouble with the installation process, please refer to the <i>install.log</i> file. This file will display any errors that were encountered during the install, including items such as file permission or disk space errors.
-------------------	---

Additional RadiusX for Linux and Solaris General information:

The RadiusX Administrator is accessed by entering `http://computename:8011/`. Use the login: "Administrator" and password: "password" to initially log in when prompted. It is strongly recommended that you change the default access password immediately for security reasons. RadiusX configuration via the RadiusX Administrator is described in detail in the RadiusNT/X Administrator section of this document.

Once the application has been installed, the database created (if running in ODBC mode), and the RadiusX application configured, start the RadiusX server by executing the following command:  
`"/usr/local/radius/radiusd -x15"`

### ***Upgrading From an Earlier Version of RadiusNT or RadiusX***

Before you upgrade to a newer version of RadiusNT/X, make sure you **back up** all **server**, **clients** and **users** files.

To perform an upgrade installation of either RadiusNT or RadiusX, please follow the installation instructions in [Chapter 1](#). This will replace old files with the updated files that are needed. Please note that there is no need to uninstall the application. If you are a **beta tester**, please note any updated installation information in the `readme.txt` file before proceeding.

The upgrading of your database will depend on your existing installation configuration:

For Microsoft Access, the databases are compatible and no changes need to be made.

For SQL Server & Sybase, running the `radius4_up.sql` script will copy data from an existing 2.5 or 3.0 Radius database to a v4 database created with `radius4_mssql.sql`(Microsoft SQL Server) or `radius4_Sybase.sql`(Sybase) database scripts. See the comments within `radius4_up.sql` for more information on running the conversion script.

For Emerald 2.5 installations of RadiusNT, running the `emer25_up.sql` script will upgrade an existing Microsoft SQL Server Emerald 2.5 database to be compatible with RadiusNT version 4.0.

Please note existing RadiusNT/X 3.0 databases are backwards compatible with Radius v4 making this an optional step. Those upgrading from RadiusNT/X 2.5 must perform a database upgrade.

## The RadiusNT/X Administrator

The Web-based RadiusNT and RadiusX Administrators provide an easy-to-use interface for configuring your RadiusNT/X servers for your authentication, authorization and accounting needs. The RadiusNT/X Administrator is used for the local configuration of each RadiusNT/X server. Please note that the Administrator settings are stored locally for each server. On Windows systems, the settings are stored directly within the Registry. Therefore, the settings supplied and saved are only valid for **that specific server and execution** of RadiusNT or RadiusX.

The RadiusNT/X Administrator requires that the RadiusNT/X Configuration server be started and running prior to it being launched. The Configuration server will be automatically started during the installation process. It can however be manually started and stopped at any time. If it is not started, you can start the Configuration server, by doing the following:

- On Windows systems: Select Programs/RadiusNT/**RadiusNT Admin** from the **Start Menu**
- On UNIX and Linux systems: Enter **"/usr/local/radius/radadmn"** in the command line

The RadiusNT/X Administrator can be launched from any web browser, by accessing the following URL: <http://localhost:8011>. By default, the configuration web server will listen on port 8011. Once started, you will be prompted for a user name and password. Initially use the Username "Administrator" and Password: "password". It is strongly recommended that you change the default access password immediately for security reasons.



The RadiusNT/X Administrator has 12 different main menu options: General, Authentication, Accounting, Advanced, Proxy, Smart caching, Licensing, LDAP, External auth, Tacacs+, Defender and Safeword. To move between each area, click on the corresponding link in the navbar along the top of the Administrator interface. Please remember that you will need to fill out your **license information** on the Licensing tab (or directly within the Licenses table in the database) in order for the Radius server to function. Also, note that the *users* and *clients* files must be edited **outside** of the Administrator with a text editor if you intend to run your RadiusNT/X server in text mode.

# RadiusNT Administrator version 4.0.10

[\[General\]](#) | [ODBC settings](#) | [Authentication](#) | [Accounting](#) | [Advanced](#) | [Proxy](#) | [Smart caching](#) | [Licensing](#) | [LDAP](#) | [External auth](#) | [Tacacs+](#) | [Defender](#) | [Safeword](#) | [Save changes](#) | [Reset changes](#) | [Change password](#)

---

**Welcome**

Welcome, select an item from the list above to get started. When your finished making changes click 'Save Changes'

---

© 1994-2001 IEA Software, Inc. All rights reserved, world wide.

Note: An **alternative** method of configuring RadiusNT is via the command line options, although this is **not** recommended unless you are trying to debug a problem.

**Quick Tip!**

Please remember to save your configuration information and any changes you have made by selecting **File**, then **Save** from the pull-down menus. If you simply exit, the settings will not be saved.

### **Configuration Options for RadiusNT/X Administrator**

The tables below display detailed information about the options available. You will find brief explanations of each option in the RadiusNT/X Administrator here. Please note that some options are explained in finer detail in later sections.

#### **GENERAL Option**

General	
Database mode	Database Only
Debug options	<input checked="" type="checkbox"/> Informational <input checked="" type="checkbox"/> Database queries <input checked="" type="checkbox"/> Authentication <input type="checkbox"/> File messages <input type="checkbox"/> SNMP <input type="checkbox"/> Smart cache <input type="checkbox"/> Memory stats <input type="checkbox"/> Configuration
Allow malformed	<input checked="" type="checkbox"/>
Accounting directory	
Data directory	c:\emerald
Users file	Users



Option	Description
<b>Database Mode</b>	
<b>Text</b>	RadiusNT/X will read the users, clients and dictionary files to retrieve all standard information.  If database mode is enabled as well as text mode, the only text file that will be read is the <i>users</i> file. Accounting information will be stored in the database <b>and</b> in the detail files. All other configurations (dictionary, clients, etc.) will be read from the ODBC database.
<b>Database</b>	RadiusNT/X will try to attach to a database via the ODBC Data Source Name (DSN) specified in the DSN list. If ODBC is enabled, RadiusNT/X will retrieve all standard information (dictionary, clients, users, etc.) from the ODBC database and will <b>not</b> use the text files. Accounting information will be stored in the ODBC database <b>rather</b> than the text files.
<b>Debug Options</b>	
<b>Informational</b>	Show detailed information.
<b>Database queries</b>	ODBC information, including SQL statements.
<b>Authentication</b>	User information during authentication (passwords, etc).
<b>File messages</b>	File Information, including accounting and logging.
<b>SNMP</b>	SNMP Concurrency and query information.
<b>Smart cache</b>	Information on cache related events.
<b>Memory stats</b>	Show object sizes.
<b>Configuration</b>	Show RADIUS configuration at startup.
<b>Allow Malformed</b>	A RADIUS attribute with a length of two or fewer bytes is considered to be a malformed packet. By enabling this option, you will allow RadiusNT/X to accept attributes with a length of two or fewer bytes.
<b>Accounting Directory</b>	The directory to use as the base accounting directory if Text Files mode is selected. A subdirectory will be created for each NAS, with the accounting logfiles for that NAS in the subdirectory. To run RadiusNT as a service, this must be a fully qualified path.
<b>Data Directory</b>	The directory to look in for configuration files (dictionary, users, clients, etc.) if Text Files mode is selected. This must be a fully qualified path for RadiusNT to run as a service. If you are using ODBC mode, this option directs RadiusNT/X where to write the log file.

**Users File**

The filename containing the user information. This should be just the filename, and the file must exist in the specified data directory.

**ODBC SETTINGS Option**

You can edit an existing datasource or create a new one by entering that datasource's name. In the example below, we're creating a new RADIUS datasource:

The screenshot shows a dialog box titled "ODBC settings" with a red header. It has two main sections. The first section, "Edit existing datasource", has a dropdown menu currently showing "(none)". The second section, "Create new datasource", has a text input field containing the word "Radius". A button labeled ">> Continue" is located at the bottom right of the dialog.

Next, select a database type. You will then be presented with different options depending on the type of database you choose. In this example, we're going to choose Microsoft SQL.

The screenshot shows the same "ODBC settings" dialog box. The "Database type" dropdown menu is now open, showing a list of options: "Microsoft SQL 7+", "Microsoft SQL 7+", "Sybase 11", and "Oracle 8". The first "Microsoft SQL 7+" option is highlighted. A button labeled ">> Continue" is visible at the bottom right.

On UNIX platforms the server address for Microsoft and Sybase is the IP Address of the SQL server followed by “;” and then the server’s TCP port number. Note: TCP socket support must be enabled in the SQL server’s protocol setup for RadiusX to communicate with your database.

When using Oracle with RadiusX, or when connecting to any database using RadiusNT ODBC drivers, the server name is based on the underlying client library for that database platform. For example, Microsoft SQL Server addresses are configured based on the ‘Client Network utility’ settings; Sybase uses ‘dsedit’ and Oracle uses the ‘Net8 Configuration’ utility.

ODBC settings	
Datasource description	My RADIUS database
Database name	Radius
Server address (ex 127.0.0.1,1433)	127.0.0.1,5000

>> Continue

After creating a new datasource, you can select it from the Authentication and Accounting menus.

**AUTHENTICATION Option**

Authentication	
Authentication datasource	<div style="border: 1px solid gray; padding: 5px;"><div style="display: flex; align-items: center;"><div style="flex: 1;"><div style="border: 1px solid gray; padding: 2px;">Emerald</div><div style="border: 1px solid gray; height: 100px; margin-top: 2px;"></div></div><div style="margin-left: 10px;"><div style="border: 1px solid gray; padding: 2px; margin-bottom: 5px;">Up</div><div style="border: 1px solid gray; padding: 2px; margin-bottom: 5px;">Down</div><div style="border: 1px solid gray; padding: 2px; margin-bottom: 5px;">Delete</div></div></div><div style="margin-top: 10px;"><div style="display: flex; align-items: center;"><div style="border: 1px solid gray; padding: 2px; flex: 1;">LocalServer</div><div style="border: 1px solid gray; padding: 2px; margin-left: 5px;">Add</div></div></div></div>
Username	<input type="text" value="sa"/>
Password	<input type="password" value="*****"/>
Authentication port	<input type="text"/>
Log file	<input type="text"/>
Ignore case	<input type="checkbox"/>
Trim domain	<input checked="" type="checkbox"/> Authentication <input checked="" type="checkbox"/> Accounting
Pre delimiter	<input type="checkbox"/>
Post delimiter	<input type="checkbox"/>
Bad characters	<input type="text"/>
Users file	<input type="text" value="users"/>

Option	Description
<b>Auth datasource</b>	This specifies the ODBC DSN RadiusNT/X uses to connect to the ODBC database. Multiple DSNs can be specified (space separated) to failover to other database servers if the primary is not available. Other databases are tried in the order they're entered.
<b>Username</b>	Use this to specify the username RadiusNT/X uses to log into the ODBC database.
<b>Password</b>	This option specifies the password for the database user.
<b>Auth Port</b>	This option allows you to specify the port RadiusNT/X will "listen" on for authentication requests.
<b>Log file</b>	The entry shows what log file is used for RADIUS authentication requests (and accounting requests if an accounting logfile is not specified).
<b>Ignore case</b>	By default, RadiusNT/X is case sensitive when authenticating a username and password. If this option is enabled, RadiusNT/X will perform case insensitive comparisons for authentication. Note that CHAP authentication will not work if this option is selected.
<b>Trim domain</b>	When enabled, the Trim Domain option will cause RadiusNT/X to trim the domain prefix or suffix from a username. You can also set whether it will trim the domain for authentication and/or accounting. Both of these settings only apply to local authentication and/or accounting, and do not govern the behavior or style of proxied requests.
<b>Pre delimiter</b>	A list of delimiters denoting everything before the delimiter is the domain. The default for this is the list "%\\".
<b>Post delimiter</b>	A list of delimiters denoting everything after the delimiter is the domain. The default for this is the list "@".
<b>Bad characters</b>	A list of characters that, if found in the authentication name, will cause an immediate reject of the authentication request without further processing.
<b>Users file</b>	The filename containing the user information. This should be just the filename, and the file must exist in the specified data directory.

**ACCOUNTING Option**

Accounting	
Accounting datasource	<div style="border: 1px solid gray; padding: 5px;"><div style="display: flex; align-items: center;"><div style="flex: 1;"><div style="border: 1px solid gray; padding: 2px;">Radius4</div><div style="border: 1px solid gray; height: 100px; margin-top: 2px;"></div></div><div style="margin-left: 10px;"><div style="border: 1px solid gray; padding: 2px; margin-bottom: 5px;">Up</div><div style="border: 1px solid gray; padding: 2px; margin-bottom: 5px;">Down</div><div style="border: 1px solid gray; padding: 2px; margin-bottom: 5px;">Delete</div></div></div><div style="display: flex; align-items: center; margin-top: 5px;"><div style="border: 1px solid gray; padding: 2px; margin-right: 5px;">radius</div><div style="border: 1px solid gray; padding: 2px; margin-right: 5px;">▼</div><div style="border: 1px solid gray; padding: 2px; margin-left: 5px;">Add</div></div></div>
Username	<input type="text"/>
Password	<input type="password" value="*****"/>
Accounting port	<input type="text"/>
Log file	<input type="text"/>
Require secret	<input checked="" type="checkbox"/>
VSA Mapping	<input type="checkbox"/>
Max spooled items	<input type="text"/>
Max batch hold time (secs)	<input type="text"/>
Max items per batch	<input type="text"/>

Option	Description
<b>Accounting datasource</b>	This specifies the ODBC DSN RadiusNT/X uses to connect to the ODBC database. Multiple DSNs can be specified (space separated) to failover to other database servers if the primary is not available. Other databases are tried in the order they're entered.
<b>Username</b>	Use this to specify the username RadiusNT/X uses to log into the ODBC database.
<b>Password</b>	This option specifies the password for the database user.
<b>Accounting port</b>	The Port option allows you to specify the port RadiusNT/X will "listen" on for accounting requests.
<b>Log file</b>	The entry shows what log file is used for RADIUS authentication requests (and accounting requests if an accounting logfile is not specified).
<b>Require secret</b>	This option requires accounting packets to be "signed". This option is rarely needed, and should normally be left unchecked.
<b>VSA Mapping</b>	When this option is enabled, certain vendor specific attributes are mapped to a matching standard attribute and entered into the Calls table.
<b>Max spooled items</b>	<p>If the accounting database is too slow or down, the accounting data can be stored in memory, then moved to the accounting database as conditions improve. Every 25,000 items require about 2MB of memory.</p> <p>New additions will be dropped if Max Spooled Items already exist in memory. RadiusNT/X will not ACK the accounting packet, giving another RADIUS server the opportunity to respond. (Emerald-only edition limited to 500).</p>
<b>Max batch hold time</b>	RadiusNT/X can queue accounting information and then send a batch of multiple requests to the database server as a single query. This reduces overall load on the database at the expense of added latency. This option limits the number of seconds any single piece of accounting data can be queued in a batch. Set this low if you use Time Banking or require concurrent login checking. (Enterprise & Professional version only)
<b>Max items per batch</b>	The maximum number of items that can be sent in a single accounting batch. (See Max Batch time) (Enterprise & Professional version only)

**ADVANCED Option**

Advanced	
Authentication and accounting options	<input type="checkbox"/> (Auth) Concurrency control <input type="checkbox"/> (Auth) Time banking <input checked="" type="checkbox"/> (Auth) Server port access <input type="checkbox"/> (Auth) Ascend max time <input type="checkbox"/> (Auth) Password replace <input type="checkbox"/> (Auth) IP pooling <input type="checkbox"/> (Auth) DNIS Access <input type="checkbox"/> (Auth) Reverse DNIS access <input type="checkbox"/> (Auth) Command triggers <input type="checkbox"/> (Auth) Reject attributes <input checked="" type="checkbox"/> (Acct) Manual calls update <input type="checkbox"/> (Acct) Stop records only <input type="checkbox"/> (Acct) Manual service update <input type="checkbox"/> (Acct) Disable '0' Session-ID port clear <input type="checkbox"/> (Acct) Disable Acct On/Off port clear <input type="checkbox"/> Disable Class ServerID/AccountID tracking
SNMP options	<input type="checkbox"/> Statistics <input type="checkbox"/> Concurrency check <input type="checkbox"/> Server-Ports update
Bind IP-Address ( <i>Leave blank to bind all local addresses</i> )	<input type="text"/>
Database test ( <i>secs</i> )	<input type="text"/>
Database time offset ( <i>days</i> )	<input type="text" value="5"/>



Option	Description
<b>Authentication</b>	
<b>Concurrency Control</b>	RadiusNT/X can prevent users from initiating more than one session at a time if this option is enabled.
<b>Sever Port Access</b>	Enabling this option allows RadiusNT/X to restrict who can connect to a port based on access information. See Advanced Options in <a href="#">Chapter 9</a> for more details.
<b>Password Replace</b>	When using External Password Authentication ('UNIX' and 'WINNT' for the password), RadiusNT/X can replace the database password with the password the user entered, as long as the password was authenticated using the PAP protocol.
<b>DNIS Access</b>	This enables the Dialed Number Identification Service (DNIS) checking option. Please see the ODBC Advanced section in <a href="#">Chapter 9</a> for more details on DNIS checking and restrictions.
<b>Reverse DNIS Check</b>	Enabling this option reverses the default DNIS checking logic. Any number not in the DNIS table is allowed access, while any number that is in the table is denied access.
<b>Reject attributes</b>	This option enables Reject List checking. Please see the ODBC Advanced section in <a href="#">Chapter 9</a> for more details on the Reject List option.
<b>Time banking</b>	The Time Banking feature allows you to specify a set number of maximum minutes the user can log in for (a block of time). Please note that this is not a recurring number, and once the number of minutes is gone, you <b>must</b> manually add more minutes or the user will not be able to log on.
<b>Ascend max time</b>	Enabling this option causes RADIUS to send the Ascend-Maximum-Time attribute instead of the standard Session-Timeout attribute. This is necessary for compatibility with very old versions of Ascend's operating system. It's recommended you upgrade rather than enable this option.
<b>IP Pooling</b>	IP Pooling enables RADIUS-based address allocation. Please see the <a href="#">Chapter 9</a> for more details on IP Pooling.
<b>Command Trigger</b>	Enables RADIUS to execute other programs after specified users authenticate. For example, when a user logs in, this feature would allow RADIUS to execute a program to send all spooled e-mail messages for users in that domain.
<b>Accounting</b>	

<b>Manual Calls Update</b>	RadiusNT/X will manually update the ServerPorts table. This is only needed for databases that do not have trigger support. The option is <b>not</b> needed with Emerald/SQL Server or an active database that can update the calls on-line view automatically.
<b>Stop Records Only</b>	RadiusNT/X usually stores both start and stop records in the database. With this option enabled, RadiusNT/X will not store start records in the database, but will instead perform a manual update to the ServerPorts table to track calls on-line.
<b>SNMP</b>	<b>All SNMP features are Professional/Enterprise version only.</b>
<b>Statistics</b>	This option enables SNMP statistics. See <a href="#">Chapter 9</a> for more information about SNMP.
<b>Server-Ports update</b>	This option periodically updates ServerPorts if it detects different port changes via SNMP. When enabled, SNMP Concurrency Checking is automatically disabled.
<b>Concurrency Check</b>	This option enables SNMP Concurrency verification. See <a href="#">Chapter 9</a> for more information about SNMP.
<b>Bind IP-Address</b>	The IP address to listen for requests on. Selecting ALL will allow RadiusNT/X to listen on all IP Addresses configured. Otherwise, you can select a specific IP Address to listen on.
<b>Database test</b>	RADIUS opens a connection to every datasource available to it. The duration of each connection will be the number of seconds specified. If the connection fails, the datasource is marked unavailable ( <b>Enterprise &amp; Professional version only</b> ).
<b>Database time offset</b>	How often (in days) the authentication and accounting databases are queried to compute a time offset from the local clock for various authentication and accounting functions. The default value is optimal and should not require changing.
<b>Cache persistence</b>	Enable the Accounting and/or Authentication cache database to be regularly written to disk. This enables RadiusNT/X to recover after being restarted where no valid authentication data sources exist. (Enterprise & Professional version only)
<b>Syslog IP</b>	Both error and informational messages can be directed to a syslog server by specifying an IP address.
<b>Disable '0' Session-ID port clear</b>	Prevent RadiusNT/X from clearing all users from the On-line view for a NAS that sends a 0 Session-ID.
<b>Disable Acct On/Off port clear</b>	Prevent RadiusNT/X from clearing all users from the On-line view when a NAS sends an Accounting Start/Stop request.

**Disable Class  
ServerID/AccountID tracking**

Prevent RadiusNT/X from using the Class attribute to track users and servers by ID. Disabling this option prevents separation of accounting data for multiple accounts with the same username.

## PROXY Option

Proxy	
Proxy options	<input checked="" type="checkbox"/> User - Auth <input type="checkbox"/> User - Auth - Unknown <input checked="" type="checkbox"/> Accounting <input type="checkbox"/> Accounting - Echo <input type="checkbox"/> Accounting - local copy <input type="checkbox"/> Server proxy
Store & forward accounting mode	<input type="checkbox"/>
Persistent store & forward log	<input type="checkbox"/>
Force flush store and forward log before accounting ack	<input type="checkbox"/>
Proxy timeout	<input type="text" value="30"/>
Proxy identifier	<input type="text"/>

Option	Description
<b>Proxy Options</b>	See <a href="#">Chapter 9</a> for information about proxy options.
<b>Store and forward</b>	Enables store and forward proxy mode. <b>(Enterprise version only)</b>
<b>Persistent log</b>	When store and forward mode is enabled, this option controls whether to log accounting data to disk, allowing recovery of unsent accounting data if the system reboots. <b>(Enterprise version only)</b>
<b>Flush log before ack</b>	Enabling this option guarantees accounting data is physically written to persistent storage before replying to an accounting request. <b>(Enterprise version only)</b>
<b>Proxy Timeout</b>	This value sets the total timeout period for a proxy server before the proxy server is determined to be down. (Note: This does not set the individual request timeout for a proxy server, it sets the total timeout for any proxy server over multiple attempts).
<b>Proxy Identifier</b>	RadiusNT/X replaces the NAS-Identifier with this IP Address when sending a proxy request. This can "hide" the NAS-Identifier from the Proxy Server.

### SMART CACHING Option

Smart caching	
Preload users who've called within ( <i>days</i> )	<input type="text" value="15"/>
Last modified account check ( <i>secs</i> )	<input type="text" value="300"/>
Delete unused accounts ( <i>secs</i> )	<input type="text" value="25"/>
Force cache update ( <i>days</i> )	<input type="text" value="7"/>
Check for deleted accounts ( <i>mins</i> )	<input type="text" value="360"/>
Refresh account types ( <i>mins</i> )	<input type="text" value="34"/>
Double-check override where cache data is newer ( <i>secs</i> )	<input type="text" value="15"/>
Server access refresh ( <i>mins</i> )	<input type="text" value="31"/>
Refresh DNIS ( <i>mins</i> )	<input type="text" value="37"/>
Refresh roam servers ( <i>mins</i> )	<input type="text" value="20"/>
Refresh attribute rejects ( <i>mins</i> )	<input type="text" value="60"/>
Refresh proxy attributes ( <i>mins</i> )	<input type="text" value="20"/>
Free update memory ( <i>mins</i> )	<input type="text" value="30"/>
Cache double-check	<input checked="" type="checkbox"/>
Write cache database to disk ( <i>mins</i> )	<input type="text" value="60"/>
Cache root directory	<input type="text"/>

Option	Description
<b>Preload</b>	Number of days since the last successful authentication an account should be preloaded into the cache.
<b>Last modified acct check</b>	This option determines how often the database is checked for modifications and the cache is updated with the new information (in seconds)..

<b>Delete unused accounts</b>	Number of days an account can remain in the cache without being requested before being removed.
<b>Force cache update</b>	The time (in days) that an idle entry can remain in the cache before a forced update of the entry occurs.
<b>Check for deleted accounts</b>	Users can authenticate as long as there is a valid entry in the cache. This option controls how often the cached entries are compared with the database for deleted database entries. This option is similar to, but distinct from, "modify", which sets the time between checks for database entries being marked inactive. Users can authenticate if a login attempt occurs after a deletion or inactivation within these refresh timeout windows.
<b>Refresh account types</b>	Service type cache update interval (in minutes).
<b>Double-check override</b>	Interval (in seconds) to override checking the database (for new information that may cause the authentication to succeed) to prevent extra database queries.
<b>Server access refresh</b>	Server-Access cache update interval (in minutes).
<b>Refresh DNIS</b>	DNIS cache update interval (in minutes).
<b>Refresh roam servers</b>	Roam Server cache update interval (in minutes).
<b>Refresh attribute rejects</b>	Reject cache update interval (in minutes).
<b>Refresh proxy attributes</b>	Proxy attributes update interval (in minutes)
<b>Free update memory</b>	The memory used to update account information is not immediately freed. Instead, it is placed in a queue to be removed later. This option controls how often the delete process is run. Please note that any object less than 5 minutes old cannot be removed. If you are performing Time Banking and do not have ample memory, set this low (a couple of minutes). In most cases, the default value is optimal. (Enterprise & Professional version only)
<b>Cache double-check</b>	The Double Check option queries the database when the cache copy would otherwise reject an authentication request (for example, in the case of an expired account, bad password or when there is no time left in the time bank). This usually isn't necessary, as account changes are regularly synchronized with the database. 0/1 Enabled    2 Disabled
<b>Write cache db to disk</b>	This option enables you to specify how often the contents of the cache database should be written to disk to allow starting to a useable state where no authentication database is available. (Enterprise & Professional version only)

**Cache root directory**

This entry shows the directory where RadiusNT stores cache data.  
(Enterprise & Professional version only)

### **LICENSING Option**

Licensing	
Company name	<input type="text" value="ISP, Inc."/>
License key	<input type="text"/>

Option	Description
Company Name	License Key Company Name (Including IP Address if present). Enter exactly as in the license description provided by IEA Software.
License Key	RadiusNT/X License Key

### **Users and Clients files**

Please note that you **must** configure the *clients* and *users* files outside of the Administrator using any text editor. See "users.example" and "clients.example" for sample configurations.



## LDAP Option

LDAP	
Server address <i>(Multiple servers for failover)</i>	<div style="border: 1px solid gray; padding: 5px;"><div style="display: flex; align-items: flex-start;"><div style="border: 1px solid gray; padding: 2px; margin-right: 5px;">ldap1</div><div style="border: 1px solid gray; padding: 2px; margin-right: 5px;">ldap2</div><div style="margin-left: 10px;"><input type="button" value="Up"/> <input type="button" value="Down"/> <input type="button" value="Delete"/></div></div><div style="margin-top: 5px;"><input style="width: 100%;" type="text"/><input type="button" value="Add"/></div></div>
Server port	<input style="width: 50%;" type="text"/>
Server timeout (secs)	<input style="width: 50%;" type="text"/>
Netscape 4.x SSL Cert	<input style="width: 100%;" type="text"/>
Search filter	<input style="width: 100%;" type="text" value="(uid=\$login)"/>
Search bind DN	<input style="width: 100%;" type="text" value="cn=Directory Manager"/>
Search bind password	<input style="width: 100%;" type="password" value="*****"/>
Search scope	<input style="width: 100%;" type="text" value="One level"/> <input type="button" value="v"/>
Base directory (DN)	<input style="width: 100%;" type="text" value="ou=users,o=test.com"/>
Account type attribute	<input style="width: 100%;" type="text"/>
Login limit attribute	<input style="width: 100%;" type="text"/>

Option	Description				
<b>Servers</b>	The list of LDAP Servers to authenticate against. Secondary servers are used only if the primary is not available.				
<b>SSL Cert</b>	If you are connecting to the LDAP server using an SSL connection, this field should be the name of your Netscape 4 SSL certificate file.				
<b>Username</b>	The username(DN) to connect to the LDAP server as.				
<b>Password</b>	The password to connect to the LDAP server with.				
<b>Port</b>	The port to connect to the LDAP Server on. The default port is 389, unless using SSL that would then be 636.				
<b>Timeout</b>	The Directory Search timeout in seconds. When the limit is reached, the LDAP module returns "ignore", giving another authentication method a chance to succeed.				
<b>Login Limit</b>	The LDAP attribute used to specify a Database Concurrency Login Limit. If left blank, this feature is disabled. RadiusNT/X must be running in database mode to use this feature.				
<b>Account Type</b>	The LDAP attribute used to specify a Database Account Type (Profile). If left blank this feature is disabled. RadiusNT/X must be running in database mode to use this feature.				
<b>Search</b>	The search string used to search accounts or bind as a user. Please see the LDAP Authentication section in <a href="#">Chapter 10</a> for more details on this option.				
<b>Base DN</b>	The Base directory under which to search for matching user entries.				
<b>Scope</b>	This option determines how deep to search the directory tree for the user (In this example, "neila"). [ ]s represent the Base DN.				
	<table> <tr> <td>One Level Deep:</td> <td>uid=neila,[ou=moon,o=nasa]</td> </tr> <tr> <td>Sub-Tree:</td> <td>uid=neila,ou=moon,[o=nasa]</td> </tr> </table>	One Level Deep:	uid=neila,[ou=moon,o=nasa]	Sub-Tree:	uid=neila,ou=moon,[o=nasa]
One Level Deep:	uid=neila,[ou=moon,o=nasa]				
Sub-Tree:	uid=neila,ou=moon,[o=nasa]				

## EXTERNAL AUTHENTICATION Option

**External auth**

Authentication methods (Try order)

safeword  
authapi.dll\dom1  
tacacs  
ldap

External auth library path

c:\vss\radiusnt\authapi\debug

Option	Description
<b>Authentication Methods</b>	<p>The list of additional authentication sources in which to look for users. The order is important, as users will be searched in the order specified. Methods can be restricted to domains by appending “\domain” to the end of the method. For example, LDAP becomes LDAP\ldap.com. Domain specific auth methods take precedence over global methods. Available built-in authentication methods are: unix, winnt, ldap, tacacs, ace3, safeword and defender. <b>Authentication methods are not available in RadiusNT/X Emerald-only.</b></p> <p>If you are using an external authentication library as an authentication method, enter the name of the shared library, including any file extension.</p>
<b>External auth path</b>	<p>The directory where external authentication libraries are kept. This option is not required if you are using one of the built-in authentication methods listed above.</p>

RadiusNT/X Ver. 4

42

IEA Software, Inc.

### DEFENDER Option – Token Based Security Configuration

Defender	
Server address <i>(Multiple servers for failover)</i>	<div style="border: 1px solid gray; padding: 5px;"><div style="display: flex; align-items: flex-start;"><div style="flex: 1;"><input type="text" value="test.com"/></div><div style="flex: 0 0 40px; text-align: center;"><input type="button" value="Up"/> <input type="button" value="Down"/> <input type="button" value="Delete"/> <input type="button" value="Add"/></div></div></div>
Server port	<input type="text"/>
Server timeout <i>(secs)</i>	<input type="text" value="34"/>
Length to count timed out servers down <i>(secs)</i>	<input type="text"/>
Agent ID	<input type="text"/>

Safeword	
Server address	<input type="text"/>
Port number	<input type="text"/>

Option	Description
<b>SafeWord</b>	
<b>Hosts</b>	A space-separated list of SafeWord Servers to authenticate against. Secondary servers are used only if the primary server is not available.
<b>Port</b>	The port to connect to the Safeword server on.
<b>Defender</b>	
<b>Hosts</b>	A space-separated list of SafeWord Servers to authenticate against. Secondary servers are used only if the primary is not available.
<b>Agent ID</b>	The AgentID of the RadiusNT server. Defaults to RadiusNT or RadiusX, respectively. You must configure this AgentID on the SafeWord server before RadiusNT/X can make requests to the SafeWord server.
<b>Port</b>	The port to connect to the Safeword server on.
<b>Timeout</b>	This value sets the amount of time to wait for a response before trying a secondary server.
<b>Down</b>	This value sets the total timeout period for the server before it is determined to be down.

### TACACS+ Option

Tacacs+	
Server address	<input type="text" value="207.53.165.6"/>
Shared secret	<input type="text" value="localhost"/>
Timeout (secs)	<input type="text" value="3"/>
Port number	<input type="text" value="49"/>

Option	Description
<b>TACACS</b>	
<b>Server</b>	The host name or IP address of the TACACS server.
<b>Secret</b>	The shared Secret between the TACACS server and RadiusNT/X.
<b>Timeout</b>	The amount of time to wait for a response from the TACACS server.
<b>Port</b>	The port of the TACACS server. Defaults to 49.

<b>Quick Tip!</b>	Please note that RadiusX does <b>not</b> run as a Service. After configuration, you will need to run the RadiusX program in the background by typing <code>./radiusd&amp;</code> in the <code>/usr/local/radius</code> directory.
-------------------	---

## Chapter 2 - MODES

### **RadiusNT/X User and Configuration Mode Options**

RadiusNT/X has the capability to run in three different modes: Text, ODBC or Both. Each offers a different advantage and each returns different results. For example, most of the Advanced features are only available in ODBC mode, as they require a database configuration. On the other hand, Text mode is convenient when you need a fast and 'light weight' RADIUS server without a lot of advanced features. (For example, if you wanted to authenticate users from the NT SAM and do not care about accounting records.) Text mode doesn't require a database setup, and is a good quick failover mode in the case that a problem occurs with the database or the database connection.

#### **Quick Tip!**

If you are using the Emerald Management Suite, you will need to set up RadiusNT in ODBC mode. The ODBC DSN needs to point to the Emerald database you created with the Emerald Administrator.

### **Text Mode**

The simplest way to authenticate users is by running RadiusNT/X in Text mode. When RadiusNT/X starts in Text mode, the system will read in and initialize itself using the configuration data in the Users, Clients and Dictionary files. If you change any of these files, you **must** stop and re-start RadiusNT/X for the changes to take effect. Please follow the steps below to configure and run RadiusNT/X in Text mode:

1. Create the directory that you specified as the Accounting Directory in the RadiusNT/X Administrator during system configuration.
2. Copy the *clients.example* file to a file named *clients*. Although you can simply rename the file, copying is preferred so that you can retain the provided *clients* file example. For RadiusNT, the default directory for this file is c:\radius; for RadiusX, it is the /usr/local/radius directory.
3. Next, use a text file editor to edit the *clients* file. Within the file, replace "**Portmaster1**" with the IP address of your NAS. **DO NOT USE THE DNS NAME YET**. You can change this to a DNS name at a later time, if desired.
4. Change the default password, "**localhost**", to your RADIUS server secret value. The secret may NOT have any spaces, and it is case sensitive. Please choose a secret that is between 4-10 characters in length. Remember your secret, as you will need it again when configuring your NAS.
5. Save the *clients* file changes.

#### **Important Note!**

For these file modifications, it is required to use a text file editor that will recognize and preserve Tabs. Please use an editor such as [Programmer's File Editor](#), pico, or vi. Older versions of Notepad and the DOS "edit" program do not preserve Tabs on File Save.

6. Edit the file named *users*, then uncomment the following four lines from it:

```
test Password = "test"  
User-Service = Framed-User,  
Framed-Protocol = PPP,  
Framed-Address = 255.255.255.254
```

**Note!**

Please make certain that there is only ONE Tab between **test** and **Password**. Spacing is crucial, and there **must** be exactly one tab before the other three lines. Note that CASE is also significant.

7. Save the *users* file. In future, you may want to refer to the *users.example* file to explore more complex user entries.
8. Next, go to the Command Prompt and change to the directory where RadiusNT/X is installed.
9. Execute the following command to start RadiusNT/X in debug mode:

```
"radius -x15"
```

RadiusNT/X will return errors in the case that something is not configured correctly within the files. If everything is properly configured, an "initialized..." status line will be returned. At this point, you can continue on to the Terminal Server Configuration section.

Please note that the *dictionary* file is only used in Text mode. It is used to identify RADIUS attribute values and it is automatically created upon installation. The file lists all of the types of information that you can collect about users and their connections. Each attribute has a value or a list of possible values. Please refer to the following table to more clearly understand the *dictionary* file entries and how it is used:

Question	Attribute
Who are you?	User-Name
Where are you located?	Framed-IP-Address
What is your phone number?	Calling-Station-ID
What address are you entering the network from?	NAS-IP-Address
How do you want to enter?	Framed-Protocol
How will we know it is you?	Password
What service will you want to use?	Service-Type
How long will you be a user?	Expiration
How can we limit what you can see?	Filter-ID

Please remember, if you choose to change the information in any of these three files, you **must** stop and restart RadiusNT/X for the changes to take effect.



## **ODBC Mode**

The ODBC feature of RadiusNT/X sets it apart from most other RADIUS servers. RadiusNT/X was specifically designed to offer in-depth support and features using ODBC data sources.

RadiusNT/X's ODBC layout is based on the database layout of the Emerald Management Suite (please see <http://www.iea-software.com/products>). With some understanding of databases, you can easily set up RadiusNT/X to work with most relational database systems. We have included a sample MS Access 7.0 database in the RadiusNT distribution with forms and sample data already created for your convenience.

In order to run RadiusNT/X in ODBC mode, a system ODBC DSN must be created for use with your operating system. The following sections outline how to create the required DSN.

### **Creating a system ODBC DSN for Windows (RadiusNT):**

1. Select **Start, Settings** and then **Control Panel**.
2. From the Control Panel, (Win2000 users select **Admin Tools**), then select **ODBC**. Please note that if you do not have ODBC installed, you will need to install ODBC 2.5 or higher to proceed. ODBC is shipped with many applications, and is available from Microsoft's FTP site at <ftp://ftp.microsoft.com/developr/ODBC/public/>. You can also install ODBC from the SQL Server CD-ROM directory `\i386\odbc`.
3. After the ODBC Administrator opens, select the **System DSN** button. If your system does not display a System DSN button, you will need to upgrade to at least ODBC 2.5 or higher.
4. Click the **Add** button.
5. For a SQL Server installation, select the **SQL Server Driver**. For other database types, select the corresponding **ODBC Driver**. For an Emerald installation, please see [Appendix B](#).
6. For the Data Source Name option, type "**Radius**".
7. Enter "**RadiusNT**" for the Description.
8. Depending on what type of driver you have installed, the next step will vary. Please refer to your database documentation to learn more about configuring an ODBC DSN for your database system.

#### ?? SQL Server

- ?? For Server, enter the name of the SQL Server you are using.
- ?? Leave the Library and Network addresses set to default.

#### ?? MS Access

- ?? Click the **Select** button in the database box and choose your MS Access file. Please note that if you need to log into the database, you will need to select the Advanced option and fill in the required information.
- ?? Finally, select **Save** and close the Control Panel.

## Creating a system ODBC DSN for Linux or Solaris (RadiusX):

When RadiusX was installed, it generated the ODBC driver and manager needed to connect to the database from information you provided. The configuration file created is named ***odbc.ini*** and is located in the ***/usr/local/radius*** directory. A sample *odbc.ini* file is listed below:

```
[ODBC]
Trace=0
TraceFile=/usr/local/radius/log/odbctrace.log
TraceDll=/usr/local/radius/lib/odbctrac.so
InstallDir=/usr/local/radius/lib/..
```

```
[ODBC Data Sources]
Radius_MSSQL65=RadiusX ODBC Driver
```

```
[Radius_MSSQL65]
Driver=/usr/local/radius/lib/E-msss16.so
Description=Radius_MSSQL65
Database=Radius
ServerIPAddress=127.0.0.1
ServerPortNumber=1433
LogonID=
Password=
UseProcForPrepare=0
QuotedId=No
AnsiNPW=No
```

```
[SOFTWARE\Microsoft\MSSQLServer\Client\TDS]
Radius_MSSQL65=4.2
```

If you would like to modify the file in any way, you must either delete the *odbc.ini* file and run the installation program again, or edit the file. The most common lines to be modified for Microsoft SQL Server and Sybase are as follows: (Please note that the installer automatically creates the DSN names.)

Database=Radius

This is the name of the database containing your RADIUS database.

ServerIPAddress=127.0.0.1

This reflects the IP address of the SQL Server and must be numeric.

ServerPortNumber=1433

This indicates the TCP port that the SQL Server is 'listening' on.

When you start RadiusX, it sets the ODBCINI environment. To edit the settings, please do the following:

1. Begin by changing to the directory where the ***odbc.ini*** file exists, ***/usr/local/radius***.
2. Open the ***odbc.ini*** file with a plain text editor.
3. Make the needed changes.
4. When you have completed your changes, be sure to **Save** the file.

5. **Restart** RadiusX.

Please note that, should you need to debug the [ODBC] section, by setting Trace=1 you will log all SQL commands to a file named *odbctrace.log* in the */usr/local/radius/log* directory.

### Configuring RadiusNT/X for ODBC Mode

Once the System ODBC DSN has been created, the RadiusNT/X Administrator is used to configure the RadiusNT/X application for ODBC mod against the system ODBC DSN configuration. To configure RadiusNT/X for ODBC mode, follow these steps:

1. While in the RadiusNT/X Administrator, select **Database Mode** from the **General** menu option.
2. From the **DSN** pick list on the Authentication page, select the **System ODBC DSN** that you created in the steps above.
3. Next, enter the database Username and Password.
4. Click the **Save Changes** menu option to test your database connection.
5. The next step is to configure the database **before** starting RadiusNT/X. Please use your database platform's SQL command interface to insert server entries directly to the Servers table (RadiusNT/X Enterprise edition customers should use the RadiusNT/X User Manager to do this). These entries should reflect the information you would have entered in the *Clients* file for Text Mode (see prior explanation). The three Server table fields that are required for each entry are: **Name**, **IP Address**, and **Secret**; all other fields are informational only.
6. For the Calls Online feature to function properly, you may also need to populate the ServersPorts table detailing the available ports associated with each Server table entry.
7. Lastly, start RadiusNT/X. Do this by accessing a Command Prompt and executing the following command from within the RadiusNT/X installation directory:

"radius -x15", or

"/radiusd -x15" to start RadiusX in full debug mode.

If everything is configured correctly, a "initialized..." line will be returned. At this point you can minimize the window and continue on to the Terminal Server Configuration section. RadiusNT/X will return error messages if something is not configured correctly. If this occurs, please go back and run through the directions again carefully.

For an Emerald installation, please see [Appendix B](#).

## ***Both Mode***

Both mode is a special case where you want to either authenticate from both the ODBC database and the *users* file, or store accounting information in the ODBC database and the detail files.

For authentication, the *users* file is read when RadiusNT/X starts. RadiusNT/X will attempt to locate the user in the ODBC database first. If the user is not found, then RadiusNT/X will search its copy of the *users* file in memory for the user.

For accounting, RadiusNT/X will first store the information in the Calls table, and then append the information to the detail file for that NAS.

Please note that if you do **not** want duplicate accounting, and want the two authentication choices, you may specify an Accounting Directory that does not exist. In this case, RadiusNT/X will not write any accounting information. You **must** have a *users* file if you have text file mode checked. If you **only** want duplicate accounting, simply create an empty *users* file, and RadiusNT/X will authenticate from the database only.

## Chapter 3 - TERMINAL SERVER CONFIGURATION

RadiusNT/X can interact with many different RADIUS clients simultaneously, even if they are from different vendors. Sample configurations for several of the more popular NAS vendors' equipment are listed below. You **must** consult the documentation for your NAS as the final authority on how to configure your NAS for RADIUS interaction.

### ***Livingston Portmasters***

Telnet to the Portmaster and enter these commands:

```
set authentic x.x.x.x
set accounting x.x.x.x
set secret yyyyy
save glo
```

Where x.x.x.x is the IP address of the machine that you have RadiusNT/X running on and yyyyy is the secret which you entered for **THIS NAS** in the *clients* file or ODBC database. Remember that the secret is case sensitive and **must** match exactly.

### ***Ascend MAX and Pipeline***

Configure the device in the menu system as shown below. The configuration menus may vary slightly based on the OS version.

Ethernet...Mod Config...Auth... as:

```
Auth=RADIUS
Auth Host #1=x.x.x.x
Auth Port=1812
Auth Timeout=5
Auth Key=yyyyy
Auth Pool=No
Auth Req=Yes
```

Ethernet...Mod Config...Accounting... as:

```
Acct=RADIUS
Acct Host #1=x.x.x.x
Acct Port=1813
Acct Timeout=5
Acct Key=yyyyy
```

Where x.x.x.x is the IP address of the machine that you have RadiusNT/X running on and yyyyy is the secret which you entered for **THIS NAS** in the *clients* file or ODBC database. Remember that the secret is case sensitive and **must** match exactly.

## ***Other RADIUS compatible NAS***

Basic configuration settings are as follows:

- ?? Set Authentication and Accounting to RADIUS
- ?? Set Authentication and Accounting servers to the Radius NT/X server's IP address
- ?? Set Authentication and Accounting secrets to the same as they are in the *clients* file or ODBC database
- ?? Set Authentication and Accounting ports to **1812** and **1813**, respectively

Please check the RADIUS Technology Partners Web page on our Web site [at http://www.iea-software.com/products](http://www.iea-software.com/products) for links to vendor configuration instructions and RADIUS information.

## Chapter 4 - TESTING RADIUSNT/X

You can easily test RadiusNT/X by dialing into your NAS and trying to log in as a user that you have configured in either the *users* file or the ODBC database. If the login is successful, you will receive an authentication response from RadiusNT/X and your NAS. Once a successful test has been completed, you can install RadiusNT to run as a service to start up automatically, or RadiusX to start up automatically through a script.

### **Radlogin**

There may be times when you would like to test the authentication and accounting features of RadiusNT/X or an account without going through the trouble of dialing into a RADIUS client. Radlogin (included with RadiusNT/X) is a program that can make authentication and accounting requests to a RADIUS server without going through the dialup process.

In order to utilize Radlogin, you **must** configure RadiusNT/X to accept requests from the machine that is running Radlogin, just as if Radlogin were a terminal server itself. If Radlogin and RadiusNT/X are running on the same machine, you can use the localhost address. Otherwise, you will need to use the IP Address of the machine Radlogin is running on.

For example, if you are running RadiusNT/X in text mode, edit your *clients* file to look like the example below:

```
1.2.3.4 mysecret
127.0.0.1 localhost
```

The first entry is your NAS entry as described in [Chapter 2](#). The second entry signifies to RadiusNT/X that requests can come from the localhost using a secret of "localhost". If you are running RadiusNT/X in ODBC mode, you will need to add a similar entry to your servers table.

**Note:** You **must** restart RadiusNT/X for these changes to take effect.

Radlogin uses a file named *server* to read its configuration information. The *server* file has the same format as the *clients* file. If you are running Radlogin on the same machine as RadiusNT/X, your server entry will be exactly like the line you added to your *clients* file above. Radlogin reads only the first line of the *server* file; all other lines are ignored. Please see the sample *server* file entry below:

```
127.0.0.1 localhost
```

Now that all components have been configured, open a Command Prompt and change to the directory where RadiusNT/X is installed (typically C:\radius for Windows NT or /usr/local/radius for UNIX).

The Radlogin program allows two or three parameters. When you type "Radlogin" at the Command Prompt, command line options will be displayed as shown below:

```
Radlogin RADIUS test client for RadiusNT/X
Copyright 1996-1999 IEA Software, Inc.
```

Usage: radlogin [username] [password] [# of checks]

Usage: radlogin [username] START

Usage: radlogin [username] STOP

### ***Authentication Test***

To send an authentication request to RadiusNT/X, type "radlogin", followed by a username and password. Please note that you may need to put quotes around the username or password if they include a space. By default, Radlogin will return a verbose result stating whether the request was acknowledged, along with any attributes RadiusNT/X returned. Optionally, you can include a number as the third parameter to send multiple, sequential tests. This is a handy way to check performance. The Radlogin results will summarize the requests and give an average response time.

### ***Accounting Test***

To send an accounting request to RadiusNT/X, type "radlogin" followed by a username and either "**START**" or "**STOP**". The second parameter **must** be in all upper case or it will be interpreted as an authentication request's password. By default, Radlogin will return a verbose result stating whether the request was responded to along with any attributes RadiusNT/X returned. Optionally, you can include a number as the third parameter to send multiple, sequential tests. This is a handy way to check performance. The Radlogin results will summarize the requests and give an average response time.

### ***Troubleshooting***

If your Radlogin test was not successful, please check the following hints. You can find additional troubleshooting tips and Frequently Asked Questions (FAQ) in Chapters [10](#) and [11](#).

1. If you do not see the authentication request on the RadiusNT/X screen, your NAS is not set up correctly and is not sending the RADIUS requests to RadiusNT/X. Please check the NAS RADIUS configuration and make sure RadiusNT/X is "listening" on the same port the NAS is sending the request to.
2. If you see the request on the RadiusNT/X screen, but RadiusNT/X returns the error "security breach", then the request was received from an IP address which is not authorized to send RADIUS requests to RadiusNT/X. Please check the *clients* file or the ODBC database servers table to make sure the NAS making the request is listed along with the proper information. Don't forget to restart RadiusNT/X if you have changed the client information.
3. Address mismatch errors point to DNS problems. The error shows that RadiusNT/X received a request from the IP address x.x.x.x. When RadiusNT/X looked up the IP address x.x.x.x, it received the host named yyyy. However, the DNS for host yyyy is NOT the same IP address as x.x.x.x. Please note that RadiusNT/X uses the servers table to lookup hosts.
4. If RadiusNT/X is sending a NAK to the NAS, and the decrypted password looks like strange characters, then the secret that is configured in the NAS is not the same secret you configured for the NAS in the *clients* file or ODBC database servers table.



## Chapter 5 – RADIUSNT AS A SERVICE

RadiusNT runs natively as a service. Once a successful test of RadiusNT has been completed, you can install it to run as a service and start up automatically. Please note that if you run RadiusNT from a DOS prompt without using the -x command line option, RadiusNT will attempt to start as a service, fail and then return to the command prompt.

### Quick Tip!

Running RadiusNT as a service is handy for times when you are not logged in and need to start or stop RadiusNT remotely.

### ***Installing RadiusNT as a Service***

**To install RadiusNT as a service, follow the steps below:**

Select the “**Install as a service**” icon from the RadiusNT program group.

**To manually install RadiusNT as a service, follow these steps:**

1. Access a Command Prompt and change to the directory where RadiusNT is installed (typically *c:\radius*).
2. Type the command “Radius.exe -install”. Do not leave off the .exe extension, or the installation will not work. A message will be displayed stating that the service is being installed. If the service does not install, please use the -x15 command line option to begin troubleshooting. For more information, please check out the [Debug](#) option section. Make sure that services can interact with the desktop, and that the userid RadiusNT is using to run as a service has the proper permissions to access the ODBC datasource.

### ***Removing the Service***

**To manually remove the RadiusNT service, follow these steps:**

1. Open a Command Prompt.
2. Change to the directory where RadiusNT resides (typically *c:\radius*).
3. Type the command “Radius.exe -remove”. A message stating that the service has been removed will be displayed.

### ***Service Considerations***

You can start and stop the RadiusNT service using the Services applet on the Control Panel.



Should you encounter any problems, run RadiusNT from a Command Prompt using the “-x15” option. In most cases, the debug feature will return a statement explaining why RadiusNT is not starting. Also, you

can use the Services applet on the Control Panel to configure the service to start automatically when the computer is booted. This default installation option is highly recommended.

## Chapter 6 – EXTERNAL AUTHENTICATION

### ***UNIX passwd File***

RadiusNT/X can authenticate from a UNIX *passwd*, *spasswd* or comparable file, similar to the way UNIX RADIUS servers function. For RadiusNT/X to authenticate a user from the “*passwd*” file, you will need to make the user’s password value be “UNIX” in the RadiusNT/X *users* file (Text Mode) or database (ODBC mode). Please note that case *is* significant. When RadiusNT/X discovers a password of “UNIX”, it searches for a file called “*passwd*” in its current directory or the directory where the system has located the file. This will vary depending on what type of system configuration you are using. RadiusX actually uses the Unix Application Program Interface (APIs) to authenticate the user, rather than directly looking into the “*passwd*” file, which the system itself does.

The file **must** match the format of a “*passwd*” file from a standard UNIX machine. The user’s password is typically one-way encrypted and compared to with the entry in the “*passwd*” file. If no entry is found, the user is not authenticated.

This works for both database and *users* file entries. There is a special option that can be enabled in ODBC mode to allow RadiusNT/X to replace the “UNIX” password with the password the user entered during authentication (if the passwords match). This option is used for migration purposes to reverse the encrypted passwords, clearing text passwords stored in the database. To enable this option, select the **Replace Password** option under the **Advanced** section within the RadiusNT/X Administrator. For more information, please read the RadiusNT/X [Registry](#) entries section.

Note: CHAP cannot be used when authenticating against a UNIX password file.

Below is a sample *users* file entry. Please remember that case is **very** important.

```
name Password = "UNIX"
      User-Service = Framed-User

DEFAULT Password = "UNIX"
        User-Service = Framed-User
```

### ***Windows NT SAM Support***

RadiusNT can also authenticate from Windows NT SAM. For RadiusNT to authenticate users from the NT SAM, RadiusNT **must** run as an Administrative user. Using the Services applet on the Control panel, you can specify how RadiusNT will log in when it runs as a service.

For RadiusNT to authenticate a user from the Windows NT SAM, you will need to make the user’s password value be “WINNT” in the RadiusNT *users* file (Text Mode) or database (ODBC mode). When RadiusNT discovers a password starting with “WINNT”, it searches for a backslash (\) following the password. If there is a backslash, and it is **not** the last character, then RadiusNT uses whatever follows the backslash as the NT Domain for the user. If the Password is simply “WINNT” or “WINNT\”, the local Windows NT user database is used to authenticate the user (assuming RadiusNT is running on a non-Domain Controller).

This works for both database and *users* file entries. There is a special option that can be enabled in ODBC mode to allow RadiusNT to replace the "WINNT" password with the actual password the user entered during authentication (if the passwords match). This is used for migration purposes to reverse the encrypted passwords, clearing text passwords. To enable this option, select the **Replace Password** option under the **Advanced** section within the RadiusNT/X Administrator. For more information, please read the RadiusNT/X [Registry](#) entries section.

Below is a sample *users* file entry: (Please remember that case is **very** important.)

```
name Password = "WINNT"  
      User-Service = Framed-User
```

If you are running RadiusNT in **Text** mode, you can use the DEFAULT user entry to examine the NT SAM for the usernames and passwords. To accomplish this, create an entry at the end of the *users* file as shown below:

```
DEFAULT Password = "WINNT\DOMAIN"  
        User-Service = Framed-User
```

Please note that the \DOMAIN is optional and should either be removed or changed to the default domain which to authenticate against.

### ***Additional Authentication Methods***

RadiusNT/X provides additional authentication method options when running the Enterprise edition. Please see [Chapter 9](#) for more information on LDAP authentication and [Chapter 10](#) for more information on the Enterprise authentication and External Authentication API features.

## Chapter 7 – COMMAND LINE AND REGISTRY SETTINGS

RadiusNT has the ability to accept a variety of command line options. Typically, you will only use these if you are trying to debug a problem or test a configuration. You may also set command line options to permanent options in the Registry.

### Warning!

**Changing values in the Windows NT Registry can cause the system to become unstable or to stop working. Always use caution when manually changing registry entries.**

When radius.exe -install is used to install RadiusNT as a service, it will create the KEY as follows:

```
HKEY_LOCAL_MACHINE\Software\IEA\RadiusNT
```

In order to add parameters to RadiusNT via the registry, you will need to add specific values to the RadiusNT key. Please note that command line options **override** registry defaults. As an example, to set the default MODE for RadiusNT, you would add the value as shown below:

```
HKEY_LOCAL_MACHINE\Software\IEA\RadiusNT\Mode
```

Where mode "1" is for ODBC, and "2" is for **both** ODBC and Text mode. Zero (0) is the default for text mode. RadiusNT will only read the registry values at startup. If you change a value, you **must** re-start RadiusNT in order for the change to take affect.

### Command Line and Registry/INI Listings

The following is a list of all Command Line Options and Registry/INI values currently supported by RadiusNT/X:

Command Line	Registry/INI	Description
-a [path]	AcctDirectory	This option specifies the accounting directory (the default is \radius\acct). Within the directory there will be a directory for each NAS that sends accounting requests to RadiusNT. An accounting file containing all accounting information named <i>detail</i> will reside in each NAS directory.
-A	ReqAcctAuth	Use this option to advise RadiusNT to require Accounting packets to have the secret appended. Otherwise, any valid accounting packet from a NAS in the <i>clients</i> file or servers table is allowed.
-C	SNMP	This enables the SNMP Functions of RadiusNT. Add up the options you wish to use: 1 Statistics 2 Concurrency Checking 3 Both

<b>-d [path]</b>	DataDirectory	This designates the directory where RadiusNT reads the <i>users</i> , <i>clients</i> , <i>dictionary</i> and <i>passwd</i> files.
<b>-I[#]</b>	IgnoreCase	Use this to ignore case when comparing the username and password. You can instruct RadiusNT to compare the username by specifying the number "1" or the password by specifying the number "2". Using the "-I" option by itself specifies <b>both</b> username and password case insensitive comparisons.
<b>-M[#] -o or -b</b>	Mode	By default, RadiusNT uses text mode because it reads all of its configuration from text files. The "-o" or "-b" options instruct RadiusNT to connect to an ODBC database to read all configuration information and to authenticate users from the database. The "-b" option allows RadiusNT to authenticate from <b>both</b> the <i>users</i> file and the database. Please note that the database is checked <b>first</b> . This option also sends accounting information to both. The "-M" parameter allows you to set text mode (0), ODBC (1) or both (2).
<b>-n [DataSource]</b>	ODBCDataSource	If RadiusNT is in ODBC mode (-o or -b), it will use the specified ODBC DataSource Name rather than the default of "radius".
<b>-p0 [port]</b>	AuthPort	This option designates the ports RadiusNT should "listen" to for Authentication requests. This will default to the port specified in the RadiusNT Administrator, or port 1812.
<b>-p1 [port]</b>	AcctPort	This option designates the ports RadiusNT should "listen" to for Accounting requests. This will default to the port specified in the RadiusNT Administrator, or port 1813.
<b>-P[#]</b>	Proxy	If you have a Enterprise & Professional version only license, this option will allow both Authentication and Accounting proxy. While the default is both, you can enable just authentication (1) or accounting (2).

-R[#]	Options	<p>This option is used to set many flags or options within RadiusNT, mostly dealing with concurrency control. Simply add up all options that you wish to use. For example, if you want Concurrency Lockout and Enable Time Banking, use -R5.</p> <table border="0"> <tr> <td>1</td><td>Concurrency Lockout</td> <td>2</td><td>Manual ServerPorts Update</td> </tr> <tr> <td>4</td><td>Enable Time banking</td> <td>8</td><td>Manual SubAccounts Update</td> </tr> <tr> <td>16</td><td>No clear clear by AcctStatusType</td> <td>32</td><td>Ascend Max Time Support</td> </tr> <tr> <td>64</td><td>Reserved</td> <td>128</td><td>External Password Replace</td> </tr> <tr> <td>256</td><td>Server Port Access</td> <td>512</td><td>Account Start Records Only</td> </tr> <tr> <td>1024</td><td>User Login Triggers</td> <td>2048</td><td>Allow any request type</td> </tr> <tr> <td>4096</td><td>Server DNIS Access</td> <td>8192</td><td>Check RadRejects</td> </tr> <tr> <td>16384</td><td>Disable class support.</td> <td>32768</td><td>No clear by AcctStatusType</td> </tr> </table> <p>Note: The RDBMS type is automatically sensed from the ODBC driver and the MS Access mode option above has been deselected. However, you may wish to force MS Access mode if you are using an ODBC database that is compatible with MS Access rather than SQL Server (the default).</p>	1	Concurrency Lockout	2	Manual ServerPorts Update	4	Enable Time banking	8	Manual SubAccounts Update	16	No clear clear by AcctStatusType	32	Ascend Max Time Support	64	Reserved	128	External Password Replace	256	Server Port Access	512	Account Start Records Only	1024	User Login Triggers	2048	Allow any request type	4096	Server DNIS Access	8192	Check RadRejects	16384	Disable class support.	32768	No clear by AcctStatusType
1	Concurrency Lockout	2	Manual ServerPorts Update																															
4	Enable Time banking	8	Manual SubAccounts Update																															
16	No clear clear by AcctStatusType	32	Ascend Max Time Support																															
64	Reserved	128	External Password Replace																															
256	Server Port Access	512	Account Start Records Only																															
1024	User Login Triggers	2048	Allow any request type																															
4096	Server DNIS Access	8192	Check RadRejects																															
16384	Disable class support.	32768	No clear by AcctStatusType																															
-S	ExtSupport	This option is used to select External Authentication support.																																
-T	ProxyTimeout	If you have an Enterprise or Professional license, this option will allow setting the timeout for Authentication and Accounting proxy. The default timeout is 30 seconds.																																
-u [file]	UsersFile	This option specifies an alternate filename to read in the <i>users</i> file from. This is <b>not</b> a full path and should <b>only</b> be a filename. The file is looked for in the DataDirectory.																																
-v		Use this option to display RadiusNT version information.																																
-x[level]	Debug	<p>The debug mode is typically used directly from the command line to diagnose problems. Debug options are:</p> <table border="0"> <tr> <td>1</td><td>Information</td> <td>2</td><td>User Debug</td> <td>4</td><td>ODBC Debug</td> </tr> <tr> <td>8</td><td>File Debug</td> <td>16</td><td>SNMP Debug</td> <td>32</td><td>Smart cache debug</td> </tr> <tr> <td>64</td><td>Memory debug</td> <td></td><td></td> <td></td><td></td> </tr> </table> <p>Simply add up the options you want. For instance, if you want Information and ODBC debugging, you would use -x5. The common full debug mode is -x15.</p>	1	Information	2	User Debug	4	ODBC Debug	8	File Debug	16	SNMP Debug	32	Smart cache debug	64	Memory debug																		
1	Information	2	User Debug	4	ODBC Debug																													
8	File Debug	16	SNMP Debug	32	Smart cache debug																													
64	Memory debug																																	
-X		This option specifies packet level debugging.																																

The following registry entries do **not** have corresponding command line options:

Registry	Description

<b>License</b>	This entry displays the RadiusNT license.
<b>CompanyName</b>	This entry displays the company name that is licensed for RadiusNT use.
<b>DBM</b>	<p>This entry shows the ODBC RDBMS mode that RadiusNT will run in. It determines the style of SQL statements and procedures that are used. Please see the ODBC <a href="#">Supported Database Systems</a> section for more details. Modes include the following:</p> <p>0 Automatic detection    1 Microsoft SQL Server  2 Microsoft Access        3 Sybase SQL Server  4 Oracle Database Server</p>
<b>ODBCTimeout</b>	This entry displays the number of seconds RadiusNT will wait for an ODBC query to return (default is 15 seconds).
<b>Username</b>	This shows the username that RadiusNT will use to make the ODBC connection.
<b>Password</b>	This shows the password that RadiusNT will use to make the ODBC connection.
<b>Logfile</b>	This entry shows what log file is used for RADIUS authentication requests (and accounting requests if an accounting logfile is not specified).
<b>AcctODBCDataSource</b>	RadiusNT uses this DNS name, rather than the default of "radius", for the Accounting ODBC connection. Please note that this is only applicable in ODBC multi-thread mode.
<b>AcctUsername</b>	This entry displays the username RadiusNT will use to make the ODBC connection to the alternate ODBC datasource for accounting.
<b>AcctPassword</b>	This entry displays the password RadiusNT will use to make the ODBC connection to the alternate ODBC datasource for accounting.
<b>AcctLogfile</b>	This entry shows the filename in which the Accounting Logs will reside. This is typically used in text only mode.
<b>TrimName</b>	When this entry is set to 1, RadiusNT trims spaces around a name, and also truncates a name when a space is encountered. Normally RadiusNT tries to authenticate the user with <b>exactly</b> what the Username attribute contains.
<b>IPCheck</b>	When this entry is set to 0, if RadiusNT does not have a specific entry for the client making the request, it allows the request and uses the Global Secret specified below. This should <b>only</b> be used for testing or emergency reasons since it allows <b>anyone</b> who knows your global secret to make requests to your RadiusNT server.



<b>GlobalSecret</b>	This displays the global secret to use when IPCheck is set to 0 and the client is unknown.
<b>ProxyTimeout</b>	This entry shows the number of seconds RadiusNT will store a proxy request in memory before it clears (default is 30 seconds).
<b>ProxyID</b>	RadiusNT will replace the NAS-Identifier with this IP Address when sending a proxy request. This can "hide" the NAS-Identifier from the Proxy Server.
<b>TestDatabaseSecs</b>	Radius opens a connection to every datasource available to it, each for the number of seconds shown. If the connection fails, the datasource is marked unavailable ( <b>Enterprise &amp; Professional version only</b> ).
<b>CacheUserModifyCheckSecs</b>	This entry displays how often (in seconds) the cache database is checked for modifications and updated with fresh information.
<b>CacheUserPrefetchLastDays</b>	Upon startup, this will load users who have called within the specified number of days into the smart cache.
<b>CacheDoubleCheck</b>	<p>The Double Check option queries the database when the cache copy would otherwise reject an authentication request (for example, in the case of an expired account, bad password or when there is no time left in the time bank). This usually isn't necessary, as account changes are regularly synchronized with the database.</p> <p>0/1 Enabled    2 Disabled</p>
<b>CacheUserNoQueryOnFailSecs</b>	<p>This entry displays the interval (in seconds) to override checking the database (for new information that may cause the authentication to succeed) to prevent extra database queries.</p> <p>For example: Consider an ISDN user with an expired account and the Cache Double Check Option enabled. Each channel of the ISDN router might try once a second to reconnect, causing unneeded database work.</p>
<b>CacheUserForceUpdateDays</b>	Lists the refresh interval for any user who has been in the cache without being updated. This makes certain that any inconsistencies cannot exist for more than the number of days specified.
<b>AcctMaxHoldTime</b>	RADIUS can buffer accounting information and send a batch of multiple requests to the database server as a single query. This reduces overall load on the database, but at the expense of added latency. This option will limit the number of seconds any single piece of accounting data can be queued in a batch. Note: Set this entry low (a few seconds) if you're doing time banking or require concurrent login checking. ( <b>Enterprise &amp; Professional version only</b> )

<b>SyslogIP</b>	<p>Both error and informational messages can be directed to a syslog server by specifying an IP address. The following are facility codes:</p> <p>[DAEMON] Messages not specific to authentication or accounting  [LOCAL0] Authentication specific messages  [LOCAL1] Accounting specific messages</p>
<b>CacheServerAccessUpdateMins</b>	<p>This entry shows the Server-Access cache update interval (in minutes).</p>
<b>CacheRootDirectory</b>	<p>This entry shows the directory where RadiusNT stores cache data.  <b>(Enterprise &amp; Professional version only)</b></p>
<b>CacheRoamServerUpdateMins</b>	<p>This shows the Roam Server cache update interval (in minutes).  <b>(Enterprise &amp; Professional version only)</b></p>
<b>MaxAcctSpoolItems</b>	<p>If the accounting database is too slow or in a down state, the accounting data can be stored in memory, then moved to the accounting database as conditions improve. Please note that every 25,000 items require approximately 2MB of memory.</p> <p>New additions will be dropped if Max Spooled Items already exist in memory. RadiusNT will not ACK the accounting packet, giving another RADIUS server the opportunity to respond. <b>(Emerald-only edition limited to 500)</b></p>
<b>CacheAccountTypesUpdateMins</b>	<p>This entry shows the interval specified for updating of the service types cache.</p>
<b>AgentxSocket</b>	<p>This displays the directory of the Agentx domain socket, the pathname of the directory where the master agent's (snmpd) UNIX domain socket endpoint is located. Usually this can be left blank to accept the default of /var/agentx.</p> <p>If errors are logged in regard to initializing the Agentx library, make sure the directory exists and both programs have the proper permissions to access the directory. <b>(UNIX Enterprise &amp; Professional version only)</b></p>
<b>CacheWriteMins</b>	<p>If cache persistence is enabled, this option allows you to specify how often the contents of the cache database should be written to disk to allow starting RADIUS to a useable state when no authentication database is available. <b>(Enterprise &amp; Professional version only)</b></p>

<b>DeferredMemFreeMins</b>	Memory used to update account information is not immediately freed. Instead it is placed in a queue to be removed later. This option controls how often the delete process is run. Please note that any object less than 5 minutes old <b>cannot</b> be removed. If you are performing Time Banking and do not have ample memory, set this low (a couple of minutes). In most cases the default value is optimal. <b>(Enterprise &amp; Professional version only)</b>
<b>DatabaseTimeOffsetDays</b>	This entry displays the Database Time Offset Update (in days). This option controls how often the authentication and accounting databases are queried and computes a time offset from the local clock for various authentication and accounting functions (such as time-stamping call records or checking to see whether an account has expired).
<b>CacheDNISUpdateMins</b>	This entry displays the DNIS cache update interval (in minutes).
<b>CacheUserDeleteAfterUnusedDays</b>	This entry shows the number of days specified before unrequested accounts will be removed from the cache.
<b>NVFlag</b>	This flag shows whether the option to have the accounting and authentication cache database regularly written to disk is enabled. It allows RadiusNT/X to recover after being restarted when no valid authentication data sources exist. <b>(Enterprise &amp; Professional version only)</b> The flags are as follows:
<b>TacHost</b>	1 Accounting    2 Authentication This is the address of the Tacacs server to authenticate against. <b>(Enterprise version only)</b>
<b>TacSecret</b>	This is the Tacacs secret key. Leave it blank to disable password encryption. <b>(Enterprise version only)</b>
<b>TacTimeout</b>	This shows the Tacacs query timeout (in seconds). <b>(Enterprise version only)</b>
<b>TacPort</b>	This is the Tacacs port number of service name (default is port 49). <b>(Enterprise version only)</b>
<b>AuthMethods</b>	This is the space delimited - ordered list, including an optional domain of authentication methods.  Ex: (ldap\ldapdomain mycustom.dll\mydomain unix tacacs\tacdomain ldap tacacs) <b>(Enterprise &amp; Professional version only)</b>
<b>ExtLibDirectory</b>	This is the directory to load external authentication libraries from. If no directory is specified, the "radius" directory is used.

<b>ProxyCheckInterval</b>	This displays the number of seconds between requests to a down proxy server to see if it is responding again.
<b>ProxyDown</b>	This displays the number of seconds elapsed between detecting a timeout and considering the proxy server to be down.
<b>DefenderHost</b>	This is a list of Defender servers for authentication. Secondaries are used only when the primary server is not available. <b>(Enterprise version only)</b>
<b>DefenderPort</b>	The Defender port number <b>(Enterprise version only)</b>
<b>DefenderTimeout</b>	The number of seconds to wait for a response from the DMS. <b>(Enterprise version only)</b>
<b>DefenderDown</b>	This is the length of time (in seconds) to wait between detecting a timeout and assuming all Defender servers are down. At this point, RadiusNT/X will cease attempts to reconnect. <b>(Enterprise version only)</b>
<b>DefenderAgentID</b>	The AgentID of the DMS session. Defaults to RadiusNT on the Win32 platform and RadiusX on UNIX platforms. <b>(Enterprise version only)</b>
<b>SWECHost</b>	The IP Address of the Safeword authentication server. <b>(Enterprise version only)</b>
<b>SWECPort</b>	The port number <b>(Enterprise version only)</b>
<b>LDAPHost</b>	The list of LDAP Servers to authenticate against. Secondary servers are used only if the primary server is not available. <b>(Enterprise version only)</b>
<b>LDAPPort</b>	The LDAP Port to bind to. This option applies to standard LDAP and LDAP over SSL. If left blank, the default ports are used (Emerald-only:389 SSL:636). <b>(Enterprise version only)</b>
<b>LDAPSSLCert</b>	The Netscape Communicator 4.x cert7.db Client certificate file. Used to determine whether it can trust the certificate sent from the server. Specifying a file or directory where cert7.db can be found enables SSL Encryption. <b>(Enterprise version only)</b>
<b>LDAPSearch</b>	The search string used to search accounts or bind as a user. \$login - replaced with current login name. \$domain - replaced with current domain name. <b>(Enterprise version only)</b>
<b>LDAPTimeout</b>	The Directory Search timeout interval (in seconds). When the limit is reached, the LDAP module returns "ignore", giving another authentication method a chance to succeed. <b>(Enterprise version only)</b>

<b>LDAPSearchBind</b>	The DN (Distinguished Name) to bind to the server in order to find the correct DN to authenticate and retrieve user attributes. This is normally left blank to allow anonymous connections. <b>(Enterprise version only)</b>
<b>LDAPSearchPassword</b>	If LDAPSearchBind is set, this is the password used to validate the search bind request. This is normally left blank to allow anonymous connections. <b>(Enterprise version only)</b>
<b>LDAPBaseDirectory</b>	This is the base directory under which to search for matching user entries. <b>(Enterprise version only)</b>
<b>LDAPAccountType</b>	The LDAP attribute used to specify a Database Account Type (Profile). If left blank, this feature is disabled. <b>(Enterprise version only)</b>
<b>LDAPLoginLimit</b>	The LDAP attribute used to specify how many concurrent logins the user is allowed to have. If left blank, this feature is disabled and login limit checking is disabled for LDAP authentication. <b>(Enterprise version only)</b>
<b>LDAPScope</b>	This entry determines how deep to search the directory tree for the user (In this example [ ]s represent the Base DN). 1 - One Level Deep (ex: uid=neila,[ou=moon,o=nasa]) 2 - Sub-Tree (ex: uid=neila,ou=moon,[o=nasa]) <b>(Enterprise version only)</b>

## Chapter 8 – ODBC DATABASE SCHEMA

One of the most powerful features of RadiusNT/X is its ability to integrate with a back-end RDBMS. RadiusNT/X accomplishes this through ODBC. Many features available in RadiusNT/X ODBC mode are not available in Text mode, simply because the back-end RDBMS allows RadiusNT/X to easily keep track of and manage a larger user base over a distributed, fail-safe environment. Compound rules can be defined in the database to alter RadiusNT/X's authentication behavior. This chapter details what is available.

### Table Layout

RadiusNT/X requires many different tables. The following is a list of those tables along with field descriptions. Please note that an asterisk (\*) with a field denotes a field that is only used or active if a flag or option is set; these fields are **not** enabled by default.

Required Table	Field	Type	Description
<b>AccountTypes</b>			The AccountTypes table is not directly used for RadiusNT/X, but is used as a lookup table for the Service type fields in the SubAccounts and RadATConfigs tables to identify user account service types.
	SortOrder	int	The order in which subaccounts are displayed to the Radius user.
	AccountTypeID	int	Account type identifier (IDENTITY)
	AccountType	varchar(15)	Name of the Service Type.
	Description	varchar(100)	Full description of the Service Type.
	DNISGroupID	int	The DNIS Group that the Service Type is allowed to login to (related DNISGroupID from DNISGroup table). If NULL, then no DNIS group is enforced for this Service Type.
<b>Calls</b>			
	NASPort	varchar(10)	NAS Port the call came in on.
	AcctDelayTime	int	How many seconds the client has been trying to send this record for, and can be subtracted from the time of arrival on the server to find the approximate time of the event generating this Accounting-Request. (Network transit time is ignored.)

Required Table	Field	Type	Description
	AcctSessionID	varchar(16)	NAS generated unique ID for the call.
	UserName	varchar(40)	Username of caller.
	FramedAddress	varchar(16)	Address configured for the user. It may be used in Access-Accept packets. It may be used in an Access-Request packet as a hint by the NAS to the server that it would prefer that address, but the server is not required to honor the hint.
	CallDate	smalldatetime	Date of Call
	NASIdentifier	varchar(16)	Identifier for the NAS (generally the NAS IP address)
	ConnectInfo	varchar(32)	Customer (Modem protocol/baud) connection information
	AcctTerminateCause	smallint	How the session was terminated (integer codes)
	AccountID	int	Subaccount identifier of user (if known)
	ServerID	int	Server identifier
	CallerID	varchar(15)	Phone number the user called
<b>DNISGroups</b>			Defines each DNIS group that an Service Type is allowed to use.
	DNISGroupID	int	Group identifier (IDENTITY)
	Description	varchar(45)	Full description of the DNIS Group.
	DNISGroup	varchar(25)	Name of the DNIS Group
<b>DNISNumbers</b>			Defines each DNIS number that is associated to a DNIS group
	DNISGroupID	int	Related DNIS group identifier (foriegn key from DNISGroup table)
	DNISNumber	varchar(10)	The DNIS number as reported by the Radius client
<b>Licenses</b>			Holds Radius NT/X license information
	LicenseID	varchar(40)	License key provided by IEA Software upon purchase
	Company	varchar(40)	The company name in the license. Please note that this is case sensitive and must match exactly what is provided with the license key itself.

Required Table	Field	Type	Description
<b>MapAttributes</b>			This table is used to map internal attributes from custom external systems (created with the External Auth API or LDAP support) to Radius (rfc2138) attributes
<b>MapAttributes</b>			
	Attribute	varchar(32)	
	ReplyType	smallint	
	RadVendorID	int	Radius Vendor ID of mapped radius attribute
	RadAttributeID	int	The Radius attribute mapped to
	RadVendorType	int	If radius attribute is vendor-specific (RadAttributeID = 26), then this denotes a vendor type, otherwise the value should be NULL or 0.
	MapAttribute	varchar(32)	Identifier of external attribute
	MapType	int	
	Description	varchar(255)	
<b>MapValues</b>			This table is used to track the values of custom external systems attributes (created with the External Auth API or LDAP support) mapped to Radius (rfc2138) attributes
	RadValue	int	Radius attribute value (number)
	Description	varchar(255)	Description of external attribute value
	MapAttribute	varchar(32)	
	Value	varchar(32)	Attribute value (number)
<b>MasterAccounts</b>			Master account information (first tier information)
	StartDate	datetime	Date the account became, or will become, active
	CreateDate	datetime	Date the account was created
	Active	smallint	Account active flag  0 -- not active, will not be authenticated 1 - active
	Operator	varchar(32)	Operator that created the account
	Comments	text	Account comments



Required Table	Field	Type	Description
	LastModifyUser	varchar(32)	Username that last modified the account record (if available)
	OverDue	smallint	How many days overdue to allow for all accounts.
	LastName	varchar(25)	Customer last name
	CancelDate	datetime	Date the account will become non-active or terminated
	FirstName	varchar(25)	Customer first name
	LastModifyDate	datetime	Date the master account record was last modified
<b>Operators</b>			Table of valid system operators
	LastName	varchar(25)	Operator's last name
	OperatorID	int	Operator identifier (IDENTITY)
	Email	varchar(40)	Operator's email address
	Password	varchar(15)	Operator's password
	Operator	varchar(15)	Operator's system username
	FirstName	varchar(25)	Operator's first name
<b>RadATConfigs</b>			RADIUS Reply attributes for AccountTypes
	RadCheck	smallint	
	LastModifyDate	datetime	Date record last modified/updated
	RadATConfigID	int	RadATConfig identifier (IDENTITY)
	RadAttributeID	int	Associated Radius attribute (related RadAttributeID from RadAttributes table).
	Value	int	Used for integer attribute types.
	RadVendorType	int	If this attribute is a vendor specific attribute (radattribute = 26) then this denotes a vendor type. Otherwise the value should be NULL or 0
	AccountTypeID	int	Associated Service Type (related AccountTypeID from AccountType table).
	Tag	int	For attributes supporting it tag values allow grouping multiple attributes within a single radius response.

Required Table	Field	Type	Description
	RadVendorID	int	If this attribute is a vendor specific attribute (radattribute = 26) then this denotes a vendor id. Otherwise the value should be NULL or 0
	LastModifyUser	varchar(32)	User that last modified/updated this record
	Data	varchar(100)	Used for string, IP address, or date attribute types
<b>RadAttributes</b>			Stores the RADIUS dictionary information (possible attributes)
	RadVendorID	int	If this attribute is a vendor specific attribute (radattribute = 26) then this denotes a vendor id. Otherwise the value should be NULL or 0.
	RadVendorType	int	
	ReplyType	int	Reply type  0 Accounting Only 1 Reply only 2 Check only 3 Check & Reply
	AliasAttributeID	int	Radius attribute (from RadAttributes table) of similar Radius attribute for logging of accounting data.
	RadAttributeType	int	RADIUS attribute type  0 string 1 32-bit integer 2 IP address 3 Date 4 Ascend Binary  10 Tag String 11 Tag 32-bit integer 12 Tag IP address 13 Tag Date
	Name	varchar(32)	Name of the radius attribute
	RadAttributeID	int	Radius Attribute identifier (IDENTITY)
<b>RadConfigs</b>			RADIUS Reply attributes for individual subaccounts
	Data	varchar(100)	Used for string, ip address or date attribute types

Required Table	Field	Type	Description
	AccountID	int	Associated subaccount (related AccountID from SubAccounts table).
	RadVendorID	int	If this attribute is a vendor specific attribute (radattribute = 26) then this denotes a vendor id. Otherwise the value should be NULL or 0.
	LastModifyDate	datetime	Date this record was last updated
	Value	int	Used for integer attribute types
	Tag	int	
	RadCheck	smallint	attribute type  0 denotes a normal reply attribute non-zero denotes this is a check attribute
	LastModifyUser	varchar(32)	User that last modified this record
	RadVendorType	int	If this attribute is a vendor specific attribute (radattribute = 26) then this denotes a vendor type. Otherwise the value should be NULL or 0.
	RadConfigID	int	RadConfig identifier (IDENTITY)
	RadAttributeID	int	Associated Radius attribute (RadiusAttributeID from RadAttributes table).
<b>RadIPAccountTypes</b>			Controls Service Type access to IP & ServerGroups for IP Pooling.
	AccountTypeID	int	Associated with Service Type (related AccountTypeID from AccountType table).
	RadIPAccountTypeID	int	RadIPAccountType identifier (IDENTITY)
	ServerGroupID	int	Associated Server Group (related ServerGroupID from ServerGroup table).
	RadIPGroupID	int	Associated RadIP Group (related RadIPGroup from RadIPGroup table).
<b>RadIPAddresses</b>			IP Pool - Address and checkout status
	IPAddress	varchar(16)	Associated IPAddress
	NASPort	varchar(10)	NAS Port associated with server/port.

Required Table	Field	Type	Description
	RadIPGroupID	int	Associated Radius IP Group (related RadIPGroupID from RadIPGroup table).
	ServerID	int	Associated Server (related ServerID from Servers table).
	State	int	Address checkout state  0 Available 1 Auth In Use 2 Acct In Use
	LastUsed	datetime	Date this IP last checked out
<b>RadIPGroups</b>			Groups individual IP Addresses into a group of addresses used in IP pooling
	RadIPGroupID	int	RadIPGroup Identifier (IDENTITY)
	RadIPGroup	varchar(32)	Name of RadIPGroup
<b>RadLogMsgs</b>			Provides text descriptions of the RadLogMsgID numbers in the RadLogs table
	Description	varchar(50)	Description of Log Message
	Severity	int	Error severity of associated Log Message
	RadLogMsgID	int	Log Message Identifier (see ODBC logging)
<b>RadLogs</b>			Contains log information if RadiusNT/X is run in either ODBC or Both mode
	Data	varchar(50)	Additional data, dependent on the Log Message ID. Note: The ServerPorts table contains information about each port available for a NAS. This is required for concurrency control and for monitoring who is online.
	CallerID	varchar(15)	The associated Caller ID of log entry
	LogDate	smalldatetime	The log message date
	UserName	varchar(40)	The associated username (if exists) of log entry
	RadLogMsgID	int	Log Message Identifier (type of log message)
	NASIdentifier	varchar(16)	The associated NAS Identifier of log entry

Required Table	Field	Type	Description
	NASPort	varchar(10)	The associated NAS Port of log entry
<b>RadProxyAttributeGroups</b>			Used to associate a group of RadProxyAttributes with a proxy server
	RadProxyAttributeGroupID	int	Group Identifier (IDENTITY)
	RadRoamServerID	int	Server to proxy matching requests
	ProxyGroupName	varchar(32)	Identifying name of the Proxy group
	Priority	int	
	Description	varchar(255)	Description of the proxy group
<b>RadProxyAttributes</b>			Holds attributes and value pairs for proxying of radius requests
	RadAttributeID	int	Related Radius attribute (RadAttributeID from RadAttribute table)
	RadVendorID	int	Related Radius attribute vendor
	SearchType	smallint	type of rules used in searching for matching attribute/values  1 string, 2 substring, 3 equal, 4 less than, 5 greater than
	RadProxyAttributeGroupID	int	Associates a group of attributes to a proxy server (foreign key to RadProxyAttributeGroups table)
	String	varchar(253)	Value to search on
	RadVendorType	int	If attribute is vendor-specific (RadAttributeID = 26), then this denotes a vendor type, otherwise the value should be NULL or 0.
<b>RadRejects</b>			Contains a list of attribute/value information for RadiusNT/X to immediately reject a request.
	RadVendorID	int	
	Value	int	Used for integer attribute types.
	RadAttributeID	int	Associated Radius attribute (related RadAttributeID from RadAttribute table).
	RadVendorType	int	

Required Table	Field	Type	Description
	Data	varchar(100)	Used for string, IP address or date attribute types.
	RadRejectID	int	RadReject identifier (IDENTITY)
<b>RadRoamDomains</b>			Contains the domains that RadiusNT can proxy requests for and which Roam Server the request should be forwarded to.
	Priority	int	The Roam Server's priority in this domain
	RadRoamServerID	int	Which Rad Roam Server this entry is associated with (RadRoamServerID from RadRoamServer table).
	AccountTypeID	int	If this option is NULL, then RadiusNT/X will ignore the attributes returned in the proxy reply and return the set of attributes associated to the Service Type.
	Domain	varchar(32)	Roam domain in the login (user@domain).
	RadRoamDomainID	int	Rad Roam Domain identifier (IDENTITY)
<b>RadRoamServers</b>			Contains information regarding Roam servers which RadiusNT can proxy requests to.
	RadRoamServerID	int	Radius Roam Server identifier (IDENTITY)
	AuthPort	int	Port number to send authentication request to (defaults to 1645). Please note that if this field is 0 or NULL, authentication requests will not be forwarded to this server.
	Retries	int	Number of retries (not currently used)
	AcctPort	int	Port number to send accounting requests to (defaults to 1646). Please note that if this field is 0 or NULL, accounting requests will not be forwarded to this server.
	Secret	varchar(16)	Shared Secret for requests going to roam server.
	Server	varchar(32)	Name of the Roam Server
	StripDomain	smallint	Strip the domain form the username before sending request.

Required Table	Field	Type	Description
	Timeout	int	Number of seconds to wait for a reply.
	RateMax	int	Maximum number of requests per second this roam server is allowed to receive.
	IPAddress	varchar(16)	IP address of the Roam Server
<b>RadTriggers</b>			Contains program information for RadiusNT/X which can be executed when the associated account logs in (accounting start record is received).
	RadTriggerID	int	Trigger identifier (IDENTITY)
	FileName	varchar(64)	Executable program or file to run
	AccountID	int	Trigger associated to this subaccount id
	TriggerType	int	Type of trigger (currently not used)
	Directory	varchar(128)	Working directory for the program or file
	Parameters	varchar(64)	parameter(s) for the program or file
<b>RadValues</b>			Lookup values for some of the RADIUS attributes.
	RadVendorType	int	
	Name	varchar(25)	Attribute value name
	RadVendorID	int	If this attribute is a vendor specific attribute (radattribute = 26) then this denotes a vendor id. Otherwise the value should be NULL or 0
	RadAttributeID	int	Associated radius attribute (RadAttributeID from RadAttributes table).
	Value	int	Attribute value number
<b>RadVendors</b>			Radius Vendor Ids
	Name	varchar(32)	Name of vendor
	RadVendorID	int	RadVendor identifier (industry/vendor specified)
<b>ServerAccess</b>			Contains information on which AccountTypes can access which Ports
	AccountTypeID	int	What Service Type this entry is associated with (related AccountTypeID from AccountType table).

Required Table	Field	Type	Description
	MaxSessionLength	int	The maximum session length allowed.
	ServerID	int	What Server this entry is associated with (related ServerID from Servers table).
	StopTime	int	The stop time allowed to login, in minutes from midnight.
	StartTime	int	The start time allowed to login, in minutes from midnight
	Port	varchar(10)	Which port that this record is associated with (related Port from ServerPorts table).
<b>ServerGroups</b>			Allows servers to be grouped for IP pooling
	ServerGroup	varchar(32)	Server Group name (description).
<b>ServerPorts</b>			Contains information about each port available for a NAS. This is required for concurrency control and for monitoring who is online.
	AccountID	int	The RadiusNT subaccount id of the last user of the port (if available).
	SNMPUser	varchar(64)	SNMP Object Identifier (OID) string for the SNMP concurrency checking.
	MaxSessionTime	int	The maximum session time allowed on the port.
	IPAddress	varchar(16)	The IP address of the last user on the port.
	ServerID	int	Which server this port is associated with (related serverid from Servers table).
	UserName	varchar(40)	The last username that used the port.
	Port	varchar(10)	The port number.
	CallDate	smalldatetime	The call date of the last user on the port.
	CallerID	varchar(15)	The CallerID of the last user of the port.
	AcctStatusType	smallint	The status of the last user on the port.
	AcctSessionID	varchar(16)	The NAS AccountSessionID value of the last user on the port.
	FramedAddress	varchar(16)	The Framed Address of the last user on the port.



Required Table	Field	Type	Description
	ConnectInfo	varchar(32)	The Connect Information from the NAS for the last user of the port.
<b>Servers</b>			RADIUS client information
	ServerID	int	Server identifier (IDENTITY)
	ServerGroupID	int	Associated Server Group identifier (foreign key from ServerGroup table)
	Secret	varchar(16)	The Shared Secret for the RADIUS client
	Comments	text	Optional comments regarding the server
	IPAddress	varchar(16)	IP address of RADIUS client
	RadRoamServerID	int	Optional Roam Server to unconditionally forward all requests to. Set to NULL (default) for normal user-based proxy.
	ServerType	int	Type of server
	Community	varchar(16)	SNMP Community for the server.
<b>ServerTypes</b>			Tracks the types of servers available. This information is primarily used for SNMP Concurrency Checking.
	Vendor	varchar(32)	Vendor identifier
	SNMPType	int	Associated SNMP Type
	ServerType	int	Server Type identifier
	Model	varchar(32)	Server model
<b>SubAccounts</b>			The subaccount/services associated with the Master Account (second tier information).
			Note: There may be several subaccount records associated with each Master Account record.
	FirstName	varchar(25)	The first name of the subaccount user
	AccountTypeID	int	The Service Type of the service
	CustomerID	int	Associated Master account identifier
	LastName	varchar(25)	The last name of the subaccount user
	Operator	varchar(32)	The operator which created this subaccount record.

Required Table	Field	Type	Description
	Password	varchar(16)	The password of the subaccount user
	LastModifyDate	datetime	The date this record was last modified.
	LastModifyUser	varchar(32)	The username that last modified this record (if available)
	Login	varchar(32)	The login id for the subaccount user
	Email	varchar(40)	the email address of the subaccount user
	Active	smallint	Subaccount active flag  0 -- not active, will not be authenticated 1 - active
	LastUsed	datetime	The last date that the user logged in, NULL if this is not being tracked. This field is used by the RadiusNT/X caching system to preload recently authenticated users into the cache database.
	ExpireDate	datetime	The date this subaccount will expire. If NULL, the subaccount will not expire.
	AccountID	int	Subaccount identifier (IDENTITY)
	TimeLeft	int	The login time left (minutes) for the subaccount. This should be set to NULL if the user has no time limitations.

### ***Inside the Database***

The key to shaping RadiusNT/X to perform as you wish lies in understanding the RadiusNT/X database. The next section describes common operating procedures and assumes that you have a general understanding of databases overall.

### ***Authentication Process***

When RadiusNT/X receives an incoming authentication request, the following steps are performed to authenticate the user:

1. First, there is a check to see if a record exists in the SubAccounts table (and a related record in MasterAccounts via the CustomerID field) with either a login or e-mail field matching the username attribute in the request. The active flag in both the SubAccounts and MasterAccounts table **must not** be 0.
2. If no match is found, RadiusNT/X sends a reject (NACK).
3. If the requested password does not match the database password (with the proper case check), RadiusNT/X sends a reject.
4. If the saExpireDate Field is not NULL and the SubAccount saExpireDate plus Extension is before the current date, then RadiusNT/X sends a reject. Please note that this is **only** applicable to SQL Server or Sybase, as MS Access or Oracle does not support this.
5. If the saExpireDate is NULL and the MasterAccounts maExpireDate plus Extension and Overdue is before the current date, then RadiusNT/X sends a reject.
6. If Time Banking is enabled and the SubAccount's TimeLeft field is not NULL and less than 1, RadiusNT/X sends a reject.
7. If Concurrency Checking is enabled, and the user is listed in the ServerPorts table (with more entries than they are allowed), RadiusNT/X sends a reject.
8. If Server Access Checking is enabled, and the Service Type does not have an entry in the ServerAccess table for the port the user is logging into, RadiusNT/X sends a reject.
9. If there are matching records in the RadConfigs table for the user's AccountID, RadiusNT/X sends an ACK with them for the reply attributes.
10. If there are matching records in the RadATConfigs table for the user's Service Type, RadiusNT/X sends an ACK with them for the reply attributes.
11. If all of the steps above fail, RadiusNT/X sends a reject.

There are typically two ways to return a set of attributes for a user's authentication. If you want to return a set of attributes specific to a single user, then you need to add records to the RadConfigs table that correspond to the user's AccountID from the SubAccounts table. One of the primary uses of the RadConfigs table is to assign a specific IP address to a user, a unique set of routing information, or for specific user check attributes, such as Caller-ID.

The RadATConfigs table has attribute sets for each Service Type. This is where you place attributes for generic Service Types. Please note that you do **not** place **user specific** attributes in the RadATConfigs table.

If RadiusNT/X finds entries in the RadConfigs table that match the user's AccountID, it does **not** look to the RadATConfigs table for Service Type matching entries. Therefore, if you do add an entry in the RadConfigs table, you **must** add a **complete** set of attributes, since RadiusNT/X will not bring other attributes in.

### ***Accounting Process***

When RadiusNT/X starts, it reads the list of fields from the Calls table. This information is then cached in memory so RadiusNT/X will know which accounting attributes you want it to store.

When an accounting record is received by RadiusNT/X, it checks each attribute of the accounting request to see if there is a matching entry in the Calls table list that it read into memory. If it exists, the attribute is stored into the Calls table. Since RadiusNT/X does not check for a minimum set of records, it is possible for an error to arise while trying to insert the new record. However, this will not cause RadiusNT/X to stop working.

You may add columns to the Calls table to have RadiusNT/X store additional information. You will need to look at a data sample that will be stored in the column, then create an appropriate column. Each RADIUS attribute has a type associated with it, which dictates how RadiusNT/X will create the INSERT statement. For a type of string, IP address, or date/time, RadiusNT/X creates a character type (varchar). For an integer type (number), RadiusNT/X creates an integer type. The attribute types are stored in the RadAttributes tables.

**Additional ODBC procedures**

Please see [Chapter 9](#) for additional information on Advanced ODBC operations.

**Supported Database Systems**

Although RadiusNT/X is designed to use ODBC for database connectivity, not all ODBC drivers and SQL statements are the same across all database platforms. RadiusNT/X checks with the ODBC driver and automatically switches to support the RDBMS, if it has internal knowledge of the RDBMS (please see the list below). Otherwise, RadiusNT/X will **default** to Microsoft SQL server mode. Please note that you may modify the DBM registry entry to force RadiusNT/X into a particular mode if you are using an unknown database. Please contact support@iea-software.com if you would like to use RadiusNT/X with a database system that is not listed below. Note that there is a charge for assistance with non-supported databases.

**Microsoft SQL Server**

RadiusNT/X can be an Enterprise-wide solution when used with Microsoft SQL server. The inherent Client/Server design allows simultaneous multiple-client access to the database with no impact on performance. SQL Server is also suited to handle tables that can contain over one million records, and includes replication and fail-safe operations.

When RadiusNT/X is used with Microsoft SQL Server, almost all SQL statements are stored procedures. This provides maximum flexibility and control of the RadiusNT/X database interaction. Below is a list of stored procedures RadiusNT/X will use for authentication and accounting.

Name	Description
<b>RadCheckOnline</b>	Check to see how many concurrent on-line sessions a user has.
<b>RadCheckTrigger</b>	Check to see if an external trigger is available for this user.
<b>RadAtCache</b>	Retrieve a list of service attributes.
<b>RadServerAccessCache</b>	Retrieve server access information.
<b>RadDNISCache</b>	Retrieve DNIS information.
<b>RadGetProxyAttributes</b>	Fetch proxy attributes.
<b>RadGetRejects</b>	Retrieve reject attributes.
<b>RadRoamCache</b>	Retrieve roaming information.

<b>RadUserDefaults</b>	Retrieve a list of service RADIUS defaults.
<b>RadGetPoolConfigs</b>	Retrieve an IP Address from a RADIUS-managed address pool.
<b>RadSetTimeLeft</b>	Subtract a user's call times from his or her time bank.
<b>RadGetConfigs</b>	Retrieve a list of RADIUS default attributes for an AccountID.

Below is a list of the stored procedures that RadiusNT/X uses when packaged within the Emerald Management Suite. The standard RadiusNT/X stored procedures **can** be modified from the initial database design as long as the parameters and returned columns remain the same number and type, and you are **not** using Emerald.

```
CREATE PROCEDURE RadCheckOnline @UserName varchar(64), @accountid INT AS
Select Count(*) From ServerPorts (NOLOCK) Where ((@accountid IS NULL AND UserName=@UserName)
OR (@accountid IS NOT NULL AND AccountID=@accountid)) and AcctStatusType=1
GO
```

```
CREATE PROCEDURE RadCheckOnlineSNMP @UserName varchar(64), @accountid INT AS
SELECT s.IPAddress, st.SNMPTType, s.Community, sp.SNMPUser, sp.AcctSessionID
FROM Servers s (NOLOCK), ServerPorts sp (NOLOCK), ServerTypes st
WHERE ((@accountid IS NULL AND sp.UserName=@UserName)
OR (@accountid IS NOT NULL AND sp.AccountID=@accountid))
AND sp.AcctStatusType=1
AND s.ServerType = st.ServerType
GO
```

```
CREATE PROCEDURE RadRoamCache AS
Select Domain AS Label, Server, IPAddress, Secret, AuthPort, AcctPort,
Priority, Timeout, Retries, StripDomain, TreatAsLocal, at1.AccountType, rrs.RateTarget, rrs.RateMax
From RadRoamDomains rrd, RadRoamServers rrs, AccountTypes at1
Where rrd.RadRoamServerID = rrs.RadRoamServerID
AND rrd.AccountTypeID *= at1.AccountTypeID
UNION
Select rrd2.Domain AS Label, Server, IPAddress, Secret, AuthPort,
AcctPort, rrd.Priority, Timeout, Retries, StripDomain, TreatAsLocal,
at1.AccountType, rrs.RateTarget, rrs.RateMax
From RadRoamDomains rrd, RadRoamServers rrs, RadRoamDomains rrd2, AccountTypes at1
Where rrd.RadRoamServerID = rrs.RadRoamServerID
AND rrd.Domain = 'DEFAULT'
AND rrd.AccountTypeID = at1.AccountTypeID
UNION
Select CONVERT(VARCHAR(5),RadRoamServerID) AS Label, Server, IPAddress,
Secret, AuthPort, AcctPort, 0, Timeout, Retries, StripDomain,
TreatAsLocal, NULL, NULL, NULL
From RadRoamServers
Order By Label,Priority
GO
```

```

CREATE PROCEDURE RadCheckTrigger @AccountID int AS
Select FileName, Parameters, Directory, TriggerType from RadTriggers Where AccountID=@AccountID
GO

```

```

CREATE PROCEDURE RadServerAccessCache AS
Select MaxSessionLength, StartTime, StopTime, s.IPAddress, sa.Port, at1.AccountType
From Servers s, ServerAccess sa, AccountTypes at1
    WHERE s.ServerID = sa.ServerID
    AND sa.AccountTypeID = at1.AccountTypeID
GO

```

```

CREATE PROCEDURE RadDNISCache AS
Select at1.AccountType, dn.DNISNumber
FROM AccountTypes at1, DNISNumbers dn
    WHERE at1.DNISGroupID = dn.DNISGroupID
GO

```

```

CREATE PROCEDURE RadGetCacheUsers @date DATETIME, @flag SMALLINT AS
IF (@flag = 1)
BEGIN
SELECT sa.AccountID, sa.Login, sa.Password, NULL, at1.AccountTypeID, sa.LoginLimit, sa.TimeLeft * 60,
MasterExpire=CASE WHEN CancelDate IS NULL THEN NULL ELSE
DATEDIFF(Day,'19700101',CancelDate) END,
SubExpire=CASE WHEN ExpireDate IS NULL THEN NULL ELSE
DATEDIFF(Day,'19700101',DATEADD(Day,sa.Extension+ma.OverDue,ExpireDate)) END,
0 AS OverLimit, CASE WHEN sa.Active = 0 OR ma.Active = 1 THEN 0 ELSE 1 END AS StartDate
FROM SubAccounts sa, MasterAccounts ma, AccountTypes at1
    WHERE sa.CustomerID = ma.CustomerID
    AND sa.AccountTypeID = at1.AccountTypeID
    AND sa.Login <> "
    AND (sa.LastModifyDate > @date OR ma.LastModifyDate > @date)
END ELSE IF (@flag = 2)
BEGIN
SELECT sa.AccountID, sa.Login, sa.Password, NULL, at1.AccountType, sa.LoginLimit, sa.TimeLeft * 60,
MasterExpire=CASE WHEN CancelDate IS NULL THEN NULL ELSE
DATEDIFF(Day,'19700101',CancelDate) END,
SubExpire=CASE WHEN ExpireDate IS NULL THEN NULL ELSE
DATEDIFF(Day,'19700101',DATEADD(Day,sa.Extension+ma.OverDue,ExpireDate)) END,
0 AS OverLimit, CASE WHEN sa.Active = 0 OR ma.Active = 1 THEN 0 ELSE 1 END AS StartDate
FROM SubAccounts sa, MasterAccounts ma, AccountTypes at1
    WHERE sa.CustomerID = ma.CustomerID
    AND sa.AccountTypeID = at1.AccountTypeID
    AND sa.Login <> "
    AND (sa.LastUsed > @date OR sa.LastUsed IS NULL)
END
GO

```

```

CREATE PROCEDURE RadGetUser @user VARCHAR(64) , @password VARCHAR(32) AS
SELECT sa.AccountID, sa.Login, sa.Password, NULL, at1.AccountType, sa.LoginLimit, sa.TimeLeft * 60,

```

```

MasterExpire=CASE WHEN CancelDate IS NULL THEN NULL ELSE
DATEDIFF(Day,'19700101',CancelDate) END,
SubExpire=CASE WHEN ExpireDate IS NULL THEN NULL ELSE
DATEDIFF(Day,'19700101',DATEADD(Day,sa.Extension+ma.OverDue,ExpireDate)) END,
0 AS OverLimit, CASE WHEN sa.Active = 0 OR ma.Active = 1 THEN 0 ELSE 1 END AS StartDate
FROM SubAccounts sa, MasterAccounts ma, AccountTypes at1
    WHERE sa.CustomerID = ma.CustomerID
        AND sa.AccountTypeID = at1.AccountTypeID
        AND sa.Login = @user
GO

```

### ***Sybase SQL Server***

RadiusNT/X operates with Sybase the same as described above with Microsoft's SQL Server. The only difference lies within the scripts used to create the database itself, since there are slight differences between Microsoft's TSQL and Sybase's TSQL. A sample set of scripts for creating a database under Sybase is included with the RadiusNT/X distribution (radius4\_Sybase.sql).

### ***Microsoft Access***

Although Access is not suited to be used in multi-user environments or Enterprise-wide implementations, it is a very simple and powerful database for single server implementations. Please note that there is a significant performance issue when multiple users access the database. Since RadiusNT/X **must** have the database open at all times; this can become an issue as you grow. Please note that there are no built-in replication or fail-safe capabilities when using MS Access either.

RadiusNT/X will internally create all SQL Statements for MS Access. This limits the flexibility of the database design to follow the Emerald layout, and does limit the power or features of what RadiusNT/X can offer. An Access 7.0 database is included with the RadiusNT/X distribution, but you will not get the full functionality of Radius. Users are welcome to use this as a starting point to test or build additional RADIUS server features or options that you would like to use at your site.

### ***Oracle***

RadiusNT/X operation with Oracle is also very similar to as described above for Microsoft's SQL Server. Differences lie within the scripts used to create the database itself, some of the stored procedure implementations, and additional triggers and system objects. A set of scripts for creating a database under Oracle is included with the RadiusNT/X distribution (radius4\_oracle.sql).

## Chapter 9 – ADVANCED FEATURES

RadiusNT/X has several Advanced features, most of which are only available when running the server in *ODBC* or *Both* mode. The following sections explain these features.

### **Concurrency Control**

RadiusNT/X has a method of preventing a single user from logging in multiple times simultaneously. This is called concurrency control. To achieve this, RadiusNT/X uses the RADIUS Accounting records to dynamically maintain a list of who is currently on-line, tracked by server and port number. For the Concurrency Control feature to work, you **must** add records into the RadiusNT/X **ServerPorts** table to identify the Ports available on each NAS Server. Each ServerPorts entry must match the ServerID from the Servers table, **and** the Port column that matches the NAS-Port attribute that will be received within the RADIUS accounting packet. RadiusNT/X only **updates** the records of the ServerPorts table, and will not **create** them. Note: If need be, you can run RadiusNT/X in -x15 debug mode to view examples of the accounting packet NAS-Port numbers so you know how they should be entered within the ServerPorts table.

When RadiusNT/X receives an authentication request and Concurrency Control is enabled, it compares the number of entries in the ServerPorts table that match the username. Please note that ISDN or MPP users must be taken under special consideration. Concurrency Control may additionally restrict the number of channels a user can “bond” together into a single session. For instance, if you want an ISDN user to utilize two channels (128K), but want all other users to only be able to log in once, set everyone’s login limit to 1, except for the ISDN user, who should be set to 2.

Concurrency Control is not completely effective against MPP connections, when customers make simultaneous login requests. Since both authentication requests will be ahead of the first accounting request, both authentication requests will be successful. However, you **can** use the Port-Limit attribute to limit the number of MPP channels someone can bond together. Please note that the Port-Limit attribute is **not** the same as Concurrency Control, since it does not limit non-MPP connections. However, you can use both together to effectively control the number of logins.

If you are using a passive database system (one that runs in-context with RADIUS) where you cannot program the database system to do something based on a record insert, such as a trigger (e.g., MS Access)), you can instruct RadiusNT/X to manually update the ServerPorts table with the proper information by selecting the “Manual Calls Update” option in the ODBC configuration. This should not be used in a true RDBMS system, since you can setup a trigger to do this much more efficiently.

### **Time Banking**

The Time Banking feature allows you to specify a set number of minutes the user can be logged on (a cumulative block of time). Please note that this is not a recurring number. Once the number of minutes is diminished, you **must** manually add more minutes or the user will not be able to log on.

The Time Banking information is stored (in minutes) in the TimeLeft field of the SubAccounts table. If the field is NULL, the account does not use Time Banking. If the field is not NULL, RadiusNT/X returns the Session-Timeout attribute equal to the number of minutes specified. If the RADIUS client (NAS) supports



the Session-Timeout attribute, this will effectively only allow the user to be on-line for the exact number of minutes specified. Please check with your NAS vendor to be sure your NAS supports the Session-Timeout attribute before enabling Time Banking.

If you are using a passive database system, you can instruct RadiusNT to manually update the user's TimeLeft information. This option should **not** be used in a true RDBMS system, since you can set up a trigger to do this much more efficiently. Please note that Time Banking is **not** enabled by default. You **must** enable Time Banking under the **Advanced** option of the RadiusNT/X Administrator and then restart RadiusNT/X. In addition, you **must** have a NAS that supports the Session-Timeout attribute.

## **Server Access**

Server Access allows you to limit the ports a RadiusNT/X Service Type can log into. When Server Access is enabled, RadiusNT/X will search for an entry in the ServerAccess table that matches the ServerID, NASPort and AccountType of the authenticating user. If a match is found, access is granted. If a match is not found, the user is not allowed to log into the port. The NASPort field may be set to NULL, which then specifies that any Port is allowed for that NAS. This helps to minimize the number of records required in the ServerAccess table. Please note that Server Access is **not** enabled by default. You **must** enable Server Port Access under the **Advanced** option of the RadiusNT/X Administrator and then restart RadiusNT/X.

## **DNIS Access**

Dialed Number Identification Service (DNIS) Access allows you to limit the telephone numbers a RadiusNT/X Service Type can log into. When DNIS Access is enabled, RadiusNT/X will search for an entry in the DNISNumbers table that matches the NAS-Port-DNIS attribute in the Authentication request (to the DNISNumber field) and DNISGroupID matching the DNISGroupID field of the ServiceType of the authenticating user. If a match is found, access is granted. If a match is not found, the user is not allowed to log in after dialing that telephone number. Please note that DNIS Access is **not** enabled by default. You **must** enable DNIS Access under the **Advanced** option within the RadiusNT/X Administrator and then restart RadiusNT/X. In addition, please check with your NAS vendor to be sure your NAS supports DNIS-related attributes before enabling DNIS restrictions.

## **Reject List**

Conveniently, you can define a set of attribute/value matches that RadiusNT/X will reject immediately, without having to actually process a request. For instance, if you want to reject any user calling from a specific phone number, you could add an entry to the RadReject table with the Caller-ID attribute and the phone number. Please note that the Reject List is **not** enabled by default. You **must** enable the Reject List feature under the **Advanced** option within the RadiusNT/X Administrator and then restart RadiusNT/X.

## **Logging**

When ODBC logging is enabled, RadiusNT/X will log error information to the database. This information can be very useful for debugging or problem solving. In addition, you can generate reports and gather statistics to help resolve problems RadiusNT/X may be exhibiting.

The log table described above is very simple. The main field is the RadLogMsgID field, which reports the error message identifier. If the error has a user associated with it, the username will be stored in the username field. The data field contains information specific to the type of log message. For example, a type 0 generic message or type 1 generic error will have a description showing what it is in the data field. Please

note that the username field is typically blank. However, in a Type 4 message (bad password), the username field will be the username the user entered and the data field will be the password the user entered. You will find a table describing the RadLogMsgIDs below:

RadLogMsgID	Log Message	Description
0	Generic Log Message	This is a generic log message, which does not have a pre-defined RadLogMsgID. It is informational only, and is not an error.
1	Generic Error Message	This is a generic error message, which does not have a pre-defined RadLogMsgID. Typically, this is a recoverable error.
10	User Not Found	The username entered was not found in the database.
11	Bad Password	The username was found, but the password was wrong.
12	Expired Account	The user's account has expired.
13	Overdue Account	The user's account is overdue or the balance is larger than allowed.
14	Concurrency Limit	The user is already logged in the maximum allowed number of concurrent sessions.
15	Time Limit	The user does not have any time left to use.
19	No Service Defaults	The user's service does not have any defined RADIUS attributes, and the service type does not have any defined RADIUS attributes.
20	User Inactive	This users account is disabled.
21	Start Date not reached	Service for this user has not yet started.
40	SNMP Check Failed	The user listed in the Calls Online list does not match the user returned in the SNMP check for that port.
50	Unauthorized Request	A RADIUS request was received from a RADIUS client which is not authorized to send requests.
51	No Username	A RADIUS request did not have a username attribute.
52	No Password	A RADIUS request did not have a password attribute.
53	Digest Mismatch	A RADIUS request did not have a correct digest. Please note that this is typically shown because the secret used by the NAS does not match the secret RadiusNT/X has for the NAS.
60	Parse Error	RadiusNT/X encountered an error parsing the data.

100

CHAP not allowed

The user authentication attempt used Challenge Authentication Protocol (CHAP), but the user's Password is "UNIX" or "WINNT". Please note that for these two cases, the user **must** use PAP.

### Special Users

Please note that there are several usernames that are **reserved** by RadiusNT/X. Successful authentication requests of these users cause special triggers or events to happen within RadiusNT/X. Each username begins and ends with an asterisk (\*). The shared secret between RadiusNT/X and the client **must** be used as the password. Please refer to the list of the reserved user names below:

Reserved User Name	Description
*RefreshServerAccess*	Reload the Server Access table list.
*LastModifiedAccounts*	Reload changed accounts from the database.
*DeleteOldAccounts*	Remove Old/Expired Accounts from the cache.
*RefreshAccountTypes*	Reload the Account Types table list.
*RefreshDNIS*	Reload the DNIS table list.
*DeferredMemFree*	Free any deferred memory.
*TestDatabase*	Test the Database.
*DatabaseTimeOffset*	Check the time offset between RadiusNT/X and the SQL Server.
*RefreshRadRejects*	Reload the RadRejects table list.
*RefreshRoamServers*	Reload the RoamServers table list.
*CacheWrite* (Enterprise & Professional version only)	Write the smart cache database to disk.
RefreshProxyAttributes (Enterprise & Professional version only)	Refresh the attribute proxy list.
*reload*	Reload the user's file.
*RefreshProxyAttributes* (Enterprise & Professional version only)	Reload the Proxy Attributes table list.

## ***IP Pooling***

Usually, the NAS auto-assigns IP addresses to users as they log in from an internal address pool. If possible, we recommend this method for assigning dynamic IP addresses. However, RadiusNT/X also provides its own IP address pooling facility. It works by relying on RADIUS accounting data to determine which addresses are in use. *Note: Missing accounting information can cause inconsistencies in the IP reservation database.*

The following RadiusNT/X configuration data is involved with IP Pooling:

- ?? Server Groups – A group of servers (RadiusNT/X clients).
- ?? IP Groups – Each group contains a list of reservable IP Addresses.
- ?? IP Service Types – Associates a Server Group with all or specific IP Groups and allows access to all or specific Service Types.

## Chapter 10 – ENTERPRISE & PROFESSIONAL VERSION ONLY FEATURES

When RadiusNT/X is run with either a Professional or Emerald license, additional features become available. Please note that the features are **not** enabled by default and several configuration steps are required for proper operation. If you have an Emerald installation, please refer to [Appendix B](#), as well. The following sections describe these additional features.

### *Proxy and Roaming*

Roaming is popular for allowing another ISP or company's users to dial locally into your facilities, rather than calling long distance to access the Internet. RADIUS proxy is also commonly known as "forwarding" or "roaming". RadiusNT/X supports RADIUS proxy in ODBC mode. This feature allows you to forward or proxy a request to another RADIUS-compatible server. Please note that RADIUS proxy is **not** enabled by default. You can easily enable it for authentication, accounting or both within the RadiusNT/X Administrator.

### *User Based Proxy*

When using user-based proxy, the remote user logs in with a full e-mail address (e.g. user@company.com). This signals to RadiusNT/X that the user is a roaming user, not a local user. RadiusNT/X extracts the domain (e.g. company.com) from the user's e-mail address. If the domain has been configured for proxy, the request is forwarded to the specified RADIUS server. After RadiusNT/X sends the proxy request to the downstream RADIUS server, it will continue to receive and process authentication and accounting requests. Once the proxy response is returned, RadiusNT/X will build the response packet and then send it back to the RADIUS client to complete the login request.

Although the theory of roaming is fairly straightforward, there are many technical aspects that RadiusNT/X **must** handle to ensure reliable delivery to the final server and an accurate response to the RADIUS client. Please follow the steps below to configure RadiusNT/X for proxy:

1. First, you will need to define the RADIUS servers that you will be proxying requests to. This server information **must** be stored in the database table, RadRoamServers.
2. Next, you will need to define the domains that you wish to forward, and associate a RadRoamServer with each domain. This domain information **must** be stored in the database table, RadRoamDomains.

There are several options for configuring the roaming feature in the two above noted tables, RadRoamServers and RadRoamDomains. One of the more useful options is the default domain. If you define a domain as "DEFAULT", RadiusNT/X will send to it all roaming requests that do not have a matching domain. However, you **must** make sure the priority for the DEFAULT domain is higher than all other domains you have listed. Any domain that has a higher priority than the default domain will be sent to the default domain. The **first** domain matching the users's domain (or the DEFAULT entry) with the lowest priority is the one used.

The TreatAsLocal flag allows you to specify that a domain should not be forwarded. This flag is useful in conjunction with the StripDomain flag, since RadiusNT/X will strip the domain and look in your local database for the user. If you have several possible local domains from which your users may try to log in (e.g. user@company.com, user@mail.company.com, and user@server.company.com), you can configure

an entry for each, with **both** flags set to “**true**”. Please note that when the TreatAsLocal flag is set to “true”, the server the domain is associated with is **not** relevant, since the request will not be forwarded.

### ***Incoming Proxy***

Incoming proxy is not a proxy request from RadiusNT/X's point of view, rather just another request similar to a NAS request. The only difference is that you will usually need to strip the @domain.com portion from the username, so that RadiusNT/X can match just the username portion of the request.

To configure incoming proxy, please do the following:

1. Start the RadiusNT/X Administrator
2. Choose the Advanced tab and select the following options:
3. User Proxy: Authentication
4. User Proxy: Accounting
5. Save your changes and restart RadiusNT/X

In addition, please modify two tables in your database to include information about the domain. You will need to add each Server, IP Address and Secret, as sent to you by the port provider, to the Servers table. This is similar to any other NAS that you receive requests from.

1. Add an entry to your RadRoamServers table with the following attributes:

Server:           Name of the Service Provider

IPAddress:       A correctly formed IP address (the IP address is not actually used)

Secret:           Not Used

TreatAsLocal:   Checked

StripDomain:    Checked

2. Add an entry to your RadRoamDomains table, with the following attributes:

Domain:        Your domain (or the domain to strip). Do **not** include the @ character.

RadRoamServerID: The automatically generated ID number of the Roam Server you created in the step above.

Priority:                0

CostPerMinute:        0

### ***Server-Based Proxy***

There may be situations where you will want to unconditionally forward all requests that are received from a RADIUS client to another RADIUS server. This is a popular option when you lease services (e.g., a set of ports from one of your NAS) to another company, but they will be maintaining a RADIUS server and user information independent of your database.

Server-Based Proxy is configured by selecting the **Server-Based Proxy** option within the RadiusNT/X Administrator. When this option is selected, RadiusNT/X knows to examine the RadRoamServerID field within the corresponding record from the Servers table of the client that is making the request. If the RadRoamServerID is **not** NULL, RadiusNT/X looks for the matching entry in the RadRoamServers table. If a matching entry is found, RadiusNT/X forwards the request on to that server.

In Server-Based proxy, RadiusNT/X forwards the request to the configured RADIUS server and returns the response to the requesting client. Please note that RadiusNT/X does **not** process the request locally. In addition, the StripDomain and TreatAsLocal options are not applicable in this case.

### ***Modifying Return Attributes***

If the ServiceType field in the RadRoamDomains table is **not** NULL, then RadiusNT/X will return the set of attributes associated with that particular ServiceType that resides in the RadATConfigs table when a user authenticates.

### ***Attribute Proxy***

Authentication requests can be proxied based on the value of a group of check items. For example a user logging in with a special character in their name or from a specific DNIS number. See the descriptions of the [RadProxyAttributes](#) and [RadProxyAttributeGroups](#) tables for more information on configuring attribute proxy.

### ***Proxy Failover***

In a proxy situation, RadiusNT/X can automatically failover to an alternate server if the primary server becomes unresponsive or fails. You can configure how many times to retry the primary server, and the interval between retries. Once RadiusNT/X has identified the primary server as down, it will automatically switch to the next defined server.

You can also define how often RadiusNT/X should check to determine whether the primary server is back up. During the time between when the primary server has been identified as down and the retry period, RadiusNT/X will automatically use the alternate server, and will not try to use the primary server. Once the defined retry time period has elapsed, RadiusNT/X will check to see if the primary server is responding again. If it is, RadiusNT/X will automatically switch back to the primary server.

## ***Simple Network Management Protocol (SNMP)***

RadiusNT/X can act as an SNMP server for external statistics tracking **and** as an SNMP client. The following section explains how to set up SNMP support for both the Windows (RadiusNT) and Linux/Solaris (RadiusX) environments. Please note that you **must** have the SNMP service already installed (via the Control Panel) in the Network Properties section before RadiusNT can receive SNMP requests. However, you do **not** need the SNMP service installed for SNMP concurrency checking.

RadiusNT supports most parts of the RADIUS accounting and authentication SNMP Management Information Base (MIB) proposal. The MIB proposal is an RFC that hasn't been finalized yet. It describes the Object Identifiers (OIDs) that a RADIUS server should support. This feature allows an SNMP agent to query statistics and information regarding RadiusNT in real-time. If SNMP is allowed and configured correctly, RadiusNT spawns a separate thread to handle the SNMP requests.

Please note that you **must** have the SNMP service installed on each machine that RadiusNT is installed on. If you do not have the SNMP service installed, you will most likely need to re-install Windows NT Service Pack 3 (SP3) to update the SNMP files to the SP3 level. Otherwise, you will receive an SNMP error whenever you try to start the SNMP service.

Once SNMP service is installed, please follow the steps below to enable the RadiusNT SNMP feature:

1. Copy the *mib.txt* and *radntmib.dll* files to the data directory specified in the RadiusNT Administrator.
2. Open the Regedt32 application, and go to the HKEY\_LOCAL\_MACHINE\Software\IEA\RadiusNT selection.
3. Create a key named "SNMP", and then a value named "Pathname" under the SNMP key. The value type is REG\_SZ. The Data needs to be full path to the *radntmib.dll* file (typically c:\radius\radntmib.dll).
4. Go to the HKEY\_LOCAL\_MACHINE\System\CurrentControlSet\Services\SNMP selection. Please note that if this key does **not** exist, the SNMP service was either not installed, or not installed correctly.
5. Go to the Parameters\ExtensionAgents key. This key includes several values, with names starting at "1", increasing incrementally by one for each new value.
6. Add a value of type REG\_SZ with the next number (ex: if 1 and 2 are present, use 3). The Data needs to be the registry path to the key created in step 3 (typically "Software\IEA\RadiusNT\SNMP") without the tree name (HKEY\_LOCAL\_MACHINE is assumed).
7. For the SNMP service to read the registry changes, you will need to restart the SNMP service.

The SNMP service communicates with RadiusNT through the *radntmib.dll* file. Please note that you can start either service (SNMP or RadiusNT) in any order and stop or restart either one without causing a problem. However, when RadiusNT is not running, the *radntmib.dll* will return a -1 for all values queried until RadiusNT is started.

Please note that if you do not have the SNMP service installed for Windows NT and you do have a service pack installed, you must re-install the service pack after installing the SNMP service or the SNMP service may not start.

### **Querying SNMP values**

The CMU SNMP tools are available as an example to query information from RadiusNT via SNMP. You can also use a variety of other SNMP tools to query RadiusNT (e.g., the SNMP tools that come with the Windows NT Resource Kit). The Object Identifier (OID) for the base information for RadiusNT is 1.3.6.1.3.79. One of the easiest ways to see each of the values available is to use the *Snmpwalk* application to "walk" the



RADIUS tree. Snmpwalk will display the tree/subtree values that you specify. Below you will find the command that illustrates an example of this:

```
C:\RADIUS>snmpwalk -v 1 radiusnt public .1.3.6.1.3.79
```

```
radius.radiusAuthentication.radiusAuthServMIB.radiusAuthServMIBObjects.radiusAuthServ.  
radiusAuthServIdent.0 = "RadiusNT 2.5.116"
```

```
radius.radiusAuthentication.radiusAuthServMIB.radiusAuthServMIBObjects.radiusAuthServ.  
radiusAuthServUpTime.0 = 119192
```

```
radius.radiusAuthentication.radiusAuthServMIB.radiusAuthServMIBObjects.radiusAuthServ.  
radiusAuthServResetTime.0 = 119192
```

```
radius.radiusAuthentication.radiusAuthServMIB.radiusAuthServMIBObjects.radiusAuthServ.  
radiusAuthServConfigReset.0 = running(4)
```

### ***SNMP Authentication***

SNMP Object Identifier	Object Name	Description
.1.3.6.1.3.79.1.1.1.1.1.0	Identification	RadiusNT/X Identification string.
.1.3.6.1.3.79.1.1.1.1.2.0	Up Time	The number of seconds RadiusNT has been running.
.1.3.6.1.3.79.1.1.1.1.3.0	Reset Time	The number of seconds since RadiusNT was reset.
.1.3.6.1.3.79.1.1.1.1.4.0	Config Reset	State of RadiusNT: 1-Unknown, 3-Init, 4-Running.
.1.3.6.1.3.79.1.1.1.1.5.1	Access Requests	Number of requests since startup.
.1.3.6.1.3.79.1.1.1.1.5.2	Invalid Requests	Number of requests from unknown clients.
.1.3.6.1.3.79.1.1.1.1.5.3	Duplicate Requests	Number of duplicate requests.
.1.3.6.1.3.79.1.1.1.1.5.4	Access Accepts	Number of good requests (successful logins).
.1.3.6.1.3.79.1.1.1.1.5.5	Access Rejects	Number of rejected requests (failed logins).
.1.3.6.1.3.79.1.1.1.1.5.6	Access Challenges	Number of CHAP Challenges.
.1.3.6.1.3.79.1.1.1.1.5.7	Malformed Requests	Number of malformed requests (not bad authenticators).
.1.3.6.1.3.79.1.1.1.1.5.8	Bad Authenticators	Number of bad authenticators (invalid secrets).
.1.3.6.1.3.79.1.1.1.1.5.9	Packets Dropped	Number of requests dropped w/out a reply sent.
.1.3.6.1.3.79.1.1.1.1.5.10	Unknown Types	Number of packets of unknown types.

### ***SNMP Accounting***

SNMP Object Identifier	Object Name	Description
------------------------	-------------	-------------

.1.3.6.1.3.79.2.1.1.1.1.0	Identification	RadiusNT/X Identification string.
.1.3.6.1.3.79.2.1.1.1.2.0	Up Time	The number of seconds RadiusNT has been running.
.1.3.6.1.3.79.2.1.1.1.3.0	Reset Time	The number of seconds since RadiusNT was reset.
.1.3.6.1.3.79.2.1.1.1.4.0	Config Reset	State of RadiusNT: 1-Unknown, 3-Init, 4-Running.
.1.3.6.1.3.79.2.1.1.1.5.1	Accounting Requests	Number of requests since startup.
.1.3.6.1.3.79.2.1.1.1.5.2	Invalid Requests	Number of requests from unknown clients.
.1.3.6.1.3.79.2.1.1.1.5.3	Duplicate Requests	Number of duplicate requests.
.1.3.6.1.3.79.2.1.1.1.5.4	Accounting Responses	Number of responses (successful requests).
.1.3.6.1.3.79.2.1.1.1.5.5	Malformed Requests	Number of malformed requests (not bad authenticators).
.1.3.6.1.3.79.2.1.1.1.5.6	Bad Authenticators	Number of bad authenticators (invalid secrets).
.1.3.6.1.3.79.2.1.1.1.5.7	Packets Dropped	Number of requests dropped without a reply sent.
.1.3.6.1.3.79.2.1.1.1.5.8	No Record	Number of packets of unknown types.
.1.3.6.1.3.79.2.1.1.1.5.9	Unknown Types	Number of packets of unknown types.

### **AgentX Support**

When running on a UNIX system, RadiusX can interact with the AgentX SNMP daemon to allow querying of SNMP statistics. (AgentX is based on the CMU Agentx implementation. You can find more information at <http://www.net.cmu.edu:80/groups/netdev/agentx.html>.) Please note that you **must** configure the AgentX socket directory where the master agent's (snmpd) UNIX domain socket endpoint is located. This can usually be left blank to accept the default (/var/agentx). This is configured in the RadiusX Administrator.

If you run across errors while initializing the Agentx library, please make sure the directory exists and that both RadiusX and AgentX have appropriate permissions to access the directory.

### **SNMP Concurrency Checking**

SNMP concurrency checking can be used if you suspect that RadiusNT/X is not tracking the on-line users correctly. If it is not working correctly, it can inadvertently cause a user to be denied access. To prevent this from happening, RadiusNT/X can verify in real-time that the user is on-line at the time of authentication by using SNMP. It will **not** update the Calls Online list nor will it correct any other problems pertaining to Calls Online. It is designed to prevent incorrect concurrency denial rather than to always prevent logins because of concurrency limits.

When RadiusNT/X queries the NAS to verify the user, it **must** know the SNMP Community and the specific OID for the port the user is listed to be on. The SNMP Community is stored within the Servers table, in the Community field. Although this entry is typically "public", you may have changed it for security reasons. The OID for each port is stored within the ServerPorts table, in the SNMPUser field. Please note that the contents of this field will change for each port. Currently, it **must** be a static entry for each port. Please note that these may **differ** from NAS models and vendors.

For example, for a Livingston Portmaster 2, the OID is “.1.3.6.1.4.1.307.3.2.1.1.1.4.x”, where x is the port number. From an SQL perspective, you can easily populate the ServerPorts table by using a derivative of the following SQL statement. For other NAS vendors, please consult the NAS documentation to verify how it supports SNMP and what the specific OID is.

Update ServerPorts

Set SNMPUser = “.1.3.6.1.4.1.307.3.2.1.1.1.4.” + convert(varchar(5), Port+1)

Where ServerID = x

Please note that the ServerID should match an entry from the Servers table for the NAS that you want to update. The following table shows the Base OID for several popular vendors and terminal servers, although it is a good idea to double-check your NAS documentation.

Vendor	Model	Base OID	ServerType	Comments
--------	-------	----------	------------	----------

<b>Lucent</b>	Portmaster2	.1.3.6.1.4.1.307.3.2.1.1.1.4. x	2	Ports are 1 to 30 or 1 to the number of ports in the PM.
<b>Lucent</b>	Portmaster3	.1.3.6.1.4.1.307.3.2.1.1.1.4. x	3	1 on the PM3 is S0. The ports are 2-25/26-49 (T1) or 2-24/26-48 (PRI).
<b>Cisco</b>	AS5248	.1.3.6.1.4.1.9.2.9.2.1.18.x	9	Ports are 1-48 for a 48 port dual T1.
<b>Ascend</b>	Max 4xxx	.1.3.6.1.4.1.529.12.3.1.4.	5, 6, 7, 8	ServerType <b>must</b> be set to 5-8 for this to work.
<b>3Com</b>	HiPer ARC	.1.3.6.1.4.1.429.4.10.1.1.18. x	13	Starts at 1513 for the first port and increment in same formula as the ports are reported to RadiusNT/X.
<b>Nortel</b>	5399	.1.3.6.1.4.1.15.2.16.1.2.1.3. 1.x	14	Ports start at 1.

When running against SQL Server, RadiusNT/X calls the following stored procedure to retrieve information about each port the user is listed on. Please note that you need to have this stored procedure in your database and that the user RadiusNT/X is connecting as **must** have execute permission for it.

```
CREATE PROCEDURE RadCheckOnlineSNMP @UserName varchar(64) AS

Select s.IPAddress, s.ServerType, s.Community, sp.SNMPUser, sp.AcctSessionID
From Servers s, ServerPorts sp
Where s.ServerID = sp.ServerID
      AND UserName=@UserName
      AND AcctStatusType=1
GO
```

### ***Server Types***

RadiusNT/X uses the ServerType field in the Servers Table to track the types of servers supported. This information is primarily used for SNMP Concurrency Checking, although it may have use in the future for other functions. Below is a list of the current Server Types and their associated denotements.

Vendor	Model	ServerType	SNMP Method
--------	-------	------------	-------------

<b>Generic</b>	Starts at 0	0	Use SNMPUser as OID
<b>Generic</b>	Starts at 0	1	Use SNMPUser as OID
<b>Lucent</b>	Portmaster 2	2	Use SNMPUser as OID
<b>Lucent</b>	Portmaster 3	3	Use SNMPUser as OID
<b>Lucent</b>	Portmaster 4	4	Use SNMPUser as OID
<b>Ascend</b>	MAX 40xx/60xx T1	5	Add ASID To SNMPUser
<b>Ascend</b>	MAX 40xx/60xx E1	6	Add ASID To SNMPUser
<b>Ascend</b>	MAX 1800	7	Add ASID To SNMPUser
<b>Ascend</b>	MAX TNT	8	Add ASID To SNMPUser
<b>Cisco</b>	AS 5x00	9	Use SNMPUser as OID
<b>3Com</b>	Total Control	10	Use SNMPUser as OID
<b>Computone</b>	Power Rack	11	Use SNMPUser as OID
<b>Microcom</b>	6000	12	Use SNMPUser as OID
<b>3Com/USR</b>	HiPer ARC	13	Use SNMPUser as OID
<b>Nortel</b>	5399	14	Use SNMPUser as OID

## **Smart Cache**

A new feature introduced in RadiusNT/X 3.0, is the inclusion of a very flexible and powerful Smart Cache engine. The Smart Cache feature loads the RadiusNT/X authentication information directly from the database into cached memory for faster account access and increased server performance. The following section describes various aspects and behaviors of the Smart Cache so that you understand how you can tune the Smart Cache options to best meet your specific needs.

The primary advantages of using the Smart Cache feature is that:

- ?? It provides the ability to maintain operations in the event of a database, or a database connection, failure. The Smart Cache allows RadiusNT/X to continue operating until the problem can be detected and resolved.
- ?? It allows a system configuration with connections to multiple databases, similar to a replication or cluster scenario, whereby RadiusNT/X can automatically failover to a second database should the first database fail.
- ?? It provides the ability to off-load redundant processing from the database to the local servers. This lessens the strain and load on the database as the number of requests and users grow.

The Smart Cache configuration within the RadiusNT/X Administrator allows the user to specify the frequency that cache updates will occur that refresh the data between the database and the memory cache. This manual configuration is generally unnecessary however, as the Smart Cache will in most cases intelligently update itself as needed before those configured limits are reached.

The Smart Cache can also perform batch updates for accounting purposes. This allows for faster processing of accounting records or the ability to handle situations where it was not able to immediately write the accounting record. In addition, you can specify the maximum number of records that can be stored in the cache through the RadiusNT/X Administrator.

## **Syslog Support**

Rather than logging information locally on each server, all log information can be sent to a central syslog server. This feature allows for greater manageability of multiple servers, since you can look in one central log file for potential or current problems. Please note that there are three types of facility codes used:

- ?? DAEMON  
Any message not specific to an Authentication or Accounting request is logged here. These can include disk write problems, or a local configuration error.
- ?? LOCAL0  
Any message specific to an Authentication request.
- ?? LOCAL1  
Any message specific to an Accounting request.

## **LDAP Authentication**

If you have users stored in an LDAP directory, you can have RadiusNT/X authentication directly from the LDAP server, rather than copy the user information. The RadiusNT/X LDAP Interface is flexible enough to operate with nearly all LDAP-based directory servers by way of a configurable search filter and LDAP->Radius attribute/value mapping system.

To Enable LDAP Authentication:

In the RadiusNT/X Administrator, enable text mode and configure LDAP server information.  
Set an LDAP default in the users file:

```
DEFAULT      Password="ldap"  
             User-Service = Framed-User,  
             Framed-Protocol = PPP
```

Included with RadiusNT/X are schema definitions for a radiusUser object class written by IEA Software. The two files *radius.at.conf* and *radius.oc.conf* contain the radiusUser object class and attributes. Many LDAP servers such as umich/openldap and Netscapes directory server can be configured to read these files directly. Others may have specialized schema managers that don't accept the standard format.

Using the radiusUser object class is not required. It's needed if you want to store user specific RADIUS attributes in the directory server. See External Attribute Mapping for more information.

The search string in the LDAP configuration is very important, as it tells RadiusNT/X how to ask the LDAP server for information. When defining the string, you can use the following tokens, which will be replaced with the authenticating user's information:

\$login	replaced with current login name.
\$domain	replaced with current domain name.

There are two search methods. Binding as the full DN in the search string, saving a search operation:

```
uid=$login,ou=$domain,o=nasa.
```

In this case, if no domain were available, Bind DN would look like: "uid=\$login,o=nasa", removing ou=... from the search string.

The other method involves searching the directory then binding as the DN of the matching entries (*Note: the query must be enclosed in (/s.):*)

```
(&(uid=$login)(ou=$domain))
```

In this case, if no domain were available, the domain attribute is replaced with the match any wildcard ("\*") symbol: (&(uid=\$login)(ou=\*)) Searches are performed using the Bind DN and Password configured in the Radius Administrator, or anonymously if they are left blank. This user must have sufficient rights to search the directory and retrieve the RADIUS-specific directory attributes and their values as the search finds matching accounts.

The following are some examples you can use with various LDAP schemas:

LDAP Server	
<b>Netscape LDAP/Messaging Server</b>	<b>(uid=\$login)</b>
<b>Microsoft Active Directory</b>	<b>cn=\$login,cn=users,dc=\$domain</b>
<b>Novell NDS</b>	<b>(cn=\$login)</b>
<b>posixAccount* objectClass</b>	<b>(&amp;(uid=\$login)!(&amp;shadowInactive=1))</b>
<b>Generic</b>	<b>(&amp;(uid=\$login)(ou=\$domain))</b>

## Chapter 11 – ENTERPRISE VERSION FEATURES

When RadiusNT/X is run with an Enterprise Edition license, additional features become available on the RADIUS server. The Enterprise feature set is focused towards External Authentication and third party secure/token authentication.

### ***ACE Server***

Native support for RSA's ACE server and hardware and software one-time token authentication is built-in. To authenticate against an ACE server, you must install the ACE client. Once the Ace client is installed, you can then use the special password, "ACE3" to direct RadiusNT/X to authenticate the user against the configured ACE server.

### ***Defender***

Native support for Axent Technologies' Defender server is built-in for hardware and software one-time token authentication, including challenge/response authentications. To authenticate against a Defender server, you must define the Defender server in the External Authentication section of the Administrator. You can then use the special password, "DEFENDER" to direct RadiusNT/X to authenticate the user against the configured Defender server.

### ***SafeWord***

Native support for Secure Computing's SafeWord server is built in for hardware and software one-time token authentication, including challenge/response authentications. To authenticate against a SafeWord server, you must install the SafeWord Client. Once SafeWord is installed, define the SafeWord server in the External Authentication section of the Administrator. You can then use the special password, "SAFEWORD" to direct RadiusNT/X to authenticate the user against the configured SafeWord server.

### ***Tacacs+***

Native support for Tacacs+ authentication is built in. Note: RadiusNT/X does not support mapping Tacacs+ attributes to RADIUS attributes.

### ***External Authentication API***

In addition to built-in authentication methods, RadiusNT/X also includes the ability for additional authentication modules to be defined. Each module has the ability to see authentication packets received by the server, and either act upon the request, or pass on the request to another module.

The C API exports the function "radiusAuth" from either a UNIX dynamic shared library (RadiusX) or a Win32 dynamic link library (RadiusNT). Please see the *radauth.c* and *radauth.h* files in the *authapi* folder for a



working C example of the API and details on the structures described below. (EXT\_USER and VALUE\_PAIR)

The authentication function is passed the EXT\_USER structure which contains all known information about the current authentication, and returns one of the following result codes:

RADIUS\_ACCEPT – The function accepted the authentication suggesting that RadiusNT/X ack this request.

RADIUS\_IGNORE – The function doesn't know about this user specifically. Give another API a chance to authenticate this user.

RADIUS\_REJECT – The function knows this user. The user's credentials are incorrect or the Administrator doesn't want the user to log in.

RADIUS\_ERROR – An error not directly related to the current user occurred. This function forces RADIUS to reject the authentication request for security purposes. If you want other APIs in the authentication list to try to authenticate, return RADIUS\_IGNORE instead.

RADIUS\_CHALLENGE – The function recognizes the user, but wants the user to provide more information to validate identity (e.g., to provide a response to a cryptographic challenge). The challenge and state fields of the EXT\_USER structure must also be set.

The API also includes utility functions available through the EXT\_USER structure. The following functions work the same as standard C, allocating memory within RADIUS. These functions must be used to allocate memory passed via the EXT\_USER structure. Using local memory routines may crash the RADIUS server.

```
user->malloc
user->free
user->realloc
user->strdup
```

We also provide some functions for handling the VALUE\_PAIR linked list:

```
vp = user->pairmalloc(void); // Allocates and initializes a VALUE_PAIR linked list.
user->pairfree(VALUE_PAIR *pair); // Frees a VALUE_PAIR linked list.
vp = user->paircopy(VALUE_PAIR *pair); // Returns a copy of a VALUE_PAIR list.
user->pairappend(&user->reply, "SessionTimeout", VENDOR_STANDARD, PW_SESSION_TIMEOUT,
PW_TYPE_INTEGER, 3600, 4, NULL); // Appends an attribute to a VALUE_PAIR list.
```

We provide password checking function (pwcheck) which automatically validates a user's password using PAP, CHAP and MS-CHAP. Pwcheck takes two parameters: The user structure (EXT\_USER) and the users plain-text password from your database. Pwcheck is required to support CHAP authentication.

```
int radiusAuth(EXT_USER *user)
{
    A simple authentication.

    // Using pwcheck (Supports PAP & CHAP)
    If user->pwcheck(user,password) == 1
        return RADIUS_ACCEPT;
    else
        return RADIUS_IGNORE;

    // string comparison (Supports PAP only)
```

```

if user->username == username && user->password == password
    return RADIUS_ACCEPT
else
    return RADIUS_IGNORE

```

The next example responds with a reply Attribute-Value-Pair if the authentication succeeds and sends a message to RadiusNT/X when it fails. It also takes the user's domain into consideration.

```

if user->username == username &&
    user->password == password &&
    user->domain = domain
{

```

It's important that all data assigned to the user be allocated using the functions provided in the EXT\_USER structure. RadiusNT/X must be able to free them without exception. If you pass static variables to the EXT\_USER structure or attempt to use local routines for memory allocation, it **will** crash the server.

All pointers in the value pair structure must be initialized to null if they are not being used.

```

vp = user->pairmalloc();

    usersavp = (VALUE_PAIR *)mygetavpfunction(username)
    user->reply = (VALUE_PAIR *)user->paircopy(usersavp)
    return RADIUS_ACCEPT
}
else if user->domain != domain
{
    user->msg = user->strdup("I don't know about your domain.")
    return RADIUS_IGNORE
}
else
{
    user->msg = user->strdup("Your username or pass didn't match.")
    return RADIUS_REJECT
}

```

Challenging the authentication request: Your API will be called twice, once to challenge the user and another to authenticate the response.

```

if *user->request has no state && user->username == username
{
    user->challenge = user->strdup("What's 1+1?")
    user->state = user->strdup(username + ":" + mysessionid)
    return RADIUS_CHALLENGE
}
else if *user->request has a known state
{
    if user->password == challengerresponse
        return RADIUS_ACCEPT
    else
    {
        user->msg = user->strdup("wrong answer.")
    }
}

```

```

        return RADIUS_REJECT
    }
}
else
{
    user->msg = user->strdup("Unknown state...")
    return RADIUS_IGNORE
}
}

```

## ***External Attribute-Value Mapping***

Custom external systems created with the External Auth API or LDAP support have the ability to map their internal attributes and values to RADIUS (rfc2138) attributes. These could be used, for example, to assign an IP address, or limit what a user can do after authentication. See the database schema in [Chapter 8](#) for more information on configuring attribute mapping.

### ***Auth API***

The EXT\_USER structure in the Auth API includes a field for specifying the type of mapping that should be done. The available types are:

- 0 = Radius Attribute (No map)
- 1 = LDAP Map
- 2 = Tacacs Map
- 3..99 = Reserved for future use
- 100 > = User specific / definable mappings.

## ***Store & Forward Proxy***

As the requirements for proxy get more complex with the proliferation of port providers and roaming scenarios over WANs and the Internet, the need to store and forward accounting data among RADIUS proxies becomes very important.

In a typical RADIUS accounting transaction, a RADIUS client sends an accounting record to a RADIUS server. The server then sends a response to the client, letting it know the client's request was received:

### **Error! Not a valid link.**

When a proxy server enters the picture, the client might send their request to the proxy server:

(nas-w1 to Radius West).

From there, the request is forwarded to the destination server:

(Radius West to Radius Central)

The response travels back, following the same path as the request was sent:

(Radius Central to Radius West to nas-w1)

To understand the advantages of store and forward proxy, let's add another proxy server to the picture. Accounting will follow the paths:

(nas-w2 to Radius West to Radius Central to Radius East)

and back

(Radius East to Radius Central to Radius West to nas-w2)

In this case, the Accounting/response packets travel through 10 network links and depend on the availability of 3 RADIUS servers (excluding hops on the Internet itself). If the RADIUS authentication or responses (UDP) are lost anywhere on the network, the client must resend the request and replay the process until it succeeds. Over WAN/Internet links with a fair amount of congestion, this could lead to several client retries adding more congestion to the link.

More important, you must depend on the availability of more and more servers over networks and systems over which you may not have direct control. NASs generally are very limited in the amount of memory available for queueing accounting data and rarely store the queue in non-volatile memory. Some NASs may halt authentication activity as the accounting queue runs out of memory, to prevent losing data.

With Store & Forward, every proxy server accepts responsibility for making sure the accounting data it receives will be forwarded to the next server in the proxy chain and acknowledges the request directly to the sending client before forwarding the request to the next hop. This shortens any retries to a maximum of 2 network links and 1 server, regardless of the complexity of your proxy chain.

With Store and Forward Proxy enabled on RADIUS West, RADIUS Central and RADIUS East, we use the same scenario (nas-w2 to Radius East via Radius West and Radius Central). The accounting transaction is broken up into several smaller transactions:

(request)

nasw-2 to Radius East,

Radius East to Radius Central,

Radius Central to Radius East,

(response)

Radius East to Radius Central,

Radius Central to Radius West,

Radius West to nasw-2.

## Chapter 12 – TROUBLESHOOTING

If you experience trouble installing or using RadiusNT/X, please research the common problems and solutions in this section.

First and foremost: **If you are having a problem with RadiusNT/X, run it in debug mode.**

The information returned will help you diagnose the problem. For a refresher on how to use debug mode, please see the [Debug](#) section. General information is listed below:

To run RadiusNT/X in debug mode, stop RadiusNT/X. Please note that you can **not** have two copies of RadiusNT/X running on the same machine. From a Command Prompt, change to the directory where RadiusNT/X is installed and enter the command:

```
For RadiusNT: "radius -x15"  
For RadiusX : "./radiusd -x15"
```

RadiusNT/X will start in foreground mode and display the debug information. The majority of the time, this information will be sufficient for you to resolve the problem. Should you need to contact the Support Team, please remember to include a "cut and paste" of the debug output of the problem.

RadiusNT/X also logs information to a file named *logfile* in the data directory or to the RadLogs table in ODBC/Both mode. This information is valuable when diagnosing problems as well.

### ***Installation and Setup Problems***

?? User receives an error message stating an RDC object can not be registered during installation.

ODBC **must** be installed, whether RadiusNT is used in ODBC or text mode. You can obtain the ODBC installation from Microsoft's Web site at <http://www.microsoft.com/odbc> or from IEA Software's FTP site at <ftp://ftp.iea-software.com/RadiusNT/ODBC>.

### ***Startup Problems***

?? RadiusNT/X reports a 'file not found' error and then quits.

Double-check your path entries in the RadiusNT/X Administrator to make certain that at least the data directory points to the directory where you have installed RadiusNT/X.

?? RadiusNT/X reports a parse error -98 for user x.

In this case, user x has an attribute in the *users* file which does not match an attribute from the dictionary. Please remember that all attributes are case sensitive and **must** match the dictionary entries **exactly**.

?? RadiusNT/X reports a lower number of users loaded than are in the *users* file.

This occurs because RadiusNT/X came upon a user entry error and therefore stopped reading in the *users* file. Look for the user who is the entry one higher than the number RadiusNT/X reports it loaded, and you will find the user with the error.

## **Operation Problems**

?? When a request is received, RadiusNT/X displays a "Security Breach" error.

This error will appear if the machine the request is coming in from is not authorized to send requests to RadiusNT/X. This is caused by the missing IP address of the requester in the *clients* file (text mode) or the Servers table in the database. Please note that you **must** re-start RadiusNT/X in order for changes to the *clients* list to take effect.

?? The decrypted password from the authentication request is garbage.

This is caused when the secret that is configured on the NAS sending the request is not the same as the secret that is set for the NAS in the *clients* file (text mode) or the Servers table in the database. Please note that you **must** re-start RadiusNT/X in order for changes to the *clients* list to take effect. Also, remember that secrets are case sensitive and should be between 6 and 15 characters long.

?? Accounting packets in ODBC mode sometimes display an error in regard to duplicate entries.

When RadiusNT/X is running in ODBC mode, it can determine whether it has received an accounting packet already from a NAS. This error indicates that RadiusNT/X has already received this accounting packet. As long as the error is not frequently encountered, this is normal. If your accounting packets have a high Acct-Delay-Time value, then you may have network problems between your RadiusNT/X server and your NAS.

## Chapter 13 – FREQUENTLY ASKED QUESTIONS (FAQS)

### General

?? *How do I know if RadiusNT/X will work with my specific NAS or terminal server?*

RadiusNT/X is designed to work with any RADIUS compatible terminal server. Since the RADIUS protocol is vendor independent, this allows RadiusNT/X to work with many different vendors. You should look in the documentation of your NAS to find out if it supports the RADIUS protocol. There is also a list of known vendors and links to helpful areas of the vendor's web site on the RadiusNT/X Web Site at <http://www.iea-software.com/products/partners/>. Please remember that not all vendors support all RADIUS attributes outlined in the RFCs.

?? *Will RadiusNT/X use clear text for authenticating or does it require PAP or CHAP?*

RadiusNT/X supports both PAP (clear text) and CHAP. However, if you will be using a user list which contains encrypted passwords (e.g., WindowsNT SAM (not for RadiusX version), UNIX passwd file, or encrypted passwords in a database), only PAP authentication will work, since RadiusNT/X **must** have the password in clear text in these cases. In addition, case sensitive checking must be used (the "Ignore Case" option must **not** be checked in the RadiusNT/X Administrator) in order for CHAP to work.

?? *I have downloaded RadiusNT/X and everything runs normally for a while, then it stops authenticating. How can I find out what the cause of this is?*

Run RadiusNT/X in -x15 debug mode and it will display information explaining why it stopped authenticating.

?? *Is there a way to make usernames and passwords case insensitive? Will the RadiusNT/X log file still show the incorrect username/password attempts?*

You can set case insensitive usernames and passwords in the RadiusNT/X Administrator. The current version of RadiusNT/X logs these errors into the RadLogs table in ODBC mode or the log file in text mode.

?? *Can RadiusNT authenticate against the Windows NT User database?*

Yes, RadiusNT can authenticate against the Windows NT User Database in both text and ODBC mode. However, only text mode will authenticate **all** users by default. If RadiusNT is running in ODBC mode, each user **must** be added to the database, as well. Please see the [NT SAM](#) section in [Chapter 6](#) for more details on NT SAM support.

?? *We would like to use RadiusNT to authenticate all users in our NT domain. All of our user names have spaces (Ex: "John Doe"). Does RadiusNT support spaces in usernames without any modification to our NT setup?*

Yes it does. Use the Trim Name feature.

?? *Is there a way to use RadiusNT with NT 4.0 RAS?*

Yes. If you install the Windows NT Option Pack, RAS can be used as a RADIUS client. You will specifically need to install Routing and Remote Access Services (RRAS).

?? *Where can I find a copy of the RADIUS RFCs?*

You can find them on the Internet Engineering Task Force's Web site at <http://www.ietf.org>. The RADIUS RFCs are 2865 and 2868. You can also refer to Appendix A.

?? *Whenever I close all programs and log on as a different user, NT forces me to end the radius.exe program. Most services do not shut down when you log off. Is this normal for RadiusNT?*

This will occur if you have started RadiusNT manually and not as a service. To remedy this, run the RadiusNT Administrator and then install the service. Next, access a Command Prompt and start the service by typing: "net start RadiusNT".

?? *I have installed RadiusNT as a service, yet when I try to start the service, I get the error message, "Could not start the RadiusNT Service on \\XXXXX Error 1067: The process terminated unexpectedly".*

If you are receiving this error message, you will need to define full paths for the accounting and data directories within the RadiusNT Administrator.

?? *Does RadiusNT/X support filters?*

RadiusNT/X supports the standard RADIUS filter attribute as well as the Ascend Binary Filter attribute. For further information on supported filters, please contact your NAS vendor. Filters themselves are configured on the NAS; RADIUS as a protocol only tells the NAS the name of the filter to apply through the Framed-Filter attribute.

?? *Does RadiusNT/X support a ... attribute?*

RadiusNT/X will support any basic attribute. In this case, please note that it is the NAS/Proxy that **must** understand what it is and support it, or it will be of no use.

?? *Can RadiusNT/X limit the number of channels that can be open on an ISDN call?*

To restrict the number of channels that a user can bond together on an ISDN call, use the Port-Limit attribute. You will need to check your NAS documentation to see if it supports this. You can also use the Concurrency Control feature to limit the number of simultaneous connections a user can make.

?? *Will RadiusNT/X assign from different groups of IP addresses?*

Yes, but only if the NAS supports an attribute to specify the pool e.g.,: Ascend), unless RADIUS-managed IP pooling is enabled.

?? *Is there a way to avoid reverse DNS lookup of an IP address ending up in the calls table?*

RadiusNT/X does not do a reverse DNS lookup on the field. It simply records what the RADIUS client sends. You can use the Servers.IPAddress field rather than the Servers.Server field if you want an IP Address rather than a server name.



?? *To prevent multiple logins, what should the Login Limit be set to?*

RadiusNT/X will refer to the LoginLimit field in the SubAccounts table and will use its value for the user's login limit. If LoginLimit is NULL, RadiusNT/X defaults to one login for each user.

?? *Can I prohibit "Dr. Watson" from displaying a dialog box that prevents RadiusNT from being restarted remotely?*

Yes, you can achieve this by editing or adding the following section to the registry of the machine that is running RadiusNT (Please note that there may be other values that you may want to change as well.):

HKEY\_LOCAL\_MACHINE\Software\Microsoft\DrWatson\VisualNotification: 0

### **Text Mode**

?? *If the users file is modified, does the RadiusNT/X service need to be restarted?*

There are several ways to handle the changes. You can either restart RadiusNT/X as the users are cached in memory, or you can use the \*reload\* user entry with Radlogin. This signals RadiusNT/X to reload the *users* file without restarting the service. Another option is to set the Reload User Minutes setting in the RadiusNT/X Administrator to periodically reload the *users* file at regular intervals.

### **ODBC Mode**

?? *I am trying to configure a call-tracking database. What fields need to be populated for the calls to be seen?*

A few things will need to happen.

1. You will need to add entries into the Servers table to match the data for your NAS.
2. Next, add entries into the ServerPorts table, matching each port (with matching ServerID) of the NAS you entered in step 1.
3. Finally, make sure that RadiusNT/X is receiving the accounting requests from the NAS, with NAS-Identifier matching Servers.IPAddress and NAS-Port matching the ServerPorts.Port fields.

?? *Can RadiusNT/X use encrypted passwords in the database? What method does it use to check them?*

RadiusNT/X can use UNIX crypt passwords in the database similar to those found in a UNIX passwd file. Please note that this is an advanced feature and is only for those who have a **thorough** understanding of what crypt encryption is. RadiusNT/X does **not** include any tools to facilitate the creation or management of passwords in encrypted form.

Either RADIUS will automatically detect a crypt password string or the encryption type can be specified as part of the password (e.g., {crypt}teH0wLpW0gyQ). Please note that **only** PAP authentication is possible when using password encryption. Also note that when using crypt passwords where the {crypt} prefix is not specified, an account can also successfully authenticate by using the encoded password string itself.

RadiusNT/X also supports automatic detection of uuencoded (128-Bit MD5 {md5} and 160-bit SHA-1 {sha}) digests.

?? *Our authentication takes place on a UNIX machine for now, but I would like to start using RadiusNT to log the accounting info right away. Can RadiusNT be used to simply log accounting information into a database without entering user information?*

Some customers start with RadiusNT and just the accounting feature. You will find the setup to be the same, but you won't have any users defined. Almost all NASs allow for a distinct accounting and authentication RADIUS server.

?? *Where can I learn more about ODBC?*

A good ODBC educational resource can be found on the Microsoft Web site at <http://www.microsoft.com/data/odbc/default.htm>.

?? *Can I modify the SQL statement that is sent by RadiusNT/X for inserting records into the Calls table?*

No. The SQL statement is dynamically created based on the fields in the Calls table and the attributes received in the accounting requests. This process is outlined in [Chapter 9](#).

?? *How do I assign a user a static IP address?*

To do this, you **must** add entries that match the user's SubAccountID in the RadConfigs table. Please note that one of the attributes needs to be the Framed-Address attribute. Also, note that you can **not** add **only** the Framed-Address into this table, as RadiusNT/X will then only send the attributes in this table (if any exist), ignoring any attributes in the RadATConfigs table. Please see [Appendix B](#) for more details on integrating RadiusNT/X and Emerald.

## **Vendor Support**

### **Ascend**

?? *I have an Ascend MAX 40xx and am having trouble with RadiusNT/X accounting. I am wondering if my "Server Ports" table is set up correctly. The Server Port table asks for server ID, which is "1" for my Ascend box. It then asks for the Port and IP address. I have no idea what the ports are, so I have assigned IP addresses from a pool. Help!*

Begin by checking the MAX to ensure that it is, indeed, configured for accounting and for sending accounting requests to RadiusNT/X. The Port field must represent what the MAX returns in the NAS-Port field. Please note that you can run RadiusNT/X in -x15 debug mode for an example. Typically this follows the format of tlcc where:

t is the type of call: 1 is digital and 2 is async/modem  
ll is the line/trunk the call came in on  
cc is the channel of the line/trunk the call came in on.

An example of ports to create for a MAX 4000 with 2 PRI lines would be:

10101-10124, 10201-10224, 20101-20124, and 20201-20224.

Please note that the IP address field in the Server Ports table is not used at this time.

?? *Where can I find a summary of the NAS-Port for the Max TNT?*

You can find this information on Ascend's Web site at: <http://www.ascend.com/>.

### **Cisco**

?? *I received two Framed-Address attributes in my accounting packets and they are preventing RadiusNT/X from inserting the accounting packets into the database.*

This issue became Cisco bug-Id CSCdi87169: "RADIUS should never include multiple Framed-IP-Address fields". Please note that it has been fixed in the following releases from Cisco and Cisco users should upgrade to one of the releases to avoid problems in ODBC mode. Please note that these are Cisco OS releases, **not** RadiusNT/X.

11.1(9.1) 11.1(9.1)AA1(1.1) 11.1(9.1)AA1(1.2) 11.2(4.2) 11.2(4.2)F 11.2(4.2)P

?? *Where can I learn more about how to configure Cisco IOS software to support RADIUS?*

You can find this information on Cisco's Web site at the following addresses:

[http://www.cisco.com/warp/public/732/General/radius\\_wp.htm](http://www.cisco.com/warp/public/732/General/radius_wp.htm)

[http://www.cisco.com/warp/public/732/111/555\\_pp.htm](http://www.cisco.com/warp/public/732/111/555_pp.htm)

### **Computone**

?? *RadiusNT/X returns errors when trying to store accounting records in the ODBC database when I reset my Computone NAS. How can I prevent this?*

This problem arises as the Computone products reset their Acct-Session-ID counter upon a reboot. To avoid the errors, you will need to setup a time server and point the Computone product to it. A time value will be inserted as the first part of the Acct-Session-ID. Please note that one drawback to this is that the Acct-Session-ID field will be larger, which could cause RadiusNT/X to fail to insert the accounting record. You may need to enlarge the AcctSessionID field in your Calls table to accommodate the new length.

### **iPass**

?? *Does RadiusNT/X support iPass roaming?*

Although this option is being researched, we have not finalized iPass support. Please watch our Web site at <http://www.iea-software.com> for update news. To learn more about iPass roaming, please check out their Web site at <http://www.ipass.com>.

### **ipSwitch**

?? *Can I use WhatsUp to monitor the status of RadiusNT running as a service?*

*WhatsUp Gold* can monitor your RADIUS servers and inform you of an outage. The *WhatsUp Gold* documentation includes details on configuring this function.

## **Livingston**

?? *I have a PortMaster 3. Is it possible to prohibit analog account access on ISDN lines? If so, what would a sample text RADIUS look like?*

You can implement this functionality using a *users* file entry similar to the one below. In addition, you can add the NAS-Port-Type check to the RadConfigs or RadATConfigs table of your database with the check field enabled for ODBC mode. Please note that **all** check attributes **must** go on the first line.

```
user Password = "blah", NAS-Port-Type = Async  
User-Service = Framed-Protocol
```

## Appendix A - RADIUS ATTRIBUTES

### *RADIUS Attributes*

The RADIUS protocol is based on a set of attributes. Although most attributes are defined in the RADIUS RFCs, there are ways to add Vendor-Specific attributes for those vendors who need specific attributes not defined in the RFC.

1	User-Name	The name of the user to be authenticated.	
2	User-Password	The password of the user to be authenticated, or the user's input following an Access-Challenge.	
3	CHAP-Password	The response value provided by a PPP Challenge-Handshake Authentication Protocol (CHAP) user in response to the challenge.	
4	NAS-IP-Address	The identifying IP Address of the NAS that is requesting Authentication of the user. It is only used in Access-Request packets. Either NAS-IP-Address or NAS-Identifier SHOULD be present in an Access-Request packet.	
5	NAS-Port	The physical port number of the NAS that is authenticating the user.	
6	Service-Type	The type of service the user has requested, or the type of service to be provided.	
	1 Login	4 Callback Framed	7 NAS Prompt
	2 Framed	5 Outbound	8 Authenticate Only
	3 Callback Login	6 Administrative	9 Callback NAS Prompt

Below you find information from the RADIUS RFC 2138:

### **5.7. Framed-Protocol**

This attribute indicates the framing to be used for framed access. It may be used in both Access-Request and Access-Accept packets.

Value

The Value field is four octets.

- 1 PPP
- 2 SLIP
- 3 AppleTalk Remote Access Protocol (ARAP)
- 4 Gandalf proprietary SingleLink/MultiLink protocol
- 5 Xylogics proprietary IPX/SLIP



Length

6

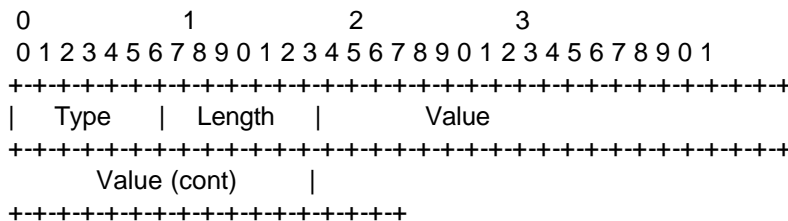
Address

The Address field is four octets specifying the IP netmask of the user.

### 5.10. Framed-Routing

This attribute indicates the routing method for the user when the user is a router to a network. It is only used in Access-Accept packets.

A summary of the Framed-Routing Attribute format is shown below. The fields are transmitted from left to right.



Type

10 for Framed-Routing.

Length

6

Value

The Value field is four octets.

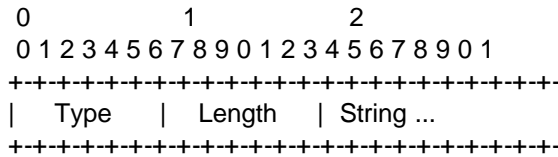
- 0 None
- 1 Send routing packets
- 2 Listen for routing packets
- 3 Send and Listen

### 5.11. Filter-Id

This attribute indicates the name of the filter list for this user. Zero or more Filter-Id attributes MAY be sent in an Access-Accept packet.

Identifying a filter list by name allows the filter to be used on different NASs without regard to filter-list implementation details.

A summary of the Filter-Id Attribute format is shown below. The fields are transmitted from left to right.



Type

11 for Filter-Id.

Length

>= 3

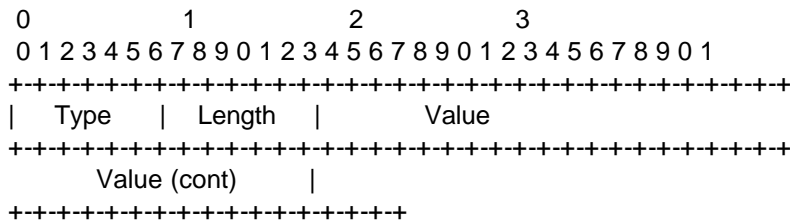
String

The String field is one or more octets, and its contents are implementation dependent. It is intended to be human readable and MUST NOT affect operation of the protocol. It is recommended that the message contain displayable ASCII characters from the range 32 through 126 decimal.

### 5.12. Framed-MTU

This attribute indicates the Maximum Transmission Unit to be configured for the user, when it is not negotiated by some other means (such as PPP). It is only used in Access-Accept packets.

A summary of the Framed-MTU Attribute format is shown below. The fields are transmitted from left to right.



Type

12 for Framed-MTU.

Length

6

Value

The Value field is four octets. Despite the size of the field, values range from 64 to 65535.

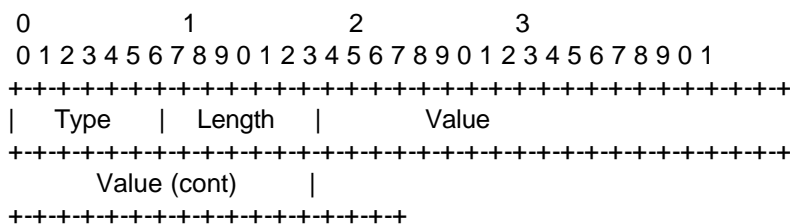


### 5.13. Framed-Compression

This attribute indicates a compression protocol to be used for the link. It MAY be used in Access-Accept packets. It MAY be used in an Access-Request packet as a hint to the server that the NAS would prefer to use that compression, but the server is not required to honor the hint.

More than one compression protocol attribute MAY be sent. It is the responsibility of the NAS to apply the proper compression protocol to appropriate link traffic.

A summary of the Framed-Compression Attribute format is shown below. The fields are transmitted from left to right.



Type

13 for Framed-Compression.

Length

6

Value

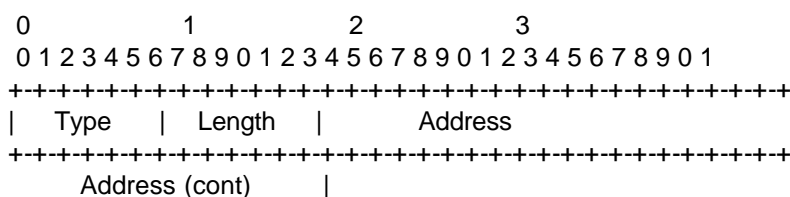
The Value field is four octets.

- 0 None
- 1 VJ TCP/IP header compression [5]
- 2 IPX header compression

### 5.14. Login-IP-Host

This attribute indicates the system with which to connect the user, when the Login-Service attribute is included. It MAY be used in Access-Accept packets. It MAY be used in an Access-Request packet as a hint to the server that the NAS would prefer to use that host, but the server is not required to honor the hint.

A summary of the Login-IP-Host Attribute format is shown below. The fields are transmitted from left to right.



+++++

Type

14 for Login-IP-Host.

Length

6

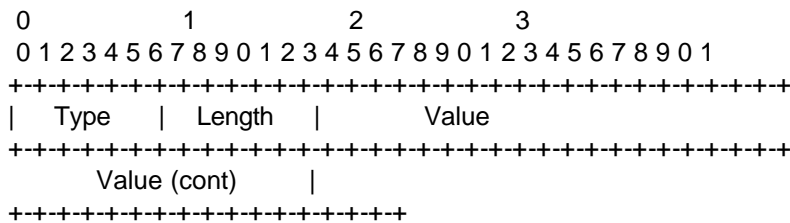
Address

The Address field is four octets. The value 0xFFFFFFFF indicates that the NAS SHOULD allow the user to select an address. The value 0 indicates that the NAS SHOULD select a host to connect the user to. Other values indicate the address the NAS SHOULD connect the user to.

### 5.15. Login-Service

This attribute indicates the service which should be used to connect the user to the login host. It is only used in Access-Accept packets.

A summary of the Login-Service Attribute format is shown below. The fields are transmitted from left to right.



Type

15 for Login-Service.

Length

6

Value

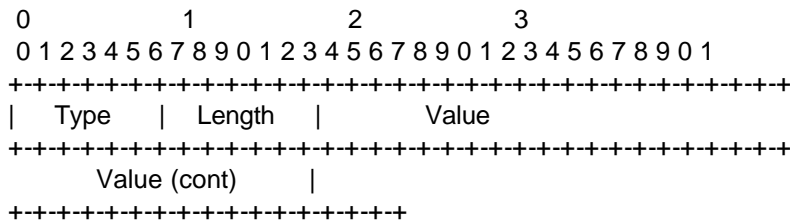
The Value field is four octets.

- 0 Telnet
- 1 Rlogin
- 2 TCP Clear
- 3 PortMaster (proprietary)
- 4 LAT

### 5.16. Login-TCP-Port

This attribute indicates the TCP port with which the user is to be connected when the Login-Service attribute is also present. It is only used in Access-Accept packets.

A summary of the Login-TCP-Port Attribute format is shown below. The fields are transmitted from left to right.



Type

16 for Login-TCP-Port.

Length

6

Value

The Value field is four octets. Despite the size of the field, values range from 0 to 65535.

### 5.17. (unassigned)

ATTRIBUTE TYPE 17 HAS NOT BEEN ASSIGNED.

### 5.18. Reply-Message

This attribute indicates text which MAY be displayed to the user.

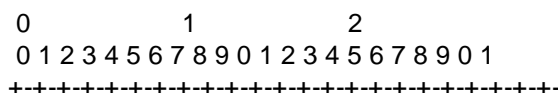
When used in an Access-Accept, it is the success message.

When used in an Access-Reject, it is the failure message. It MAY indicate a dialog message to prompt the user before another Access-Request attempt.

When used in an Access-Challenge, it MAY indicate a dialog message to prompt the user for a response.

Multiple Reply-Message's MAY be included and, if any are displayed, they **MUST** be displayed in the same order as they appear in the packet.

A summary of the Reply-Message Attribute format is shown below. The fields are transmitted from left to right.



```

| Type | Length | String ...
+++++

```

Type

18 for Reply-Message.

Length

>= 3

String

The String field is one or more octets, and its contents are implementation dependent. It is intended to be human readable, and **MUST NOT** affect operation of the protocol. It is recommended that the message contain displayable ASCII characters of values 10, 13, and 32 through 126 decimal. Mechanisms for extension to other character sets are beyond the scope of this specification.

### 5.19. Callback-Number

This attribute indicates a dialing string to be used for callback. It MAY be used in Access-Accept packets. It MAY be used in an Access-Request packet as a hint to the server that a Callback service is desired, but the server is not required to honor the hint.

A summary of the Callback-Number Attribute format is shown below. The fields are transmitted from left to right.

```

0          1          2
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+++++
| Type | Length | String ...
+++++

```

Type

19 for Callback-Number.

Length

>= 3

String

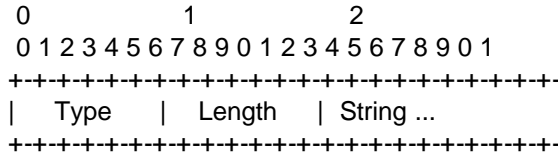
The String field is one or more octets. The actual format of the information is site- or application-specific, and a robust implementation SHOULD support the field as undistinguished octets.

The codification of the range of allowed usage of this field is outside the scope of this specification.

### 5.20. Callback-Id

This attribute indicates the name of a place to be called, to be interpreted by the NAS. It MAY be used in Access-Accept packets.

A summary of the Callback-Id Attribute format is shown below. The fields are transmitted from left to right.



Type

20 for Callback-Id.

Length

>= 3

String

The String field is one or more octets. The actual format of the information is site- or application-specific, and a robust implementation SHOULD support the field as undistinguished octets.

The codification of the range of allowed usage of this field is outside the scope of this specification.

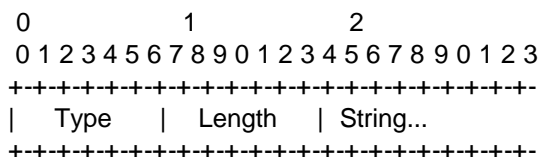
### 5.21. (unassigned)

ATTRIBUTE TYPE 21 HAS NOT BEEN ASSIGNED.

### 5.22. Framed-Route

This attribute provides routing information to be configured for the user on the NAS. It is used in the Access-Accept packet and can appear multiple times.

A summary of the Framed-Route Attribute format is shown below. The fields are transmitted from left to right.



Type

22 for Framed-Route.

Length

>= 3

String

The String field is one or more octets, and its contents are implementation dependent. It is intended to be human readable and **MUST NOT** affect operation of the protocol. It is recommended that the message contain displayable ASCII characters from the range 32 through 126 decimal.

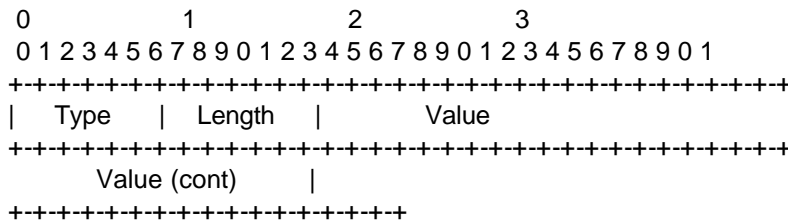
For IP routes, it **SHOULD** contain a destination prefix in dotted quad form optionally followed by a slash and a decimal length specifier stating how many high order bits of the prefix should be used. That is followed by a space, a gateway address in dotted quad form, a space, and one or more metrics separated by spaces. For example, "192.168.1.0/24 192.168.1.1 1 2 -1 3 400". The length specifier may be omitted in which case it should default to 8 bits for class A prefixes, 16 bits for class B prefixes, and 24 bits for class C prefixes. For example, "192.168.1.0 192.168.1.1 1".

Whenever the gateway address is specified as "0.0.0.0", the IP address of the user **SHOULD** be used as the gateway address.

### 5.23. Framed-IPX-Network

This attribute indicates the IPX Network number to be configured for the user. It is used in Access-Accept packets.

A summary of the Framed-IPX-Network Attribute format is shown below. The fields are transmitted from left to right.



Type

23 for Framed-IPX-Network.

Length

6

Value

The Value field is four octets. The value 0xFFFFFFFFE indicates that the NAS should select an IPX network for the user (e.g. assigned from a pool of one or more IPX networks kept by the NAS). Other values should be used as the IPX network for the link to the user.

### 5.24. State

This attribute is available to be sent by the server to the client in an Access-Challenge and **MUST** be sent unmodified from the client to the server in the new Access-Request reply to that challenge, if any.

This attribute is available to be sent by the server to the client in an Access-Accept that also includes a Termination-Action attribute with the value of RADIUS-Request. If the NAS performs the Termination-Action by sending a new Access-Request upon termination of the current session, it **MUST** include the State attribute unchanged in that Access-Request.

In either usage, no interpretation by the client should be made. A packet may have only one State Attribute. Usage of the State Attribute is implementation dependent.

A summary of the State Attribute format is shown below. The fields are transmitted from left to right.

```

0           1           2
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+++++
|  Type   |  Length  | String ...
+++++
```

Type

24 for State.

Length

>= 3

String

The String field is one or more octets. The actual format of the information is site- or application-specific, and a robust implementation SHOULD support the field as undistinguished octets.

The codification of the range of allowed usage of this field is outside the scope of this specification.

### 5.25. Class

This attribute is available to be sent by the server to the client in an Access-Accept and should be sent unmodified by the client to the accounting server as part of the Accounting-Request packet if accounting is supported. No interpretation by the client should be made.

A summary of the Class Attribute format is shown below. The fields are transmitted from left to right.

```

0           1           2
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+++++
|  Type   |  Length  | String ...
+++++
```

Type

25 for Class.

Length

>= 3

## String

The String field is one or more octets. The actual format of the information is site- or application-specific, and a robust implementation SHOULD support the field as undistinguished octets.

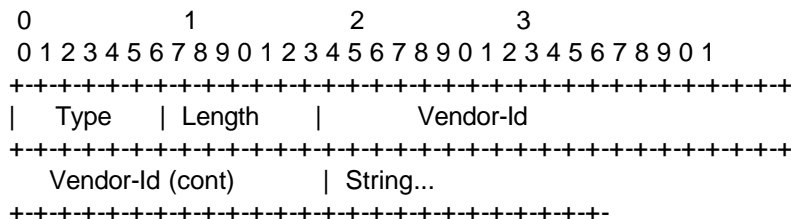
The codification of the range of allowed usage of this field is outside the scope of this specification.

### 5.26. Vendor-Specific

This attribute is available to allow vendors to support their own extended attributes not suitable for general usage. It **MUST** not affect the operation of the RADIUS protocol.

Servers not equipped to interpret the vendor-specific information sent by a client **MUST** ignore it (although it may be reported). Clients which do not receive desired vendor-specific information SHOULD make an attempt to operate without it, although they may do so (and report they are doing so) in a degraded mode.

A summary of the Vendor-Specific Attribute format is shown below. The fields are transmitted from left to right.



#### Type

26 for Vendor-Specific.

#### Length

>= 7

#### Vendor-Id

The high-order octet is 0 and the low-order 3 octets are the SMI Network Management Private Enterprise Code of the Vendor in network byte order, as defined in the Assigned Numbers RFC [3].

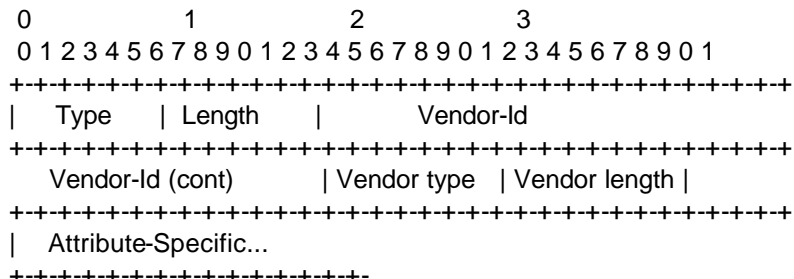
#### String

The String field is one or more octets. The actual format of the information is site- or application-specific, and a robust implementation SHOULD support the field as undistinguished octets.

The codification of the range of allowed usage of this field is outside the scope of this specification.



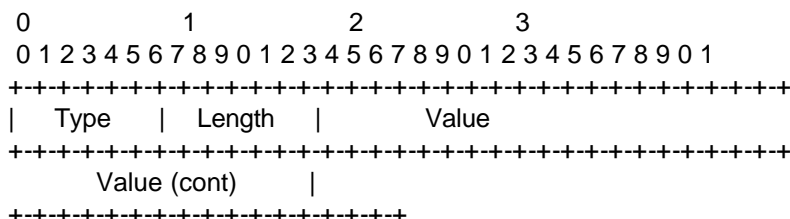
It SHOULD be encoded as a sequence of vendor type / vendor length/value fields, as follows. The Attribute-Specific field is dependent on the vendor's definition of that attribute. An example encoding of the Vendor-Specific attribute using this method follows:



### 5.27. Session-Timeout

This attribute sets the maximum number of seconds of service to be provided to the user before termination of the session or prompt. This attribute is available to be sent by the server to the client in an Access-Accept or Access-Challenge.

A summary of the Session-Timeout Attribute format is shown below. The fields are transmitted from left to right.



Type

27 for Session-Timeout.

Length

6

Value

The field is 4 octets, containing a 32-bit unsigned integer with the maximum number of seconds this user should be allowed to remain connected by the NAS.

### 5.28. Idle-Timeout

This attribute sets the maximum number of consecutive seconds of idle connection allowed to the user before termination of the session or prompt. This attribute is available to be sent by the server to the client in an Access-Accept or Access-Challenge.

A summary of the Idle-Timeout Attribute format is shown below. The fields are transmitted from left to right.



- 0 Default
- 1 RADIUS-Request

If the Value is set to RADIUS-Request, upon termination of the specified service, the NAS MAY send a new Access-Request to the RADIUS server, including the State attribute if any.

### 5.30. Called-Station-Id

This attribute allows the NAS to send in the Access-Request packet the phone number that the user called, using Dialed Number Identification (DNIS) or similar technology. Note that this may be different from the phone number the call comes in on. It is only used in Access-Request packets.

A summary of the Called-Station-Id Attribute format is shown below. The fields are transmitted from left to right.

0	1	2
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1		
+-----+		
Type	Length	String ...
+-----+		

Type

30 for Called-Station-Id.

Length

>= 3

String

The String field is one or more octets, containing the phone number that the user's call came in on.

The actual format of the information is site or application specific. Printable ASCII is recommended, but a robust implementation SHOULD support the field as undistinguished octets.

The codification of the range of allowed usage of this field is outside the scope of this specification.

### 5.31. Calling-Station-Id

This attribute allows the NAS to send in the Access-Request packet the phone number that the call came from, using Automatic Number Identification (ANI) or similar technology. It is only used in Access-Request packets.

A summary of the Calling-Station-Id Attribute format is shown below. The fields are transmitted from left to right.

0	1	2
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1		
+-----+		

```

| Type | Length | String ...
+++++
```

Type

31 for Calling-Station-Id.

Length

>= 3

String

The String field is one or more octets, containing the phone number that the user placed the call from.

The actual format of the information is site -or application-specific. Printable ASCII is recommended, but a robust implementation SHOULD support the field as undistinguished octets.

The codification of the range of allowed usage of this field is outside the scope of this specification.

### 5.32. NAS-Identifier

This attribute contains a string identifying the NAS originating the Access-Request. It is only used in Access-Request packets. Either NAS-IP-Address or NAS-Identifier SHOULD be present in an Access-Request packet.

A summary of the NAS-Identifier Attribute format is shown below. The fields are transmitted from left to right.

```

0          1          2
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+++++
| Type | Length | String ...
+++++
```

Type

32 for NAS-Identifier.

Length

>= 3

String

The String field is one or more octets, and should be unique to the NAS within the scope of the RADIUS server. For example, a fully qualified domain name would be suitable as a NAS-Identifier.

The actual format of the information is site- or application-specific, and a robust implementation SHOULD support the field as undistinguished octets.

The codification of the range of allowed usage of this field is outside the scope of this specification.

### 5.33. Proxy-State

This attribute is available to be sent by a proxy server to another server when forwarding an Access-Request and **MUST** be returned unmodified in the Access-Accept, Access-Reject or Access-Challenge. This attribute should be removed by the proxy server before the response is forwarded to the NAS.

Usage of the Proxy-State Attribute is implementation dependent. A description of its function is outside the scope of this specification.

A summary of the Proxy-State Attribute format is shown below. The fields are transmitted from left to right.

```

0           1           2
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-----+-----+-----+
| Type   | Length | String ...
+-----+-----+-----+
```

Type

33 for Proxy-State.

Length

>= 3

String

The String field is one or more octets. The actual format of the information is site or application specific, and a robust implementation SHOULD support the field as undistinguished octets.

The codification of the range of allowed usage of this field is outside the scope of this specification.

### 5.34. Login-LAT-Service

This attribute indicates the system with which the user is to be connected by LAT. It MAY be used in Access-Accept packets, but only when LAT is specified as the Login-Service. It MAY be used in an Access-Request packet as a hint to the server, but the server is not required to honor the hint.

Administrators use the service attribute when dealing with clustered systems, such as a VAX or Alpha cluster. In such an environment, several different time-sharing hosts share the same resources (disks, printers, etc.), and administrators often configure each to offer access (service) to each of the shared resources. In this case, each host in the cluster advertises its services through LAT broadcasts.

Sophisticated users often know which service providers (machines) are faster and tend to use a node name when initiating a LAT connection. Alternately, some administrators want particular users to use certain machines as a primitive form of load balancing (although LAT knows how to do load balancing itself).

A summary of the Login-LAT-Service Attribute format is shown below. The fields are transmitted from left to right.

```

      0          1          2
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-----+-----+-----+-----+-----+-----+
|  Type   | Length   | String ... |
+-----+-----+-----+-----+-----+-----+

```

Type

34 for Login-LAT-Service.

Length

>= 3

String

The String field is one or more octets, and contains the identity of the LAT service to use. The LAT Architecture allows this string to contain \$ (dollar), - (hyphen), . (period), \_ (underscore), numerics, upper and lower case alphabets, and the ISO Latin-1 character set extension [6]. All LAT string comparisons are case insensitive.

### 5.35. Login-LAT-Node

This attribute indicates the Node with which the user is to be automatically connected by LAT. It MAY be used in Access-Accept packets, but only when LAT is specified as the Login-Service. It MAY be used in an Access-Request packet as a hint to the server, but the server is not required to honor the hint.

A summary of the Login-LAT-Node Attribute format is shown below. The fields are transmitted from left to right.

```

      0          1          2
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-----+-----+-----+-----+-----+-----+
|  Type   | Length   | String ... |
+-----+-----+-----+-----+-----+-----+

```

Type

35 for Login-LAT-Node.

Length

>= 3

String

The String field is one or more octets, and contains the identity of the LAT Node to connect the user to. The LAT Architecture allows this string to contain \$ (dollar), - (hyphen), . (period), \_ (underscore), numerics, upper and lower case alphabets, and the ISO Latin-1 character set extension. All LAT string comparisons are case insensitive.

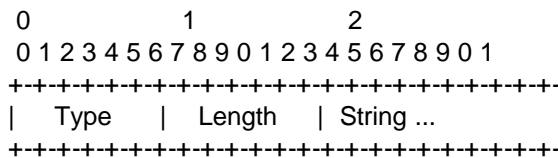
### 5.36. Login-LAT-Group

This attribute contains a string identifying the LAT group codes which this user is authorized to use. It MAY be used in Access- Accept packets, but only when LAT is specified as the Login-Service. It MAY be used in an Access-Request packet as a hint to the server, but the server is not required to honor the hint.

LAT supports 256 different group codes, which LAT uses as a form of access rights. LAT encodes the group codes as a 256 bit bitmap.

Administrators can assign one or more of the group code bits at the LAT service provider; it will only accept LAT connections that have these group codes set in the bit map. The administrators assign a bitmap of authorized group codes to each user; LAT gets these from the operating system, and uses these in its requests to the service providers.

A summary of the Login-LAT-Group Attribute format is shown below. The fields are transmitted from left to right.



Type

36 for Login-LAT-Group.

Length

34

String

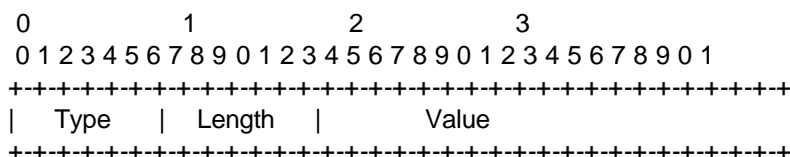
The String field is a 32 octet bit map, most significant octet first. A robust implementation SHOULD support the field as undistinguished octets.

The codification of the range of allowed usage of this field is outside the scope of this specification.

### 5.37. Framed-AppleTalk-Link

This attribute indicates the AppleTalk network number which should be used for the serial link to the user, which is another AppleTalk router. It is only used in Access-Accept packets. It is never used when the user is not another router.

A summary of the Framed-AppleTalk-Link Attribute format is shown below. The fields are transmitted from left to right.



```

      Value (cont) |
+-----+

```

Type

37 for Framed-AppleTalk-Link.

Length

6

Value

The Value field is four octets. Despite the size of the field, values range from 0 to 65535. The special value of 0 indicates that this is an unnumbered serial link. A value of 1-65535 means that the serial line between the NAS and the user should be assigned that value as an AppleTalk network number.

### 5.38. Framed-AppleTalk-Network

This attribute indicates the AppleTalk Network number which the NAS should probe to allocate an AppleTalk node for the user. It is only used in Access-Accept packets. It is never used when the user is another router. Multiple instances of this attribute indicate that the NAS may probe using any of the network numbers specified.

A summary of the Framed-AppleTalk-Network Attribute format is shown below. The fields are transmitted from left to right.

```

      0           1           2           3
      0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-----+
| Type  | Length |           Value
+-----+
      Value (cont) |
+-----+

```

Type

38 for Framed-AppleTalk-Network.

Length

6

Value

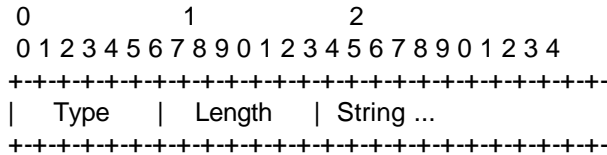
The Value field is four octets. Despite the size of the field, values range from 0 to 65535. The special value 0 indicates that the NAS should assign a network for the user, using its default cable range. A value between 1 and 65535 (inclusive) indicates the AppleTalk Network the NAS should probe to find an address for the user.

### 5.39. Framed-AppleTalk-Zone



This attribute indicates the AppleTalk Default Zone to be used for this user. It is only used in Access-Accept packets. Multiple instances of this attribute in the same packet are not allowed.

A summary of the Framed-AppleTalk-Zone Attribute format is shown below. The fields are transmitted from left to right.



Type

39 for Framed-AppleTalk-Zone.

Length

>= 3

String

The name of the Default AppleTalk Zone to be used for this user. A robust implementation SHOULD support the field as undistinguished octets.

The codification of the range of allowed usage of this field is outside the scope of this specification.

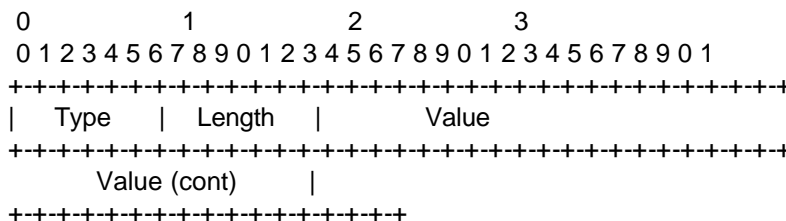
Below, you will find information from the RADIUS RFC 2139.

### 5.1. Acct-Status-Type

This Attribute indicates whether this Accounting-Request marks the beginning of the user service (Start) or the end (Stop).

It MAY be used by the client to mark the start of accounting (for example, upon booting) by specifying Accounting-On, and to mark the end of accounting (for example, just before a scheduled reboot) by specifying Accounting-Off.

A summary of the Acct-Status-Type attribute format is shown below. The fields are transmitted from left to right.



Type

40 for Acct-Status-Type.

Length

6

Value

The Value field is four octets.

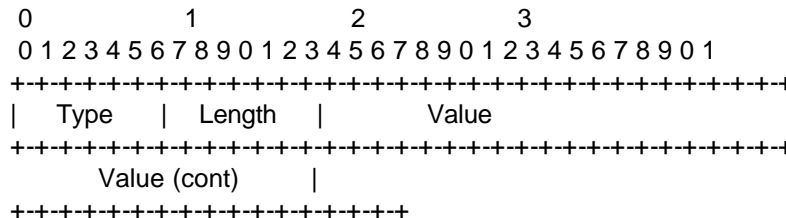
- 1 Start
- 2 Stop
- 7 Accounting-On
- 8 Accounting-Off

### 5.2. Acct-Delay-Time

This attribute indicates how many seconds the client has been trying to send this record, and can be subtracted from the time of arrival on the server to find the approximate time of the event generating this Accounting-Request. (Network transit time is ignored.)

Note that changing the Acct-Delay-Time causes the Identifier to change. See the discussion under Identifier, above.

A summary of the Acct-Delay-Time attribute format is shown below. The fields are transmitted from left to right.



Type

41 for Acct-Delay-Time.

Length

6

Value

The Value field is four octets.

### 5.3. Acct-Input-Octets

This attribute indicates how many octets have been received from the port over the course of this service being provided, and can only be present in Accounting-Request records where the Acct- Status-Type is set to Stop.

A summary of the Acct-Input-Octets attribute format is shown below. The fields are transmitted from left to right.

0						1						2						3													
0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1
+-----+																															
Type						Length						Value																			
+-----+																															
Value (cont)																															
+-----+																															

Type

42 for Acct-Input-Octets.

Length

6

Value

The Value field is four octets.

#### 5.4. Acct-Output-Octets

This attribute indicates how many octets have been sent to the port in the course of delivering this service, and can only be present in Accounting-Request records where the Acct-Status-Type is set to Stop.

A summary of the Acct-Output-Octets attribute format is shown below. The fields are transmitted from left to right.

0						1						2						3													
0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1
+-----+																															
Type						Length						Value																			
+-----+																															
Value (cont)																															
+-----+																															

Type

43 for Acct-Output-Octets.

Length

6

Value

The Value field is four octets.

#### 5.5. Acct-Session-Id

This attribute is a unique Accounting ID to make it easy to match start and stop records in a log file. The start and stop records for a given session **MUST** have the same Acct-Session-Id. It is strongly recommended that the Acct-Session-Id be a printable ASCII string.

For example, one implementation uses a string with an 8-digit upper case hexadecimal number, the first two digits increment on each reboot (wrapping every 256 reboots) and the next 6 digits counting from 0 for the first person logging in after a reboot up to  $2^{24}-1$ , about 16 million. Other encodings are possible.

A summary of the Acct-Session-Id attribute format is shown below. The fields are transmitted from left to right.

0	1	2
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3		
+-----+		
Type	Length	String ...
+-----+		

Type

44 for Acct-Session-Id.

Length

>= 3

String

The String field SHOULD be a string of printable ASCII characters.

## 5.6. Acct-Authentic

This attribute MAY be included in an Accounting-Request to indicate how the user was authenticated, whether by RADIUS, the NAS itself, or another remote authentication protocol. Users who are delivered service without being authenticated SHOULD NOT generate Accounting records.

A summary of the Acct-Authentic attribute format is shown below. The fields are transmitted from left to right.

0	1	2	3
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1			
+-----+			
Type	Length	Value	
+-----+			
Value (cont)			
+-----+			

Type

45 for Acct-Authentic.

Length

6

Value

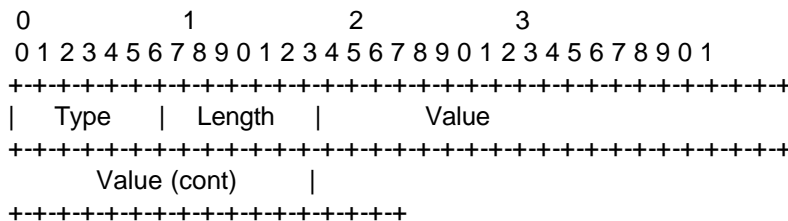
The Value field is four octets.

- 1 RADIUS
- 2 Local
- 3 Remote

### 5.7. Acct-Session-Time

This attribute indicates how many seconds the user has received service for, and can only be present in Accounting-Request records where the Acct-Status-Type is set to Stop.

A summary of the Acct-Session-Time attribute format is shown below. The fields are transmitted from left to right.



Type

46 for Acct-Session-Time.

Length

6

Value

The Value field is four octets.

### 5.8. Acct-Input-Packets

This attribute indicates how many packets have been received from the port over the course of the service being provided to a Framed User, and can only be present in Accounting-Request records where the Acct-Status-Type is set to Stop.

A summary of the Acct-Input-packets attribute format is shown below. The fields are transmitted from left to right.

0	1	2	3																		
0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1
+-----+																					
Type				Length				Value													
+-----+																					
Value (cont)																					
+-----+																					

Type

47 for Acct-Input-Packets.

Length

6

Value

The Value field is four octets.

### 5.9. Acct-Output-Packets

This attribute indicates how many packets have been sent to the port in the course of delivering this service to a Framed User, and can only be present in Accounting-Request records where the Acct-Status-Type is set to Stop.

A summary of the Acct-Output-Packets attribute format is shown below. The fields are transmitted from left to right.

0	1	2	3																		
0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1
+-----+																					
Type				Length				Value													
+-----+																					
Value (cont)																					
+-----+																					

Type

48 for Acct-Output-Packets.

Length

6

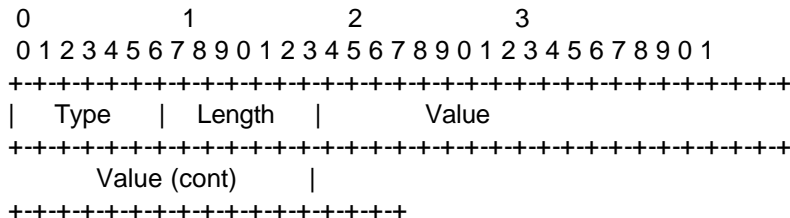
Value

The Value field is four octets.

### 5.10. Acct-Terminate-Cause

This attribute indicates how the session was terminated, and can only be present in Accounting-Request records where the Acct- Status-Type is set to Stop.

A summary of the Acct-Terminate-Cause attribute format is shown below. The fields are transmitted from left to right.



Type

49 for Acct-Terminate-Cause

Length

6

Value

The Value field is four octets, containing an integer specifying the cause of session termination, as follows:

- 1 User Request
- 2 Lost Carrier
- 3 Lost Service
- 4 Idle Timeout
- 5 Session Timeout
- 6 Admin Reset
- 7 Admin Reboot
- 8 Port Error
- 9 NAS Error
- 10 NAS Request
- 11 NAS Reboot
- 12 Port Unneeded
- 13 Port Preempted
- 14 Port Suspended
- 15 Service Unavailable
- 16 Callback
- 17 User Error
- 18 Host Request

The termination causes are as follows:

User Request

User requested termination of service; for example, with LCP Terminate or by logging out.

Lost Carrier  
DCD was dropped on the port.

Lost Service  
Service can no longer be provided; for example, the user's connection to a host was interrupted.

Idle Timeout  
Idle timer expired.

Session Timeout  
Maximum session length timer expired.

Admin Reset  
Administrator reset the port or session.

Admin Reboot  
Administrator is ending service on the NAS; for example, prior to rebooting the NAS.

Port Error  
NAS detected an error on the port. This required ending the session.

NAS Error  
NAS detected some error (other than on the port) which required ending the session.

NAS Request  
NAS ended the session for a non-error reason not otherwise listed here.

NAS Reboot  
The NAS ended the session in order to reboot non-administratively ("crash").

Port Unneeded  
NAS ended the session because resource usage fell below the low-water mark (for example, if a bandwidth-on-demand algorithm decided that the port was no longer needed).

Port Preempted  
NAS ended the session in order to allocate the port to a higher priority use.

Port Suspended  
NAS ended the session to suspend a virtual session.

Service Unavailable  
NAS was unable to provide the requested service.

Callback  
NAS is terminating the current session in order to perform callback for a new session.

User Error  
Input from the user is in error, causing termination of the session.

Host Request



Login Host terminated the session normally.

### 5.11. Acct-Multi-Session-Id

This attribute is a unique Accounting ID to make it easy to link multiple related sessions in a log file. Each linked session would have a unique Acct-Session-Id, but the same Acct-Multi-Session-Id. It is strongly recommended that the Acct- Multi-Session-Id be a printable ASCII string.

A summary of the Acct-Session-Id Attribute format is shown below. The fields are transmitted from left to right.

0	1	2
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3		
+-----+		
Type	Length	String ...
+-----+		

Type

50 for Acct-Multi-Session-Id.

Length

>= 3

String

The String field SHOULD be a string of printable ASCII characters.

### 5.12. Acct-Link-Count

This attribute gives the count of links which are known to have been in a given multilink session at the time the accounting record is generated. The NAS MAY include the Acct-Link-Count attribute in any Accounting-Request which might have multiple links.

A summary of the Acct-Link-Count Attribute format is show below. The fields are transmitted from left to right.

0	1	2	3
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1			
+-----+			
Type	Length	Value	
+-----+			
Value (cont)			
+-----+			

Type

51 for Acct-Link-Count.

Length

6

Value

The Value field is four octets, and contains the number of links seen so far in this Multilink Session.

It may be used to make it easier for an accounting server to know when it has all the records for a given Multilink session. When the number of Accounting-Requests received with Acct-Status-Type = Stop and the same Acct-Multi-Session-Id and unique Acct-Session- Id's equals the largest value of Acct-Link-Count seen in those Accounting-Requests, all Stop Accounting-Requests for that Multilink Session have been received.

An example showing 8 Accounting-Requests should make things clearer. For clarity only the relevant attributes are shown, but additional attributes containing accounting information will also be present in the Accounting-Request.

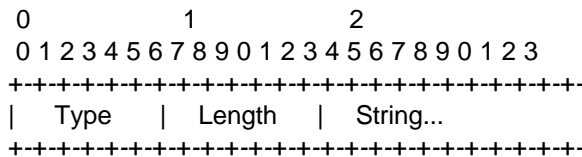
Multi-Session-Id	Session-Id	Status-Type	Link-Count
"10"	"10"	Start	1
"10"	"11"	Start	2
"10"	"11"	Stop	2
"10"	"12"	Start	3
"10"	"13"	Start	4
"10"	"12"	Stop	4
"10"	"13"	Stop	4
"10"	"10"	Stop	4

#### 5.40. CHAP-Challenge

This attribute contains the CHAP Challenge sent by the NAS to a PPP Challenge-Handshake Authentication Protocol (CHAP) user. It is only used in Access-Request packets.

If the CHAP challenge value is 16 octets long, it MAY be placed in the Request Authenticator field instead of using this attribute.

A summary of the CHAP-Challenge Attribute format is shown below. The fields are transmitted from left to right.



Type

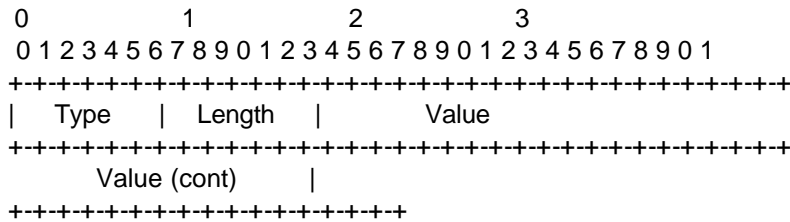
60 for CHAP-Challenge.

Length

>= 7

String





Type

62 for Port-Limit.

Length

6

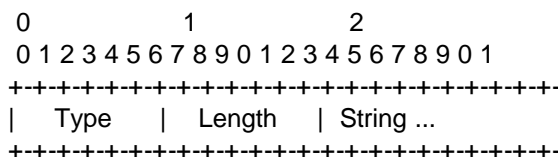
Value

The field is 4 octets, containing a 32-bit unsigned integer with the maximum number of ports this user should be allowed to connect to on the NAS.

### 5.43. Login-LAT-Port

This attribute indicates the Port with which the user is to be connected by LAT. It MAY be used in Access-Accept packets, but only when LAT is specified as the Login-Service. It MAY be used in an Access-Request packet as a hint to the server, but the server is not required to honor the hint.

A summary of the Login-LAT-Port Attribute format is shown below. The fields are transmitted from left to right.



Type

63 for Login-LAT-Port.

Length

>= 3

String

The String field is one or more octets, and contains the identity of the LAT port to use. The LAT Architecture allows this string to contain \$ (dollar), - (hyphen), . (period), \_ (underscore), numerics, upper and lower case alphabetic, and the ISO Latin-1 character set extension. All LAT string comparisons are case insensitive.

### 5.44. Table of Attributes

The following table provides a guide to the attributes found in which kinds of packets, and in what quantity:

**RFC 2138 RADIUS**

Request	Accept	Reject	Challenge	#	Attribute
1	0	0	0	1	User-Name
0-1	0	0	0	2	User-Password [Note 1]
0-1	0	0	0	3	CHAP-Password[Note 1]
0-1	0	0	0	4	NAS-IP-Address
0-1	0	0	0	5	NAS-Port
0-1	0-1	0	0	6	Service-Type
0-1	0-1	0	0	7	Framed-Protocol
0-1	0-1	0	0	8	Framed-IP-Address
0-1	0-1	0	0	0	Framed-IP-Netmask
0	0-1	0	0	10	Framed-Routing
0	0+	0	0	11	Filter-Id
0	0-1	0	0	12	Framed-MTU
0+	0+	0	0	13	Framed-Compression
0+	0+	0	0	14	Login-IP-Host
0	0-1	0	0	15	Login-Service
0	0-1	0	0	16	Login-TCP-Port
0	0+	0+	0+	18	Reply-Message
0-1	0-1	0	0	19	Callback-Number
0	0-1	0	0	20	Callback-Id
0	0+	0	0	22	Framed-Route
0	0-1	0	0	23	Framed-IPX-Network
0-1	0-1	0	0-1	24	State
0	0+	0	0	25	Class
0+	0+	0	0+	26	Vendor-Specific
0	0-1	0	0-1	27	Session-Timeout
0	0-1	0	0-1	28	Idle-Timeout
0	0-1	0	0	29	Termination-Action
0-1	0	0	0	30	Called-Station-Id
0-1	0	0	0	31	Calling-Station-Id
0-1	0	0	0	32	NAS-Identifier
0+	0+	0+	0+	33	Proxy-State
0-1	0-1	0	0	34	Login-LAT-Service
0-1	0-1	0	0	35	Login-LAT-Node
0-1	0-1	0	0	36	Login-LAT-Group
0	0-1	0	0	37	Framed-AppleTalk-Link
0	0+	0	0	38	Framed-AppleTalk-Network
0	0-1	0	0	39	Framed-AppleTalk-Zone
0-1	0	0	0	60	CHAP-Challenge
0-1	0	0	0	61	NAS-Port-Type
0-1	0-1	0	0	62	Port-Limit
0-1	0-1	0	0	63	Login-LAT-Port

[Note 1] An Access-Request **MUST** contain either a User-Password or a CHAP-Password, and **MUST NOT** contain both.

The following table defines the meaning of the above table entries:

- 0 This attribute **MUST NOT** be present in packet.
- 0+ Zero or more instances of this attribute **MAY** be present in packet.
- 0-1 Zero or one instance of this attribute **MAY** be present in packet.
- 1 Exactly one instance of this attribute **MUST** be present in packet.

### 5.13. Table of Attributes

The following table provides a guide to which attributes may be found in Accounting-Request packets. No attributes should be found in Accounting-Response packets except Proxy-State and possibly Vendor-specific.

## **RFC 2139 RADIUS Accounting**

#	Attribute
0-1	User-Name
0	User-Password
0	CHAP-Password
0-1	NAS-IP-Address [5]
0-1	NAS-Port
0-1	Service-Type
0-1	Framed-Protocol
0-1	Framed-IP-Address
0-1	Framed-IP-Netmask
0-1	Framed-Routing
0+	Filter-Id
0-1	Framed-MTU
0+	Framed-Compression
0+	Login-IP-Host
0-1	Login-Service
0-1	Login-TCP-Port
0	Reply-Message
0-1	Callback-Number
0-1	Callback-Id
0+	Framed-Route
0-1	Framed-IPX-Network
0	State
0+	Class
0+	Vendor-Specific
0-1	Session-Timeout
0-1	Idle-Timeout
0-1	Termination-Action
0-1	Called-Station-Id

0-1	Calling-Station-Id
0-1	NAS-Identifier [4]
0+	Proxy-State
0-1	Login-LAT-Service
0-1	Login-LAT-Node
0-1	Login-LAT-Group
0-1	Framed-AppleTalk-Link
0-1	Framed-AppleTalk-Network
0-1	Framed-AppleTalk-Zone
1	Acct-Status-Type
0-1	Acct-Delay-Time
0-1	Acct-Input-Octets
0-1	Acct-Output-Octets
1	Acct-Session-Id
0-1	Acct-Authentic
0-1	Acct-Session-Time
0-1	Acct-Input-Packets
0-1	Acct-Output-Packets
0-1	Acct-Terminate-Cause
0+	Acct-Multi-Session-Id
0+	Acct-Link-Count
0	CHAP-Challenge
0-1	NAS-Port-Type
0-1	Port-Limit
0-1	Login-LAT-Port

[5] An Accounting-Request **MUST** contain either a NAS-IP-Address or a NAS-Identifier, and it is permitted (but not recommended) for it to contain both.

The following table defines the above table entries:

- 0 This attribute **MUST NOT** be present
- 0+ Zero or more instances of this attribute **MAY** be present.
- 0-1 Zero or one instance of this attribute **MAY** be present.
- 1 Exactly one instance of this attribute **MUST** be present.

## Appendix B – EMERALD UPDATE



Emerald Version 2.5 is, by default, packaged with a Standard edition of RadiusNT, although there have always been RadiusNT server upgrade options available. The upcoming release of the Emerald Management Suite, Version 4.0, will be packaged with either the Standard, Professional, or Enterprise edition of Radius 4.0, depending upon the Emerald edition purchased.

Existing Emerald 2.5 customers who have previously upgrading to RadiusNT version 3.0 or 4.0 will be able to continue using Emerald 2.5 after they have upgraded their RadiusNT server. The Radius install/upgrade however, needs to occur after the installation of the Emerald software.

For Emerald Management Suite users, this section will describe additional steps needed for the new version 4.0 of RadiusNT/X to work with your existing installation. If you have any questions, or need additional information regarding the Emerald Management Suite or RadiusNT or RadiusX products, please contact our Sales department at [Sales@iea-software.com](mailto:Sales@iea-software.com).

### ***Update Script for Emerald Users***

For those who are using Emerald 2.5 and are upgrading to Radius version 4.0, you will need to run the 4.0 SQL Server upgrade script ***emer25\_up.sql*** that was included with the distribution archive. To run the script, please do the following:

1. Run the SQL Server Query Analyzer application (SQL Server 7.0+).
2. **Connect** to the server you are using.
3. Click the **Load SQL Script** icon. 
4. Browse to locate the ***emer25\_up.sql*** file, then click **Open**. The script is typically in the directory where you installed RadiusNT.
5. Click the **Execute Query** icon. 
6. **Restart** RadiusNT and Emerald.

### ***Configuring ODBC***

If you are using the Emerald Management Suite, you will need to set up RadiusNT/X in ODBC mode. The ODBC DSN needs to point to the Emerald database you created with the Emerald Administrator.



Configuring your RadiusNT/X server for ODBC mode and the steps necessary to prepare your system are described in Chapter 2 of this document on RadiusNT/X Modes. The Emerald Administrator's Guide also provides information on how to correctly set up your system for ODBC configuration.

Before RadiusNT/X will run with Emerald, you must configure the Radius options within the Emerald Administrator. Within the Emerald Administrator select the **Admin/Radius** option and consult the Emerald Administrator's guide for instructions on how to configure your RadiusNT/X options. Primarily, you will need to select the Servers option and add an entry for *each* of your NAS before the RadiusNT/X server will be able to run.

Next, start the RadiusNT/X server. Execute the following command within the Radius installation directory to start RadiusNT in full debug mode: "radius -x15 (Windows)" or "radiusd -x15 (on Unix/Linux).

If everything is configured correctly, a "waiting for requests" line will be returned. RadiusNT/X will return error messages in the case that something is not configured correctly. If this occurs, please go back and check your RadiusNT/X configuration options.

Please remember that, for RadiusNT/X to work correctly with Emerald, you **must** have already done the following steps:

1. Used the Emerald Administrator to create the Emerald database on your SQL Server.
2. Created an ODBC datasource called Emerald. Please note that it **must** be a ODBC system data source and it **must** be pointed to the Emerald database you created.
3. Specified correct login information in the RadiusNT/X Administrator to allow RadiusNT/X to log in to the SQL Server.

## Tables

Please note the following information that pertains only to Emerald installations.

<b>Accounting Manual Calls Update</b>	RadiusNT/X will manually update the ServerPorts table. This is only needed for databases that do not have trigger support . The option is <b>not</b> needed with Emerald/SQL Server or an active database that can update the Calls Online view automatically.
---	--

<b>Manual Service Update</b>	In order for Time Banking to work, RadiusNT/X will manually update the user's time left information. This option is <b>not</b> needed with Emerald or an active database that can update the Subaccounts table automatically.
------------------------------	---

<b>Master Accounts Table</b>	*OverLimit	Money	If the Balance field is less than this field, the account will <b>not</b> be authenticated. Please note that this option is only used by Emerald.
	*Balance	Money	See the Overlimit field above. Please note that this option is only used by Emerald.



## Stored Procedures

Below is a list of the stored procedures that Emerald provides for RadiusNT/X to use. The parameters and returned columns **must** be of the same type, but the stored procedures can be modified to the database design if you are not using Emerald.

```
CREATE PROCEDURE RadCheckServer @rrsid int AS
Select Server, IPAddress, Secret, AuthPort, AcctPort, 0, Timeout, Retries, StripDomain,
TreatAsLocal, NULL
From RadRoamServers
Where RadRoamServerID = @rrsid
```

```
CREATE PROCEDURE RadCheckOnline @UserName varchar(64) AS
Select Count(Username) From CallsOnline Where Username=@UserName and
AcctStatusType=1
```

```
CREATE PROCEDURE RadCheckPort @nasid varchar(16), @nasport integer, @at varchar(15)
AS
Select MaxSessionLength, StartTime, StopTime, CurrTime = (DatePart(Hour, GetDate()) * 60) +
DatePart(Minute, GetDate())
From Servers s, ServerAccess sa
Where s.ServerID = sa.ServerID AND s.IPAddress = @nasid AND (sa.Port=@nasport or
sa.Port=NULL)
AND sa.AccountType = @at
```

```
CREATE PROCEDURE RadCheckTrigger @AccountID int AS
Select FileName, Parameters, Directory, Type from RadTriggers Where
AccountID=@AccountID
```

```
CREATE PROCEDURE RadGetConfigs @AccountID int AS
Select ra.RadAttributeID, Name, Data, Value, Type, rc.RadVendorID, rc.RadVendorType,
rc.RadCheck
From RadConfigs rc, RadAttributes ra
Where ra.RadAttributeID=rc.RadAttributeID AND rc.AccountID = @AccountID
```

```
CREATE PROCEDURE RadUserDefaults AS
SELECT rc.AccountType, ra.RadAttributeID, ra.Type, rc.Data, rc.Value, rc.RadVendorID,
rc.RadVendorType, rc.RadCheck
From RadAttributes ra, RadATConfigs rc
Where ra.RadAttributeID = rc.RadAttributeID
Order By AccountType, RadCheck, ra.RadAttributeID
```

```
CREATE PROCEDURE RadUserSpecifics AS
SELECT rc.AccountID, ra.RadAttributeID, ra.Type, rc.Data, rc.Value, rc.RadVendorID,
rc.RadVendorType, rc.RadCheck
From RadAttributes ra, RadConfigs rc
Where ra.RadAttributeID = rc.RadAttributeID
Order By AccountID, RadCheck, ra.RadAttributeID
```

```
CREATE PROCEDURE RadAtCache @accounttype VARCHAR(16) AS
```

```

SELECT rc.AccountType, ra.RadAttributeID, Name, Data, Value, Type, rc.RadVendorID,
rc.RadVendorType, rc.RadCheck
FROM RadATConfigs rc, RadAttributes ra
WHERE ra.RadAttributeID = rc.RadAttributeID
      AND (ra.RadVendorID = rc.RadVendorID OR rc.RadVendorID IS NULL)
      AND (ra.RadVendorType = rc.RadVendorType OR rc.RadVendorType IS NULL)
      AND (@accounttype IS NULL OR AccountType = @accounttype)
ORDER BY AccountType
GO

```

```

CREATE PROCEDURE RadServerAccessCache AS
Select MaxSessionLength, StartTime, StopTime, s.IPAddress, sa.Port, sa.AccountType
From Servers s, ServerAccess sa
  WHERE s.ServerID = sa.ServerID
GO

```

```

CREATE PROCEDURE RadDNISCache AS
Select at1.AccountType, dn.DNISNumber
FROM AccountTypes at1, DNISNumbers dn
  WHERE at1.DNISGroupID = dn.DNISGroupID
GO

```

```

CREATE PROCEDURE RadRoamCache AS
Select Domain AS Label, Server, IPAddress, Secret, AuthPort, AcctPort,
Priority, Timeout, Retries, StripDomain, TreatAsLocal, AccountType
From RadRoamDomains rrd, RadRoamServers rrs
  Where rrd.RadRoamServerID = rrs.RadRoamServerID
UNION
Select rrd2.Domain AS Label, Server, IPAddress, Secret, AuthPort,
AcctPort, rrd.Priority, Timeout, Retries, StripDomain, TreatAsLocal,
rrd.AccountType
From RadRoamDomains rrd, RadRoamServers rrs, RadRoamDomains rrd2
  Where rrd.RadRoamServerID = rrs.RadRoamServerID
  AND rrd.Domain = 'DEFAULT'
UNION
Select CONVERT(VARCHAR(5),RadRoamServerID) AS Label, Server, IPAddress,
Secret, AuthPort, AcctPort, 0, Timeout, Retries, StripDomain,
TreatAsLocal, NULL
From RadRoamServers
Order By Label,Priority
GO

```

```

CREATE PROCEDURE RadGetCacheUsers @date DATETIME, @flag TINYINT AS
SELECT sa.AccountID, sa.Login, sa.Password, d.MailDomain, sa.AccountType, sa.LoginLimit,
sa.TimeLeft,
MasterExpire=DateAdd(Day, ma.Extension+ma.OverDue+1, ma.ExpireDate),
SubExpire=DateAdd(Day, sa.Extension+1, sa.ExpireDate),
OverLimit=CASE WHEN (ma.OverLimit > 0 AND ma.OverLimit > ma.Balance) THEN 1 ELSE 0
END
FROM SubAccounts sa, MasterAccounts ma, Domains d, Groups g
  WHERE sa.CustomerID = ma.CustomerID
  AND d.DomainID = g.DomainID

```

```

        AND ma.GroupID = g.GroupID
        AND sa.Active <> 0
        AND ma.Active <> 0
        AND sa.Login <> "
        AND ((@flag = 1 AND sa.LastModifyDate > @date)
             OR (@flag = 2 AND (sa.LastUsed > @date OR sa.LastUsed IS NULL)))
UNION
SELECT sa.AccountID, sa.Email, sa.Password, d.MailDomain, sa.AccountType, sa.LoginLimit,
sa.TimeLeft,
MasterExpire=DateAdd(Day, ma.Extension+ma.OverDue+1, ma.ExpireDate),
SubExpire=DateAdd(Day, sa.Extension+1, sa.ExpireDate),
OverLimit=CASE WHEN (ma.OverLimit > 0 AND ma.OverLimit > ma.Balance) THEN 1 ELSE 0
END
FROM SubAccounts sa, MasterAccounts ma, Domains d, Groups g
    WHERE sa.CustomerID = ma.CustomerID
        AND d.DomainID = g.DomainID
        AND ma.GroupID = g.GroupID
        AND sa.Active <> 0
        AND ma.Active <> 0
        AND sa.Email <> "
        AND ((@flag = 1 AND sa.LastModifyDate > @date)
             OR (@flag = 2 AND (sa.LastUsed > @date OR sa.LastUsed IS NULL)))
GO

CREATE PROCEDURE RadGetUser @user VARCHAR(64) , @password VARCHAR(32) AS
SELECT sa.AccountID, sa.Login, sa.Password, d.MailDomain, sa.AccountType, sa.LoginLimit,
sa.TimeLeft,
MasterExpire=DateAdd(Day, ma.Extension+ma.OverDue+1, ma.ExpireDate),
SubExpire=DateAdd(Day, sa.Extension+1, sa.ExpireDate) ,
OverLimit=CASE WHEN (ma.OverLimit > 0 AND ma.OverLimit > ma.Balance) THEN 1 ELSE 0
END
FROM SubAccounts sa, MasterAccounts ma, Domains d, Groups g
    WHERE sa.CustomerID = ma.CustomerID
        AND d.DomainID = g.DomainID
        AND ma.GroupID = g.GroupID
        AND sa.Active <> 0
        AND ma.Active <> 0
        AND sa.Login = @user
        AND (@password IS NULL OR sa.Password = @password)
UNION
SELECT sa.AccountID, sa.Email, sa.Password, d.MailDomain, sa.AccountType, sa.LoginLimit,
sa.TimeLeft,
MasterExpire=DateAdd(Day, ma.Extension+ma.OverDue+1, ma.ExpireDate),
SubExpire=DateAdd(Day, sa.Extension+1, sa.ExpireDate),
OverLimit=CASE WHEN (ma.OverLimit > 0 AND ma.OverLimit > ma.Balance) THEN 1 ELSE 0
END
FROM SubAccounts sa, MasterAccounts ma, Domains d, Groups g
    WHERE sa.CustomerID = ma.CustomerID
        AND d.DomainID = g.DomainID
        AND ma.GroupID = g.GroupID
        AND sa.Active <> 0
        AND ma.Active <> 0

```

```

        AND sa.Email = @user
        AND (@password IS NULL OR sa.Password = @password)
GO
CREATE PROCEDURE RadGetCacheUsers @date DATETIME, @flag TINYINT AS
SELECT sa.AccountID, sa.Login, sa.Password, d.MailDomain, sa.AccountType, sa.LoginLimit,
sa.TimeLeft,
MasterExpire=DateAdd(Day, ma.Extension+ma.OverDue+1, ma.ExpireDate),
SubExpire=DateAdd(Day, sa.Extension+1, sa.ExpireDate),
OverLimit=CASE WHEN (ma.OverLimit > 0 AND ma.OverLimit > ma.Balance) THEN 1 ELSE 0
END
FROM SubAccounts sa, MasterAccounts ma, Domains d, Groups g
    WHERE sa.CustomerID = ma.CustomerID
        AND d.DomainID = g.DomainID
        AND ma.GroupID = g.GroupID
        AND sa.Active <> 0
        AND ma.Active <> 0
        AND sa.Login <> "
        AND ((@flag = 1 AND sa.LastModifyDate > @date)
            OR (@flag = 2 AND (sa.LastUsed > @date OR sa.LastUsed IS NULL)))
UNION
SELECT sa.AccountID, sa.Email, sa.Password, d.MailDomain, sa.AccountType, sa.LoginLimit,
sa.TimeLeft,
MasterExpire=DateAdd(Day, ma.Extension+ma.OverDue+1, ma.ExpireDate),
SubExpire=DateAdd(Day, sa.Extension+1, sa.ExpireDate),
OverLimit=CASE WHEN (ma.OverLimit > 0 AND ma.OverLimit > ma.Balance) THEN 1 ELSE 0
END
FROM SubAccounts sa, MasterAccounts ma, Domains d, Groups g
    WHERE sa.CustomerID = ma.CustomerID
        AND d.DomainID = g.DomainID
        AND ma.GroupID = g.GroupID
        AND sa.Active <> 0
        AND ma.Active <> 0
        AND sa.Email <> "
        AND ((@flag = 1 AND sa.LastModifyDate > @date)
            OR (@flag = 2 AND (sa.LastUsed > @date OR sa.LastUsed IS NULL)))
GO

CREATE PROCEDURE RadGetUser @user VARCHAR(64) , @password VARCHAR(32) AS
SELECT sa.AccountID, sa.Login, sa.Password, d.MailDomain, sa.AccountType, sa.LoginLimit,
sa.TimeLeft,
MasterExpire=DateAdd(Day, ma.Extension+ma.OverDue+1, ma.ExpireDate),
SubExpire=DateAdd(Day, sa.Extension+1, sa.ExpireDate) ,
OverLimit=CASE WHEN (ma.OverLimit > 0 AND ma.OverLimit > ma.Balance) THEN 1 ELSE 0
END
FROM SubAccounts sa, MasterAccounts ma, Domains d, Groups g
    WHERE sa.CustomerID = ma.CustomerID
        AND d.DomainID = g.DomainID
        AND ma.GroupID = g.GroupID
        AND sa.Active <> 0
        AND ma.Active <> 0
        AND sa.Login = @user
        AND (@password IS NULL OR sa.Password = @password)

```

```

UNION
SELECT sa.AccountID, sa.Email, sa.Password, d.MailDomain, sa.AccountType, sa.LoginLimit,
sa.TimeLeft,
MasterExpire=DateAdd(Day, ma.Extension+ma.OverDue+1, ma.ExpireDate),
SubExpire=DateAdd(Day, sa.Extension+1, sa.ExpireDate),
OverLimit=CASE WHEN (ma.OverLimit > 0 AND ma.OverLimit > ma.Balance) THEN 1 ELSE 0
END
FROM SubAccounts sa, MasterAccounts ma, Domains d, Groups g
WHERE sa.CustomerID = ma.CustomerID
AND d.DomainID = g.DomainID
AND ma.GroupID = g.GroupID
AND sa.Active <> 0
AND ma.Active <> 0
AND sa.Email = @user
AND (@password IS NULL OR sa.Password = @password)
GO

```

## ***Emerald Integration FAQs***

?? *When using RadiusNT/X with Emerald, what license information do I use?*

When using RadiusNT/X in conjunction with Emerald, there is no need to configure a license in the RadiusNT/X Administrator. Once you have configured RadiusNT for ODBC mode and it is pointing to your Emerald database, RadiusNT/X uses your Emerald license. Please note that you do need to enter your Emerald license in the Emerald Administrator.

?? *Can I set up a backup copy of RadiusNT/X that does not connect to my Emerald database?*

Yes. To accomplish this, enter one of your Emerald license keys into the RadiusNTX Administrator. In addition, you may use the Emerald client to export a *users* file from your Emerald database for use in this situation.

?? *How can I put my Calls table into another database when I am using Emerald?*

Please note that this process requires an **in-depth** working knowledge of Microsoft SQL Server **and** Enterprise Manager.

1. Begin by right clicking over the current Calls table and then select **Indexes**. This selection shows the number of records and the size of your Calls table. Please use this information below.
2. Create two Database Devices, EmerCallsDev and EmerCallsLog. The first will be based on the size of the Calls table, discovered in step 1. Please add additional space for growing capacity. As a general rule, the EmerCallsLogs should be approximately 20% of the size of the EmerCallsDev (For example, 200mb and 40mb, respectively).
3. Next, create a database named EmerCalls with Data Device EmerCallsDev and Log Device EmerCallsLog. Use the full size of each.

4. Use SQL EM to revoke INSERT permissions for RadiusNT/X on your current Calls table. This will prevent RADIUS from writing to Calls during the transfer.
5. You will use SQL EM to transfer your Calls table from your Emerald database to your EmeraldCalls database. Transfer **just** the Calls table, **not** the whole database.
6. In Manage Logins (SQL EM), give each Emerald user "permit" permission for the EmerCalls database (public group). Under the EmeraldCalls database, select "groups/users" and "public", then right click to select permissions. Select "grant all", "Set" and finally "close".
7. Next, right click over the **new** Calls Table (in the EmerCalls database) and select Triggers.
8. Cut and then paste the following information in as the trigger:

```

CREATE TRIGGER calls_insert ON dbo.Calls
FOR INSERT
AS
    UPDATE Emerald..ServerPorts
        Set sp.UserName = i.UserName,
            sp.AcctStatusType = i.AcctStatusType,
            sp.CallDate = DateAdd(Second, 0-i.AcctDelayTime, i.CallDate),
            sp.FramedAddress = i.FramedAddress,
            sp.ConnectInfo = i.ConnectInfo
    FROM Emerald..Servers s, Emerald..ServerPorts sp, inserted i
    WHERE s.IPAddress = i.NASIdentifier AND
           s.ServerID = sp.ServerID AND
           sp.Port = i.NASPort AND
           DateAdd(Second, 0-i.AcctDelayTime, i.CallDate) >= sp.CallDate

    UPDATE Emerald..SubAccounts
        Set sa.TimeLeft = sa.TimeLeft - (i.AcctSessionTime/60 + 1)
    FROM Emerald..SubAccounts sa, inserted i
    WHERE sa.login = i.UserName
           and sa.TimeLeft <> NULL
           and i.AcctStatusType = 2

GO

```

9. Finally, in your Emerald Database, drop the Calls table and create a view as follows:

```

CREATE VIEW Calls AS
Select * From EmerCalls..Calls
GO

GRANT SELECT , INSERT , DELETE , UPDATE ON dbo.Calls TO Emerald
GO

```

Please note that some call records will probably be lost unless you do this during a "slow" period. Also, there may be users who show as being on-line for a while and you may have to manually clear them.



## Glossary

Term	Definition
<b>A</b>	
<b>AAA</b>	Authentication, Authorization and Accounting. A methodology for securing remote access to networks. AAA requires user identification and can restrict access to specific network resources. It also maintains usage records for billing and network audits.
<b>Accounting</b>	A method of tracking a remote user's calls. The accounting data can include such information as a user's login and how much time was spent
<b>Application Program (or Programming) Interface (API)</b>	An API is an interface between an operating system and an application program that includes the calling convention used for their communication and the services that the operating system makes available to the programs. It usually includes a set of routines, protocols and tools. Compared with an API, the Graphical User Interface (GUI) is a direct user interface to either the application or operating system.
<b>Attribute</b>	Defined parameters used to identify a user or to configure a user's call session.
<b>Authentication</b>	A method of identifying a caller before accepting a call.
<b>B</b>	
<b>Basic Rate Interface (BRI)</b>	An ISDN interface that consists of two 64Kbps B channels (for voice and/or data) and one 16Kbps D channel (for signaling).
<b>C</b>	
<b>Challenge-Handshake Authentication Protocol (CHAP)</b>	CHAP is a point-to-point protocol that is used for identifying and authenticating a dial-in user. It does not prevent unauthorized access, but simply identifies the remote end.
<b>Client</b>	A software program that is used to contact and obtain data from a Server software program on another computer.
<b>Clients File</b>	A text file that has entries that are used to identify each client of the RadiusNT/X server, including either the client hostname or IP address and its shared secret. If you are running in Both or ODBC mode, this file is not used. Instead, the information comes from the database.
<b>D</b>	
<b>Dialed Number Identification Service (DNIS)</b>	The DNIS shows the phone number the user dialed in order to access the telephony system.
<b>Digital Subscriber Line (DSL)</b>	A method for moving data over regular copper phone lines. A common configuration of DSL allows downloads at speeds of up to 1.544 megabits per second, and uploads at speeds of 128 kilobits per second. This arrangement is called ADSL: Asymmetric Digital Subscriber Line.
<b>Domain Name Services (DNS)</b>	A method of administering domain names to correlate to IP addresses, and vice versa, in a consistent and concise manner.

<b>F</b>	
<b>Firewall</b>	A combination of hardware and software that separates a network into two or more parts for security purposes. It is often used to restrict access between the Internet and an internal network.
<b>Frequently Asked Questions (FAQs)</b>	FAQs are documents that list and answer the most common questions on a particular subject.
<b>File Transfer Protocol (FTP)</b>	A very common method of moving files between two systems.
<b>H</b>	
<b>Host</b>	Any computer on a network that is a repository for services available to other computers on the network.
<b>I</b>	
<b>Internet Engineering Task Force (IETF)</b>	An group of international network designers, operators, vendors and researchers who work together to develop new Internet standards and specifications.
<b>Intranet</b>	A private network ,inside a company or organization, that uses Internet services and protocols for internal use.
<b>IP Address</b>	A unique number consisting of 4 parts separated by dots (e.g., 165.113.245.2). Every machine that is on the Internet has a unique IP number.
<b>IP</b>	Internet Protocol - An addressing standard used on TCP/IP networks.
<b>Integrated Services Digital Network (ISDN)</b>	A way to move more data over existing regular phone lines at speeds of roughly 128,000 bits-per-second.
<b>L</b>	
<b>Login</b>	Noun: The account name used to gain access to a computer system. Verb: (Log In) The act of entering into a computer system.
<b>M</b>	
<b>Maximum Transmission Unit (MTU)</b>	The largest frame or packet that can be sent through a port on a NAS without fragmentation.
<b>N</b>	
<b>Name Server</b>	A server that resolves host names into network addresses.
<b>Network Access Server(s) (NAS)</b>	A server dedicated to authenticating users that log on.
<b>Network</b>	Two or more computers connected so that they can share resources. If you connect 2 or more networks, you have an internet.
<b>O</b>	
<b>Open DataBase Connectivity (ODBC)</b>	An interface used by Windows application programs to gain access to databases.
<b>P</b>	
<b>Port</b>	A number assigned to an application running in a server. The number is used to link the incoming data to the correct service.
<b>Practical Extraction and Report Language (Perl)</b>	An interpreted language developed by Larry Wall that is freely distributed on the Internet. It includes object-oriented programming facilities.
<b>Protocols</b>	Formal sets of communication rules and standards.
<b>R</b>	

<b>Relational DataBase Management System (RDBMS)</b>	A database organization method that links files as required. The software controls the organization, storage, retrieval, security and integrity of data in a database.
<b>Request For Comments (RFC)</b>	The name of the result and the process for creating a standard on the Internet.
<b>Roaming</b>	A service that enables two or more ISPs to allow one another's users to dial in to any ISP's network. This is useful for travelers who are outside of their normal service area.
<b>Router</b>	A special-purpose computer or software application that handles the connection between 2 or more networks. Routers 'look' at the destination addresses of the packets passing through them and decide which route to send them on.
<b>S</b>	
<b>Secret</b>	A code used to gain access to a locked system. Also known as a password.
<b>Server</b>	A computer or a software package that provides a specific kind of service to client software running on other computers.
<b>Shared Secret</b>	A character string that is specified on a server and on another device or server to establish shared identification. The shared secret is used to encrypt a user's password for security across the network. The server in turn uses the shared secret to decrypt the password upon receipt.
<b>SNMP</b>	Simple Network Management Protocol - The protocol governing network management and the monitoring of network devices and their functions. It is not necessarily limited to TCP/IP networks. The details of SNMP can be found on the Internet Engineering Task Force (IETF) Web site at <a href="http://www.ietf.org/">http://www.ietf.org/</a> .
<b>Structured Query Language (SQL)</b>	A specialized programming language for sending queries to databases.
<b>T</b>	
<b>Transmission Control Protocol (TCP)</b>	The standard that is responsible for reliable end-to-end communications for transmitting datagrams across Internet networks.
<b>Trigger</b>	An SQL procedure that is executed when a record is added or deleted. It is used to maintain referential integrity in the database. A trigger may also execute a stored procedure.
<b>U</b>	
<b>User</b>	A person who dials into a NAS for negotiation.
<b>Users File</b>	A text file that contains authentication and authorization information in the form of attributes and values for each user who connects to the network.