



RadiusNT & RadiusX

Dial-Up, VPN, Wireless & VOIP

For Windows, Linux, FreeBSD and Solaris

Version 5.0

IEA Software, Inc.

Administrative and Support Office

PO BOX 1170

Veradale, Washington 99037

Phone: (509) 444-BILL

Sales@iea-software.com

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 FreeBSD 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. PO BOX 1170 Veradale WA, 99037.

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. PO BOX 1170 Veradale, WA 99037 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. *Intel* is a registered trademark of Intel Corporation. *Transact-SQL* is a registered trademark and *DB-Library* is a trademark of Sybase, Inc. *Sun Solaris* are trademarks of Sun Microsystems. *Cisco* is a trademark of Cisco Systems. All other trademarks are the property of their respective owners.

© 1995-2005 IEA Software, Inc.
All Rights Reserved, World Wide

Table Of Contents

SOFTWARE LICENSE AGREEMENT.....	1
TRADEMARKS	2
WELCOME.....	6
PREFACE.....	6
ABOUT RADIUS	6
RADIUSNT AND RADIUSX EDITIONS.....	7
Enterprise	8
Professional and Enterprise	8
CONVENTIONS	9
SYSTEM REQUIREMENTS.....	10
RADIUSNT	10
RADIUSX	10
TECHNICAL SUPPORT.....	11
CHAPTER 1 – INSTALLATION	12
INSTALLING RADIUSNT	12
WHATS NEW IN RADIUSNT/X v5.....	14
UPGRADING FROM AN EARLIER VERSION OF RADIUSNT	15
INSTALLING RADIUSX	15
Package Installation	16
RADIUSNT ADMINISTRATOR	17
RADIUSX ADMINISTRATOR.....	18
CONFIGURATION OPTIONS FOR RADIUSNT/X WEB GUI	19
General Menu Options	19
ODBC Settings	20
Authentication Menu Options	22
Accounting.....	24
Advanced	26
Proxy Options.....	30
Cache Menu Options.....	31
Licensing	34
LDAP Menu	34
External Authentication Menu.....	37
Token-based server Config.....	38
TACACS Menu	39
Custom settings.....	40
EAP	40
USERS AND CLIENTS FILES	41
CHAPTER 2 – MODES	42
USER AND CONFIGURATION MODES.....	42
TEXT MODE	42

ODBC MODE	43
BOTH MODE.....	43
CHAPTER 3 - TERMINAL SERVER CONFIGURATION	45
LIVINGSTON PORTMASTERS.....	45
ASCEND MAX AND PIPELINE	45
OTHER RADIUS COMPATIBLE NAS	46
CHAPTER 4 - TESTING RADIUSNT/X.....	47
RADLOGIN	47
TROUBLESHOOTING	47
CHAPTER 5 – RADIUSNT AS A SERVICE.....	48
INSTALLING RADIUSNT AS A SERVICE	48
REMOVING THE SERVICE	48
SERVICE CONSIDERATIONS	48
CHAPTER 6 – EXTERNAL AUTHENTICATION	50
UNIX PASSWD FILE	50
WINDOWS NT SAM SUPPORT	50
<i>Additional Authentication Methods</i>	51
CHAPTER 7 – COMMAND LINE AND REGISTRY SETTINGS.....	52
COMMAND LINE AND REGISTRY/INI LISTINGS	52
CHAPTER 8 - ODBC DATABASE SCHEMA	60
<i>Authentication Process</i>	73
<i>Accounting Process</i>	75
<i>Additional ODBC procedures</i>	75
SUPPORTED DATABASE FEATURES PER PLATFORM	75
<i>Custom Queries</i>	76
CHAPTER 9 – ADVANCED FEATURES	82
CONCURRENCY CONTROL	82
TIME BANKING	83
SERVER ACCESS	83
DNIS ACCESS	83
REJECT LIST.....	84
LOGGING	84
SPECIAL USERS	86
IP POOLING	87
RADIUS FILTERING.....	87
<i>Filter Groups (RadFilterGroups table)</i>	88
<i>Filters (RadFilters table)</i>	90
CHAPTER 10 – ENTERPRISE & PROFESSIONAL VERSION ONLY FEATURES.....	91
PROXY AND ROAMING	91
<i>User Based Proxy</i>	91
<i>Incoming Proxy</i>	92
<i>Server-Based Proxy</i>	93
<i>Modifying Return Attributes</i>	93
<i>Attribute Proxy</i>	93
<i>Proxy Failover</i>	93
SIMPLE NETWORK MANAGEMENT PROTOCOL (SNMP)	93

<i>Querying SNMP values</i>	94
<i>SNMP Authentication</i>	95
<i>SNMP Accounting</i>	95
<i>AgentX Support</i>	96
SNMP CONCURRENCY CHECKING	96
SERVER TYPES	97
SMART CACHE	98
SYSLOG SUPPORT	98
LDAP AUTHENTICATION	99
CHAPTER 11 – ENTERPRISE VERSION FEATURES	101
ACE SERVER	101
DEFENDER	101
SAFEWORD	101
TACACS+	101
EXTERNAL AUTHENTICATION API	101
EXTERNAL ATTRIBUTE-VALUE MAPPING	104
<i>Auth API</i>	104
STORE & FORWARD PROXY	104
CHAPTER 12 – TROUBLESHOOTING	106
STARTUP PROBLEMS	106
OPERATION PROBLEMS	106
CHAPTER 13 – FREQUENTLY ASKED QUESTIONS (FAQS)	108
GENERAL	108
TEXT MODE	110
ODBC MODE	110
VENDOR SUPPORT	111
<i>Ascend</i>	111
<i>Cisco</i>	111
<i>Computone</i>	112
<i>iPass</i>	112
<i>ipSwitch</i>	112
<i>Livingston</i>	112
APPENDIX A - RADIUS ATTRIBUTES	114
<i>RADIUS Attributes</i>	114
RFC 2138 - RADIUS AUTHENTICATION	144
RFC 2139 - RADIUS ACCOUNTING	146
CONFIGURING ODBC	147
<i>Both Mode</i>	148
TABLES	148
EMERALD INTEGRATION FAQs	149
GLOSSARY	150

Welcome

IEA Software would like to thank you for selecting our RadiusNT or RadiusX product. These remote access authentication solutions support 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.

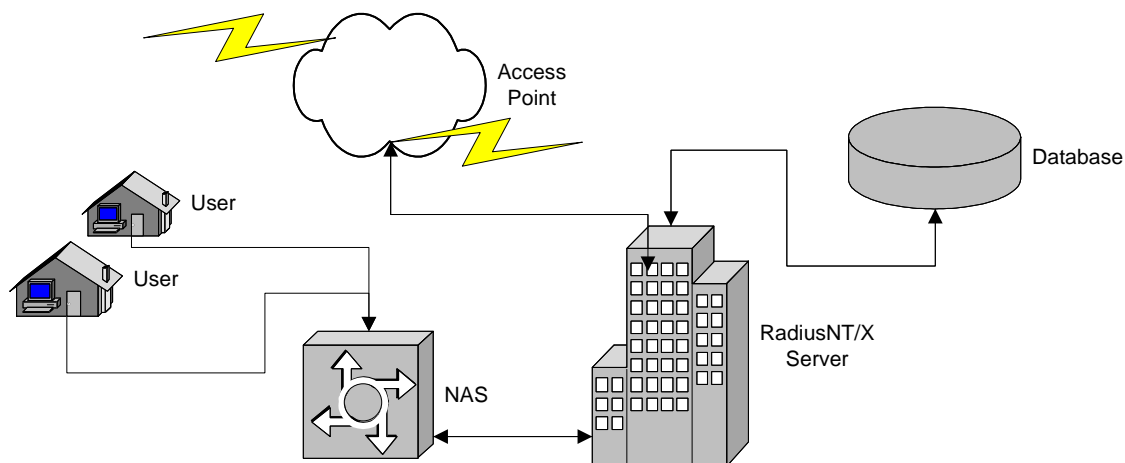
This document is not intended to delve into the technical aspects of RADIUS. You will find that technical reference materials exist in a variety of places. For RFC information, please check out the World Wide Web. A good starting point is the Internet Engineering Task Force (IETF) Web site at <http://www.ietf.org>. 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, FreeBSD** and **Solaris** 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 connect to a wide range of public and private networks to access information and to easily communicate with one another. Managing these widespread and disparate systems with more than a few 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, DSL 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 *allowed list of Radius clients* for an entry that matches the request. If a match is found, RadiusNT/X searches the available databases for a profile that matches the criteria (commonly a username and password). The RADIUS 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 stand-alone editions of RadiusNT and RadiusX: Professional and Enterprise. In addition, RadiusNT/X works with version 2.5 and 4.0+ editions of the [Emerald Management Suite](#). RadiusNT/X Professional includes advanced features that the Emerald-only version does not include, such as cache and proxy (see below). Radius Enterprise includes all professional features and, additionally, support for Token cards, LDAP, Tacacs+ and more.

Some advanced options 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 and UNIX versions 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

Differences are noted throughout the documentation. In addition, features and options available in only the Enterprise and Enterprise & Professional version are clearly noted. The following charts show the options that are only available in Professional and Enterprise editions. For more detailed information on each option, please see the [Features](#) chapter.

Enterprise

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

Professional and Enterprise

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

Conventions

This User Guide has standardized 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
Bold	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
RadiusNT/X	Applies to the Windows NT & UNIX versions of Radius
RadiusNT	Applies to the Windows NT version of Radius
RadiusX	Applies to the UNIX version of Radius
Italic	Directory or filename. Also used to emphasize a word, term or concept
"quoted text"	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

The requirements listed here are minimal requirements needed to install and use the software with a small user base. Performance is almost always limited by any backend authentication and accounting systems used and largely dependant on your environment (network,database, software) as well as the configuration of RadiusNT/X itself. We recommend you do sufficient load testing of the software before putting it into a production environment.

RadiusNT

- Windows NT 4.0 sp5+, Windows 2000, XP, 2003 or later.
- 64MB of RAM or greater
- (x86 processor - pentium 100 or greater)
- Web browser (Netscape 4.x+ or IE 4.x+)

RadiusX

- Solaris 2.6 or later, RedHat Linux 6.0 or later, FreeBSD 5.0 or later
- 64MB of Ram or greater
- >30MB Disk space
- Perl 5.0 or higher
- Web browser (Netscape 4.x+ or IE 4.x+)

Technical Support

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

- Please read the *readme.txt* and *changes.txt* files that are included with your distribution archive. This file contains up-to-date information on the software, noting any changes, feature enhancements or known problems.
- This manual has much of the information you need to solve problems. Please re-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. The latest version of this document and change history for the RadiusNT and RadiusX products can be found at <http://www.iea-software.com/docs>
- 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. Please read the **readme.txt** and **changes.txt** files included with your distribution for late-breaking information before proceeding with your installation.

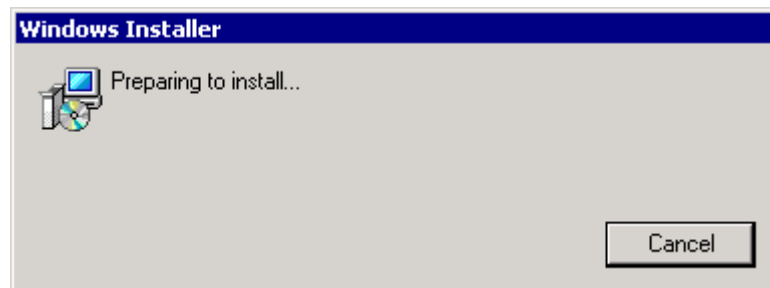
In addition, please read the licensing agreement when it is displayed during the installation process or near the beginning of this document. Make sure that you agree with the terms of the agreement before proceeding.

Installing RadiusNT

Please follow the steps below to install RadiusNT on your system:

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 the system requirements listed earlier in this section.
3. Log on to your system as "Administrator".
4. Click **Start**, then **Run**.
5. **Browse** to locate the *RadiusNT4.exe* file and then click **OK** to begin the installation process.

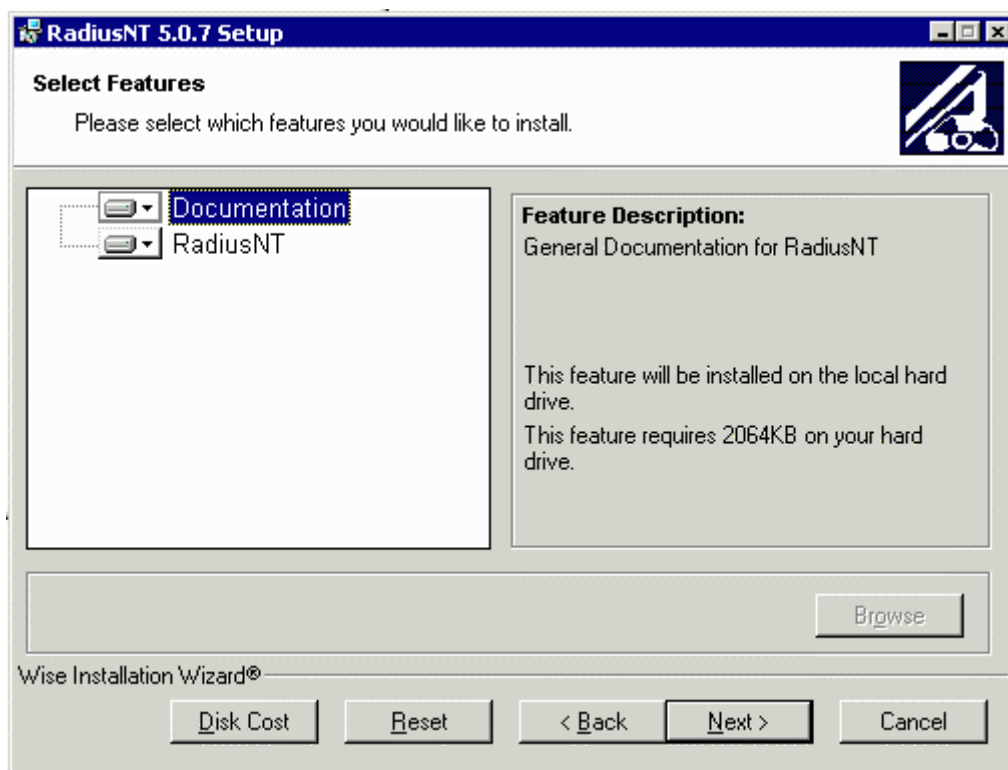
Please note that if some of your system files are out of date, RadiusNT will update the files and require you to restart Windows NT in order to proceed.



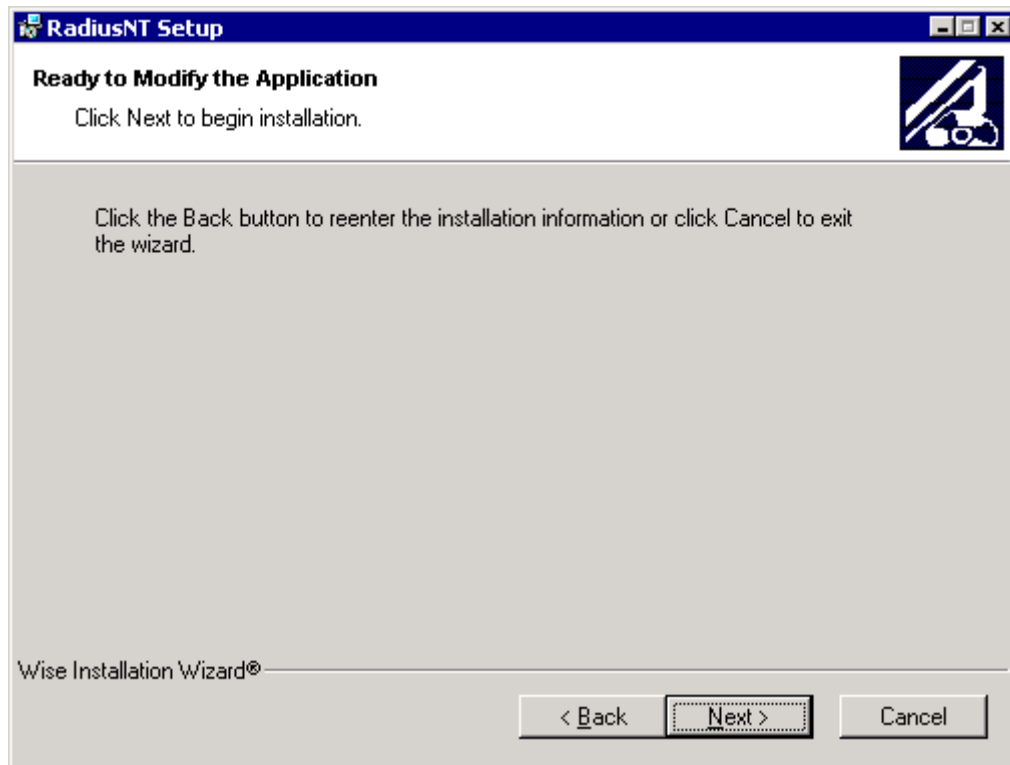
7. You will see the Welcome screen. Click **OK** to proceed.
8. Next, you will see the User License Agreement. Before you proceed, make sure that you have read and agree with the terms of the license agreement. Click **I Accept the License Agreement** to continue.
9. The Setup application will assist 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 having another Radius server installed in c:\radius,

the c: drive being out of space, etc. After changing the destination directory (if need be), click the **Installation** button to continue.

Select the features you want to install.



10. When the installation has completed, you will receive a final confirmation screen. Click **Next** to finish.



Once the Setup program has finished, you can configure RadiusNT for your operating environment via the [RadiusNT Administrator](#). Please note that for the product to function, you will need to enter your license information. Please be sure to read the **changes.txt** and **readme.txt** files for up-to-date information about the software.

Whats new in RadiusNT/X v5

- ❖ EAP and 802.11x support for wireless, user + certificate based mutual authentication and dynamic encryption keys.
 - EAP-MD5
 - EAP-LEAP (Cisco wireless)
 - EAP-PEAP v0 and v1 (Microsoft and IETF (Cisco) implementations)
 - EAP-GTC
 - PEAP-MSCHAPv2
 - PEAP-GTC
- ❖ Performance and Managability improvements for Wireless, VPN and VOIP applications.
 - Support for concurrent ODBC, LDAP and WINNT authentication requests
 - Accounting spooler transaction performance improvements
 - Packet replay improves performance over congested networks and improves consistency of accounting data by better detecting duplicate requests
 - With few exceptions server configuration changes take effect immediately without requiring a server restart.
 - All local configuration options can be overridden by settings stored in a central database.

- ❖ Expanded attribute / VSA support, we've nearly doubled the number of vendors available in our default dictionary in addition to supporting new features of existing vendors. New datatypes are now supported such as IPv6 and Redback 64-bit integers.
- ❖ Attribute filtering supports modifying attributes or making decisions based on attributes coming in, going out or proxied through RadiusNT/X. They can also direct specific types of accounting data to an alternate 'Calls' table.
- ❖ Alternate failure profiles allow bad requests to be acknowledged with a custom set of attributes. This allows the configuring of limited network access for customers whose accounts may have lapsed or need to pay for additional network access.
- ❖ Updated database schema supports new features and simplifies integration. RadiusNT v5 is backwards compatible with all Version 3 and 4 databases and local configurations. Database updates for previous versions are only required to take advantage of new features.
- ❖ Intelligent database interface
 - Dynamic parameter checking allows authentication stored procedure full access to RADIUS attributes.
 - All internal queries are documented and configurable through the administrative web interface. They allow complete control over the ODBC database interface and make integration with third-party databases easy.
- ❖ Compatibility
 - RadiusNT/X now supports two of the most popular open source databases MySQL and PostgreSQL.
 - Native FreeBSD distribution
 - CISCO VOIP accounting
- ❖ New Radlogin test client included
 - GUI and command line interfaces
 - Attribute 'Profiles' allow simulating requests of most NASes.
 - Validating packet decoder converts raw RADIUS packets into an easy to read format.
 - Server monitoring: uptime/response time statistics and email pager status notification.

Upgrading From an Earlier Version of RadiusNT

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

For 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* and *changes.txt* files before proceeding.

Upgrading your database will depend on your installation configuration.

For SQL Server & Sybase running the up_radfilters_mssql.sql script adds support for attribute filtering to your existing database. Please note existing RadiusNT/X 3.0 and 4.0 databases are compatible with RadiusNT/X v5 making this an optional step.

Installing RadiusX

Please follow the instructions below to install RadiusX for Solaris, FreeBSD and Linux:

1. Download the distribution archive for your platform (Linux, FreeBSD or Solaris) from the Download Center at <http://www.iea-software.com/download>.
2. Review the system requirements listed earlier in this section.
3. Log on to your system as “root” or a user that has sufficient permissions to install the software.
4. 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>. Instructions for manually installing RadiusX are included in the *readme.txt* file within the distribution archive, but are **not recommended**.

5. Next, un-tar the distribution (***radiusx5_solaris.tar.gz***, ***radiusx5_freebsd.tar.gz*** or ***radiusx5_linux.tar.gz***) into a temporary directory. This can be done by typing the following commands:

```
"gzip -d radiusx5_XXXXX.tar.gz"
"tar -xf radiusx5_XXXXX.tar"
```

6. Use the “**cd**” command to change to the directory where the files were expanded.

Next, to run in database mode you will need to create a database. Once the database exists, you will need to step through two more processes. The first step is to run a script against the database and the second is to install the RadiusX server.

Begin by running the correct script against your database:

- For a MS SQL database, use *./radius/radius5_mssql.sql*
- For a Sybase database, use *./radius/radius5_sybase.sql*
- For a Oracle database, use *./radius/radius5_oracle.sql*
- For a Mysql database use *./radius/radius5_mysql.sql*
- For a PostgreSQL database, use *./radius/radius5_postgres.sql*

Please refer to your database documentation to learn how to run the script. 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.

Note: If you will be using **MySQL or PostgreSQL** you must later select the appropriate option from the ‘custom settings’ menu in the RadiusNT/X administrator. In Addition the client access software for these databases must first be installed and properly configured.

After the database is created, and the .sql script has been run, proceed to the installation application.

Package Installation

1. Run the Install application by typing “**perl install.pl**”. The RadiusX Installer is displayed.

```

Welcome to IEA Software, Inc.  UNIX Installer v4

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.

4.  [Install]           RadiusX (5.0)
7.  [Install]           Radlogin test client (v4.0)

: |

```

You will be presented with two options. All components are installed by default. Once you have selected an option, you will note that the indicator changes from “**Install**”, to “**Do not Install**”. Please note that, if you make a mistake, you can simply type the corresponding option number again and this will **toggle** the “**Install**” or “**Do not Install**” option.

2. Type “**C**” to continue, or “**Q**” to abort the install process.

Once the Install program has finished, you can move on to configuring RadiusX for your operating environment via the RadiusX text-based or Web-based Administrator. For the product to function, you will need to enter your license information. Please be sure to examine the ***readme.txt*** and ***changes.txt*** files for up-to-date information about the software.

Quick Tip!

If you experience any trouble with the installation process, please refer to the *install.log* file. This file will display any errors that were encountered during the install, including items such as file permission or disk space errors.

RadiusNT Administrator

When you completed the RadiusNT setup, an icon for the Administrator was created in the RadiusNT group. To run the Administrator, do the following:

1. Click **Start**, then **Programs**.
2. Browse for the **RadiusNT** program, then select it.
3. Finally, select the **RadiusNT Admin** option. The RadiusNT Administrator window opens.

The RadiusNT/X Administrator has 15 different areas: General, ODBC settings, Authentication, Accounting, EAP, Advanced, Proxy, Smart caching, Licensing, LDAP, External auth, Tacacs+, Defender, Safeword and Custom settings. To move between each area, click on the corresponding link in the navbar along the top of the Administrator interface. Please remember to fill out your **license information** on the Licensing tab or the Licenses table in the database in order for RadiusNT to function.

RadiusNT Administrator version 5.0.3

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

Welcome

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

Note: The default password for this configuration server can be changed via the 'Change Password' option above.

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.

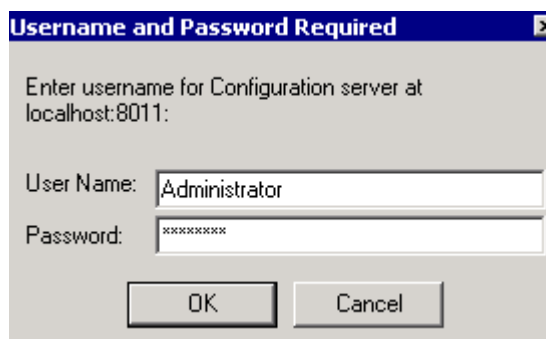
An **alternative** method of configuring RadiusNT is via the command line options, although this is **not** recommended unless you are trying to debug a problem. Please note that the RadiusNT Administrator settings are stored in the **registry**, while the given command line options are only valid for **that specific execution** of RadiusNT.

You will find brief explanations of each option in the [Configuration](#) section of the [RadiusNT/X Administrators Guide](#). Please note that some options are explained in finer detail in later sections.

RadiusX Administrator

The Web-based Administrator provides an easy-to-use Graphical User Interface (GUI) via your Web browser for configuring RadiusX for your RADIUS authentication, authorization and accounting needs.

To start the configuration server, type “/usr/local/radius/radadmn” in the command line. By default, the configuration web server will listen on port 8011 (<http://localhost:8011>).



The RadiusX Web-based Administrator has several different areas:

The RadiusX Administrator has 15 different areas: General, ODBC settings, Authentication, Accounting, EAP, Advanced, Proxy, Smart caching, Licensing, LDAP, External auth, Tacacs+, Defender, Safeword and Custom settings. To move between each area, click on the corresponding link in the navbar along the

top of the Administrator interface. Please remember to fill out your **license information** on the Licensing tab or the Licenses table in the database in order for RadiusNT to function.

RadiusNT Administrator version 5.0.3

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

Configuration Options for RadiusNT/X Web GUI

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 Menu Options

General	
Database mode	Database Only
Debug options	<input checked="" type="checkbox"/> Informational <input checked="" type="checkbox"/> Authentication <input checked="" type="checkbox"/> Database queries <input checked="" 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	d:\emerald4\acct
Data directory	d:\emerald
Users file	Users
Configuration server port	8011

Option	Description

Database Mode	
Text	<p>RadiusNT/X will read the users, clients and dictionary files to retrieve all standard information.</p> <p>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 and in the detail files. All other configurations (dictionary, clients, etc.) will be read from the ODBC database.</p>
Database	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 not use the text files. Accounting information will be stored in the ODBC database rather than the text files.
Debug Options	
Informational	Show detailed information.
Database queries	ODBC information, including SQL statements.
Authentication	User information during authentication (passwords, etc).
File messages	File Information, including accounting and logging.
SNMP	SNMP Concurrency and query information.
Smart cache	Information on cache related events.
Memory stats	Show object sizes.
Configuration	Show RADIUS configuration at startup.
Allow Malformed	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.
Accounting Directory	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.
Data Directory	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

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:

ODBC settings	
Edit existing datasource	(none)
Create new datasource	Radius
<input data-bbox="1209 567 1412 609" type="button" value=" >> Continue "/>	

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.

ODBC settings	
Database type	<div> <div>Oracle 8</div> <div> Microsoft SQL 7+ Sybase 11.9+ Oracle 8 MySQL 4.1+ PostgreSQL 7.2+ </div> </div>
<input data-bbox="1250 871 1421 913" type="button" value=" >> Continue "/>	

© 1994-2003 IEA Software, Inc. All rights reserved. world wide.

On UNIX platforms the server address for Microsoft and Sybase is the IP Address or hostname of the SQL server. Note: TCP socket support must be enabled in the SQL server's protocol setup for RadiusX to communicate with your database.

When using Oracle /w RadiusX or 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 the net8 configuration utility.

When using MySQL with RadiusX make sure you have first installed the MySQL client and MySQL ODBC drivers. RadiusX expects the MySQL odbc driver to be '/usr/local/lib/libmyodbc.so' This can be changed after creating a MySQL DSN by modifying the odbc.ini file located in the /usr/local/iea folder. MySQL and PostgreSQL users must also select 'MySQL' or 'PostgreSQL' from the list in the [custom settings](#) menu of the RadiusNT/X admin.

ODBC settings	
Datasource description	My Radius5 datasource
Server name	rad5sql
Server port	1433
Database name	Emerald4

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

Authentication Menu Options

Authentication	
Authentication datasource	<div>Radius5</div> <div>Up</div> <div>Down</div> <div>Delete</div> <div>LocalServer</div> <div>Add</div>
Username	sa
Password	*****
Authentication port	1645
Concurrent requests (<i>threads</i>)	10
Database query timeout (<i>secs</i>)	4
Trim domain	<input checked="" type="checkbox"/> Authentication <input checked="" type="checkbox"/> Accounting
Pre delimiter	%V
Post delimiter	@
Bad characters	%
Ignore case	<input checked="" type="checkbox"/>
Users file	Users
Log file	d:\emerald4\auth.log

Option	Description
Auth datasource	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.
Username	Use this to specify the username RadiusNT/X uses to log into the ODBC database.
Password	This option specifies the password for the database user.
Auth Port	This option allows you to specify the port RadiusNT/X will "listen" on for authentication requests.
Log file	The entry shows what log file is used for RADIUS authentication requests (and accounting requests if an accounting logfile is not specified).
Ignore case	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.
Trim domain	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.
Pre delimiter	A list of delimiters denoting everything before the delimiter is the domain. The default for this is the list "%V".
Post delimiter	A list of delimiters denoting everything after the delimiter is the domain. The default for this is the list "@".
Bad characters	A list of characters that, if found in the authentication name, will cause an immediate reject of the authentication request without further processing.
Users file	The filename containing the user information. This should be just the filename, and the file must exist in the specified data directory.
Concurrent requests	Number of concurrent authentication requests that can be processed at any one time.
Database query timeout	If operating in database mode this is the maximum number of seconds the execution of authentication queries can take before timing out. Setting this option to zero means there is no time limit for query execution.

Accounting

Accounting	
Accounting datasource	<div><div></div><div>Up</div><div>Down</div><div>Delete</div><div>LocalServer</div><div>Add</div></div>
Username	<input type="text"/>
Password	<input type="password"/>
Accounting port	<input type="text"/>
Log file	<input type="text" value="d:\emerald4\acct.log"/>
Require secret	<input checked="" type="checkbox"/>
VSA Mapping	<input checked="" type="checkbox"/>
Max spooled items	<input type="text" value="5000"/>

Option	Description
Accounting datasource	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.
Username	Use this to specify the username RadiusNT/X uses to log into the ODBC database.
Password	This option specifies the password for the database user.
Accounting port	The Port option allows you to specify the port RadiusNT/X will "listen" on for accounting requests.
Log file	The entry shows what log file is used for RADIUS authentication requests (and accounting requests if an accounting logfile is not specified).
Require secret	This option requires accounting packets to be "signed". This option is rarely needed, and should normally be left unchecked.
VSA Mapping	When this option is enabled, certain vendor specific attributes are mapped to a matching standard attribute and entered into the Calls table.
Max spooled items	<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>
Max batch hold time	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)
Max items per batch	The maximum number of items that can be sent in a single accounting batch. (See Max Batch time) (Enterprise & Professional version only)

Advanced

Advanced	
Authentication and accounting options	<input type="checkbox"/> (Auth) Concurrency control <input type="checkbox"/> (Auth) Time banking <input type="checkbox"/> (Auth) Limit session time to account expiration <input 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) Enable DNIS Access <input type="checkbox"/> (Auth) Reverse DNIS checking <input type="checkbox"/> (Auth) Command triggers <input type="checkbox"/> (Auth) Reject attributes <input type="checkbox"/> (Auth) Always use digital signatures <input 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 <input type="checkbox"/> Enable attribute filtering
SNMP options	<input type="checkbox"/> Statistics <input type="checkbox"/> Concurrency check <input type="checkbox"/> Server-Ports update
Bind IP-Address	Listen on all interfaces
Database test (<i>secs</i>)	
Database time offset (<i>days</i>)	5
Cache persistence & Accounting log	<input type="checkbox"/> Accounting <input type="checkbox"/> Authentication
Duplicate request replay	<input checked="" type="checkbox"/> Authentication <input checked="" type="checkbox"/> Accounting
Duplicate history size (<i>requests</i>)	30
Virtual class attribute	<input type="checkbox"/> Enable class attribute correlation for local requests <input type="checkbox"/> Enable class attribute correlation for proxied requests <input type="checkbox"/> Require strict session identifier based correlation (not recommended)
Virtual class TTL (<i>days</i>)	5
Syslog IP	

Option	Description
--------	-------------

Authentication	
Concurrency Control	RadiusNT/X can prevent users from initiating more than one session at a time if this option is enabled.
Sever Port Access	Enabling this option allows RadiusNT/X to restrict who can connect to a port based on access information. See Advanced Options in Chapter 9 for more details.
Password Replace	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.
Enable DNIS Access	This enables the Dialed Number Identification Service (DNIS) checking option. Please see the ODBC Advanced section in Chapter 9 for more details on DNIS checking and restrictions.
Reverse DNIS Check	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.
Reject attributes	This option enables Reject List checking. Please see the ODBC Advanced section in Chapter 9 for more details on the Reject List option.
Time banking	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 must manually add more minutes or the user will not be able to log on.
Ascend max time	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.
IP Pooling	IP Pooling enables RADIUS-based address allocation. Please see the Chapter 9 for more details on IP Pooling.
Command Trigger	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.
Always use digital signatures	When enabled the signature attribute is sent to verify the integrity of RADIUS packets and any RADIUS packet containing the signature attribute is verified. If disabled the signature attribute is only sent in response to an EAP authentication request.
Accounting	
Manual Calls Update	RadiusNT/X will manually update the ServerPorts table. This is only needed for databases that do not have trigger support. The option is not needed with Emerald/SQL Server or an active database that can update the calls on-line view automatically.

Stop Records Only	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.
SNMP	All SNMP features are Professional/Enterprise version only.
Statistics	This option enables SNMP statistics. See Chapter 9 for more information about SNMP.
Server-Ports update	This option periodically updates ServerPorts if it detects different port changes via SNMP. When enabled, SNMP Concurrency Checking is automatically disabled.
Concurrency Check	This option enables SNMP Concurrency verification. See Chapter 9 for more information about SNMP.
Bind IP-Address	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.
Database test	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 (Enterprise & Professional version only).
Database time offset	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.
Cache persistence	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)
Duplicate request replay	When a duplicate access or accounting request RadiusNT/X has already issued a response for is received RadiusNT/X can respond with the previously sent response instead of processing the request anew. It is recommended this option be enabled especially if Proxy or EAP authentication is used.
Duplicate history size	The number of stored responses to keep in main memory. This number should be twice the number of combined maximum authentication and accounting requests expected in a given 20-second interval or at least 250 requests. Each request reserves about 4kb of main memory.
Virtual class attribute	If a RADIUS client does not support returning the 'Class' attribute with Accounting requests RadiusNT/X has the ability to match accounting requests with an initial access-accept message effectively working around problems caused by a clients lack of support for the Class attribute. Note this feature must not be relied upon as it cannot correlate authentication or accounting requests sent to a different RADIUS server nor can it correlate existing active sessions during a restart of RadiusNT/X. The virtual class attribute requires storing information about each authentication request for an extended period of time and may substantially increase RadiusNT/X memory requirements.

	Virtual class support can be enabled for local requests and or proxied requests. 'Require strict session identifier based correlation' restricts matching of Authentication Access-Accept messages with subsequent Accounting-Request messages to clients that send Acct-Session-ID in Access-Request as well as Accounting-Request queries. If the require session identifier option is disabled RadiusNT/X will attempt to use other information such as called/calling station id, username and port to correlate unique authentication and accounting sessions should Acct-Session-ID be unavailable.
Virtual class TTL	This option reflects the maximum amount of time in days Class information can be stored by RadiusNT/X for each authentication. This should be set to at least the maximum amount of time any session can remain active. Note that arbitrarily large settings may significantly impact the memory requirements of RadiusNT/X. Setting Virtual class TTL to more than 30 days is not recommended.
Syslog IP	Both error and informational messages can be directed to a syslog server by specifying an IP address.
Disable '0' Session-ID port clear	Prevent RadiusNT/X from clearing all users from the On-line view for a NAS that sends a 0 Session-ID.
Disable Acct On/Off port clear	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.
Enable attribute filtering	When selected attribute filtering is enabled

Proxy Options

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 checked="" type="checkbox"/> Accounting - local copy <input type="checkbox"/> Server proxy <input type="checkbox"/> Ignore client retry policy
Store & forward accounting mode	<input checked="" type="checkbox"/>
Persistent store & forward log	<input type="checkbox"/>
Force flush store and forward log before accounting ack	<input type="checkbox"/>
Proxy timeout	20
Proxy identifier	

Option	Description
Proxy Options	<p>User – Auth: Enable RADIUS authentication proxy</p> <p>User–Auth-Unknown: Proxy only locally unknown authentication requests</p> <p>Accounting: Proxy RADIUS accounting requests</p> <p>Accounting-Echo: Echo accounting request attributes in accounting ack response. Do not enable this feature unless you have a specific need for it.</p> <p>Accounting-local copy: Stores a local copy of proxied accounting records in Calls table or accounting log file. Useful for account settlement with third party providers.</p> <p>Server proxy: Allows requests from specific RADIUS clients to be proxied to a specific RADIUS server.</p> <p>Ignore client retry policy: Prevents RADIUS client retransmissions from also being forwarded to the remote proxy server. Enabling this will limit retransmission attempts sent to the remote RADIUS server to the number and timeout period specified locally for that outgoing RADIUS server. This feature requires duplicate request replay be enabled from the Advanced options menu.</p>
Store and forward	Enables store and forward proxy mode. (Enterprise version only)
Persistent log	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. (Enterprise version only)

Flush log before ack	Enabling this option guarantees accounting data is physically written to persistent storage before replying to an accounting request. (Enterprise version only)
Proxy Timeout	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).
Proxy Identifier	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.

Cache Menu Options

Smart caching	
Disable smart cache	<input checked="" type="checkbox"/>
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="301"/>
Delete unused accounts (<i>days</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
Disable smart cache	When checked authentication requests are always looked up through the database to ensure cached information is correct.
Preload	Number of days since the last successful authentication an account should be preloaded into the cache.
Last modified acct check	This option determines how often the database is checked for modifications and the cache is updated with the new information (in seconds)..
Delete unused accounts	Number of days an account can remain in the cache without being requested before being removed.
Force cache update	The time (in days) that an idle entry can remain in the cache before a forced update of the entry occurs.
Check for deleted accounts	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.
Refresh account types	Service type cache update interval (in minutes).
Double-check override	Interval (in seconds) to override checking the database (for new information that may cause the authentication to succeed) to prevent extra database queries.
Server access refresh	Server-Access cache update interval (in minutes).
Refresh DNIS	DNIS cache update interval (in minutes).
Refresh roam servers	Roam Server cache update interval (in minutes).
Refresh attribute rejects	Reject cache update interval (in minutes).
Refresh proxy attributes	Proxy attributes update interval (in minutes)
Free update memory	This option controls the frequency in which internal memory 'garbage collection' is done and memory returned to the operating system for use by other applications. (Enterprise & Professional version only)
Cache double-check	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
Write cache db to disk	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)
Refresh servers	Server table / clients file update interval (in minutes). Setting this field to 0 or blank disables refreshing the RADIUS clients list. This option is disabled by default.

Licensing

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)
License Key	RadiusNT/X License Key

LDAP Menu

LDAP

Server address (<i>Multiple servers for failover</i>)	<div> <div>Up</div> <div>Down</div> <div>Delete</div> <div>Add</div> </div>
Server port	<input type="text"/>
Server timeout (<i>secs</i>)	<input type="text"/>
Netscape 4.x SSL Cert	<input type="text"/>
Search filter	<input type="text"/>
Search bind DN	<input type="text"/>
Search bind password	<input type="password"/>
Search scope	One level ▾
Base directory (<i>DN</i>)	<input type="text"/>
Password attribute	<input type="text"/>
Account type attribute	<input type="text"/>
Login limit attribute	<input type="text"/>

Option	Description
Servers	The list of LDAP Servers to authenticate against. Secondary servers are used only if the primary is not available.
SSL Cert	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.
Username	The username(DN) to connect to the LDAP server as.
Password	The password to connect to the LDAP server with.
Port	The port to connect to the LDAP Server on. Default is 389, unless using SSL, which is 636.
Timeout	The Directory Search timeout in seconds. When the limit is reached, the LDAP module returns "ignore", giving another authentication method a chance to succeed.
Login Limit attribute	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.
Account Type attribute	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.
Search	The search string used to search accounts or bind as a user. Please see the LDAP Authentication section in Chapter 10 for more details on this option.
Base DN	The Base directory under which to search for matching user entries.
Scope	<p>This option determines how deep to search the directory tree for the user (In this example, "neila"). []s represent the Base DN.</p> <p>One Level Deep: uid=neila,[ou=moon,o=nasa] Sub-Tree: uid=neila,ou=moon,[o=nasa]</p>
Password attribute	<p>Normally RadiusNT/X attempts to authenticate by binding using the DN in the results of the LDAP search and the password supplied from RadiusNT/X. This is the default behavior when this field is left blank.</p> <p>If a Password attribute is specified it's used to authenticate the client instead of performing an LDAP bind request.</p>

External Authentication Menu

External auth

Authentication methods (*Try order*)

safeword
authapi.dll\dom1
tacacs
ldap

Up
Down
Delete

Add

External auth library path

c:\vss\radiusnt\authapi\debug

RadiusNT Administrator External Authentication Menu

Option	Description
Authentication Methods	<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. Authentication methods are not available in RadiusNT/X Emerald-only.</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>
External auth path	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.

Token-based server Config

Defender	
Server address (<i>Multiple servers for failover</i>)	<div><div>test.com</div><div>Up</div><div>Down</div><div>Delete</div><div><input type="text"/></div><div>Add</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
SafeWord	
Hosts	A space-separated list of SafeWord Servers to authenticate against. Secondary servers are used only if the primary server is not available.
Port	The port to connect to the Safeword server on.
Defender	
Hosts	A space-separated list of SafeWord Servers to authenticate against. Secondary servers are used only if the primary is not available.
Agent ID	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.
Port	The port to connect to the Safeword server on.
Timeout	This value sets the amount of time to wait for a response before trying a secondary server.
Down	This value sets the total timeout period for the server before it is determined to be down.

TACACS Menu

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

Quick Tip!

Please note that RadiusX does **not** run as a Service. After configuration, you will need to run the RadiusX program in the background by typing “./radiusd&” in the /usr/local/radius directory.

Custom settings

RadiusNT/X can be configured to work with a variety of third party systems. Normally when RadiusNT/X is used with the included RADIUS v5 schema or Emerald custom settings are not necessary. However if you are using **MySQL**, **PostgreSQL** database systems or third party documentation instructs you to select a custom setting – simply select the appropriate profile from the list.

Selecting ‘custom configuration’ opens up more options allowing you to customize RadiusNT/X’s interaction with the database. You can make changes to an existing profile by selecting it first then selecting ‘custom configuration’. Note: If custom configuration is selected any custom changes made will be lost if another profile is selected. See the [custom queries](#) section for detailed information explaining each option and a description of available parameters and required result sets.

EAP

If you are using PEAP a PEAP certificate file containing your SSL public and private keys in base64 format must be specified. If applicable you need to specify your CA’s (Certificate Authority) certificate chain file provided by your CA. All other EAP options and associated protocols are negotiated automatically and require no further configuration.

EAP	
Preferred EAP method	LEAP (Cisco wireless) ▾
Preferred PEAP method	MSCHAP (Microsoft CHAP v2) ▾
PEAP Certificate	d:\radius\cert.pem
PEAP CA Certificate	d:\radius\ca.txt

Option	Description
Preferred EAP method	This should reflect the EAP method most of your clients will be using. This improves latency of requests slightly by making protocol negotiation easier for the client and server.
Preferred PEAP method	This should reflect the PEAP method most of your clients will be using. This improves latency of requests slightly by making protocol negotiation easier for the client and server.
PEAP Certificate	SSL certificate file containing a public and private key in PEM (Base64) format. If you are obtaining a certificate from a well-known certificate authority follow their instructions for creating this file for the apache web server.
PEAP CA Certificate	Your CA's certificate chain file in PEM (Base64) format.

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.

Chapter 2 – MODES

User and Configuration Modes

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. (Ex: 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 if the database happens to stop working.

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, it reads in the Users, Clients and Dictionary lists. If you change any of these files, you **must** stop and re-start RadiusNT/X for the changes to take effect. Please follow the following steps to run RadiusNT/X in Text mode:

1. Create the Accounting directory that you specified in the Administrator.
2. Copy the *clients.example* file to *clients*. Although you can simply rename the file, copying is preferred. This way, the example file can be referred to later.
3. Next, edit the *clients* 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 a secret. 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. (For RadiusNT, the default directory is c:\radius, for RadiusX, use the /usr/local/radius directory.)
6. Edit the file named *users*, then uncomment the following four lines from it: (Please note that you **must** use an editor that will preserve the Tab between **test** and **Password**. Please use an editor such as [Programmer's File Editor](#), pico, vi. Older versions of notepad and the DOS "edit" program do not preserve Tabs.)

```
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 if something is not configured correctly. If everything is properly configured, a "initialized..." 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 and its use:

Q 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

If you change the users file, you must either stop and re-start RadiusNT/X or issue a 'radlogin *reload* secret' command.

ODBC Mode

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

RadiusNT/X's ODBC layout is based on the database layout of Emerald, the Internet 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 database systems.

To configure an ODBC DSN for RadiusNT/X, follow the steps outlined in [Chapter 1 – ODBC Settings](#).

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, then append the information to the detail file for that NAS.

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 yyyy
save glo
```

Where x.x.x.x is the IP address of the machine that you have RadiusNT/X running on and yyyy 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=yyyy
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=yyyy
```

Where x.x.x.x is the IP address of the machine that you have RadiusNT/X running on and yyyy 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.

Please see the radlogin documentation for more information on using Radlogin.

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.



Services

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 can not start. 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 can authenticate from a UNIX *passwd*, *spasswd* or comparable file, similar to the way UNIX RADIUS servers function. For RadiusNT to authenticate a user from the “*passwd*” file, you will need to make the user’s password “UNIX” in the RadiusNT/X *users* file or database. Please note that case is significant. When RadiusNT 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 ODBC and text file user 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 in the advanced section of RadiusNT/X Web configuration. 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 “WINNT” in the RadiusNT *users* file or database. 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 ODBC and text file user 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 in the RadiusNT/X Configuration Administrator.

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 includes additional authentication methods when using a Professional or Enterprise license. 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
-d [path]	DataDirectory	This designates the directory where RadiusNT reads the <i>users</i> , <i>clients</i> , <i>dictionary</i> and <i>passwd</i> files.
-l[#]	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 both username and password case insensitive comparisons.																
-M[#] -o or -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 both the <i>users</i> file and the database. Please note that the database is checked first . This option also sends accounting information to both. The "-M" parameter allows you to set text mode (0), ODBC (1) or both (2).																
-n [DataSource]	ODBCDataSource	If RadiusNT is in ODBC mode (-o or -b), it will use the specified ODBC DataSource Name rather than the default of "radius".																
-p0 [port]	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.																
-p1 [port]	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.																
-P[#]	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><tr><td>1 Concurrency Lockout</td><td>2 Manual ServerPorts Update</td></tr><tr><td>4 Enable Time banking</td><td>8 Manual SubAccounts Update</td></tr><tr><td>16 No clear clear by AcctStatusType</td><td>32 Ascend Max Time Support</td></tr><tr><td>64 Reserved</td><td>128 External Password Replace</td></tr><tr><td>256 Server Port Access</td><td>512 Account Start Records Only</td></tr><tr><td>1024 User Login Triggers</td><td>2048 Allow any request type</td></tr><tr><td>4096 Server DNIS Access</td><td>8192 Check RadRejects</td></tr><tr><td>16384 Disable class support.</td><td>32768 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 not a full path and should only 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> <p>1 Information 2 User Debug 4 ODBC Debug 8 File Debug 16 SNMP Debug 32 Smart cache debug 64 Memory debug</p> <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>
-X		This option specifies packet level debugging.

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

Registry	Description
License	This entry displays the RadiusNT license.
CompanyName	This entry displays the company name that is licensed for RadiusNT use.
DBM	<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 Supported Database Systems 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>
ODBCTimeout	This entry displays the number of seconds RadiusNT will wait for an ODBC query to return (default is 15 seconds).
Username	This shows the username that RadiusNT will use to make the ODBC connection.
Password	This shows the password that RadiusNT will use to make the ODBC connection.
Logfile	This entry shows what log file is used for RADIUS authentication requests (and accounting requests if an accounting logfile is not specified).
AcctODBCDataSource	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.
AcctUsername	This entry displays the username RadiusNT will use to make the ODBC connection to the alternate ODBC datasource for accounting.

AcctPassword	This entry displays the password RadiusNT will use to make the ODBC connection to the alternate ODBC datasource for accounting.
AcctLogfile	This entry shows the filename in which the Accounting Logs will reside. This is typically used in text only mode.
TrimName	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 exactly what the Username attribute contains.
IPCheck	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 only be used for testing or emergency reasons since it allows anyone who knows your global secret to make requests to your RadiusNT server.
GlobalSecret	This displays the global secret to use when IPCheck is set to 0 and the client is unknown.
ProxyTimeout	This entry shows the number of seconds RadiusNT will store a proxy request in memory before it clears (default is 30 seconds).
ProxyID	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.
TestDatabaseSecs	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 (Enterprise & Professional version only).
CacheUserModifyCheckSecs	This entry displays how often (in seconds) the cache database is checked for modifications and updated with fresh information.
CacheUserPrefetchLastDays	Upon startup, this will load users who have called within the specified number of days into the smart cache.
CacheDoubleCheck	<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>
CacheUserNoQueryOnFailSecs	<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>

CacheUserForceUpdateDays	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.
AcctMaxHoldTime	RADIUScan 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. (Enterprise & Professional version only)
SyslogIP	Both error and informational messages can be directed to a syslog server by specifying an IP address. The following are facility codes: [DAEMON] Messages not specific to authentication or accounting [LOCAL0] Authentication specific messages [LOCAL1] Accounting specific messages
CacheServerAccessUpdateMins	This entry shows the Server-Access cache update interval (in minutes).
CacheRootDirectory	This entry shows the directory where RadiusNT stores cache data. (Enterprise & Professional version only)
CacheRoamServerUpdateMins	This shows the Roam Server cache update interval (in minutes). (Enterprise & Professional version only)
MaxAcctSpoolItems	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. 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. (Emerald-only edition limited to 500)
CacheAccountTypesUpdateMins	This entry shows the interval specified for updating of the service types cache.
AgentxSocket	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. 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. (UNIX Enterprise & Professional version only)
CacheWriteMins	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. (Enterprise & Professional version only)
DeferredMemFreeMins	Memory used to update account information s 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)
DatabaseTimeOffsetDays	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).
CacheDNISUpdateMins	This entry displays the DNIS cache update interval (in minutes).
CacheUserDeleteAfterUnusedDays	This entry shows the number of days specified before unrequested accounts will be removed from the cache.
NVFlag	<p>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. (Enterprise & Professional version only)</p> <p>The flags are as follows:</p> <p>1 Accounting 2 Authentication</p>
TacHost	This is the address of the Tacacs server to authenticate against. (Enterprise version only)
TacSecret	This is the Tacacs secret key. Leave it blank to disable password encryption. (Enterprise version only)
TacTimeout	This shows the Tacacs query timeout (in seconds). (Enterprise version only)
TacPort	This is the Tacacs port number of service name (default is port 49). (Enterprise version only)
AuthMethods	<p>This is the space delimited - ordered list, including an optional domain of authentication methods.</p> <p>Ex: (ldap\ldapdomain mycustom.dll\mydomain unix tacacs\tacdomain ldap tacacs) (Enterprise & Professional version only)</p>
ExtLibDirectory	This is the directory to load external authentication libraries from. If no directory is specified, the "radius" directory is used.

ProxyCheckInterval	This displays the number of seconds between requests to a down proxy server to see if it is responding again.
ProxyDown	This displays the number of seconds elapsed between detecting a timeout and considering the proxy server to be down.
DefenderHost	This is a list of Defender servers for authentication. Secondaries are used only when the primary server is not available. (Enterprise version only)
DefenderPort	The Defender port number (Enterprise version only)
DefenderTimeout	The number of seconds to wait for a response from the DMS. (Enterprise version only)
DefenderDown	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. (Enterprise version only)
DefenderAgentID	The AgentID of the DMS session. Defaults to RadiusNT on the Win32 platform and RadiusX on UNIX platforms. (Enterprise version only)
SWECHost	The IP Address of the Safeword authentication server. (Enterprise version only)
SWECPort	The port number (Enterprise version only)
LDAPHost	The list of LDAP Servers to authenticate against. Secondary servers are used only if the primary server is not available. (Enterprise version only)
LDAPPort	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). (Enterprise version only)
LDAPSSLCert	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. (Enterprise version only)
LDAPSearch	The search string used to search accounts or bind as a user. \$login - replaced with current login name. \$domain - replaced with current domain name. (Enterprise version only)
LDAPTimeout	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. (Enterprise version only)
LDAPSearchBind	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. (Enterprise version only)
LDAPSearchPassword	If LDAPSearchBind is set, this is the password used to validate the search bind request. This is normally left blank to allow anonymous connections. (Enterprise version only)
LDAPBaseDirectory	This is the base directory under which to search for matching user entries. (Enterprise version only)
LDAPAccountType	The LDAP attribute used to specify a Database Account Type (Profile). If left blank, this feature is disabled. (Enterprise version only)
LDAPLoginLimit	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. (Enterprise version only)
LDAPScope	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]) (Enterprise version only)

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 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.

By default RadiusNT/X requires many different tables. The following is a list of those tables along with field descriptions.

Table	Column	Datatype	Nullable	Description
AccountTypes	AccountType	varchar(30)	NOT NULL	Name of the account type.
AccountTypes	AccountTypeID	int	IDENTITY	Account type identifier (IDENTITY)
AccountTypes	Description	varchar(100)	NOT NULL	Full description of the account type.
AccountTypes	DNISGroupID	int	NULL	The DNIS Group that the account type is allowed to login to (related DNISGroupID from DNISGroup table). If NULL then no DNIS group is enforced for this account type.
AccountTypes	SortOrder	int	NOT NULL	The order in which subaccounts are displayed to the Radius user.
AccountTypes	BadAccountTypeID	int	NULL	An alternate service type profile used to ACK a request instead of responding with a NAK when an authentication request is bad. If not specified then all authentication requests which fail will be rejected.
AccountTypes	BadAck	int	NULL	<p>If specified BadAck controls the types of authentication failures, which should be acknowledged using the BadAccountType, profile. BadAck is a bit mask of the following values:</p> <p>1 = Bad login/password 2 = Account expired or over credit limit 4 = Over user/group concurrency limit 8 = No time remaining 16 = Account inactive 32 = Access denied, (Port, DNIS, check..etc)</p> <p>Add the options you'd like together. If the BadAck column is not specified then the default value is Account expired(2) and(+) No time</p>

				remaining(8). (=10)
Calls	AccountID	int	NULL	Subaccount identifier of user (if known)
Calls	AcctDelayTime	int	NULL	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.)
Calls	AcctInputOctets	numeric(18 0)	NULL	
Calls	AcctOutputOctets	numeric(18 0)	NULL	
Calls	AcctSessionID	varchar(32)	NOT NULL	NAS generated unique ID for the call.
Calls	AcctSessionTime	int	NULL	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.
Calls	AcctStatusType	smallint	NOT NULL	Account record type: 1 Start 2 Stop 3 Interim Update
Calls	AcctTerminateCause	smallint	NULL	How the session was terminated (integer codes)
Calls	CallDate	smalldatetime	NOT NULL	Date of Call
Calls	CallerID	varchar(20)	NULL	Phone number the user called
Calls	ConnectInfo	varchar(32)	NULL	Customer (Modem protocol/ baud) connection information
Calls	FramedAddress	varchar(64)	NULL	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.
Calls	NASIdentifier	varchar(64)	NOT NULL	Identifier for the NAS (generally the NAS IP address)
Calls	NASPort	varchar(10)	NOT NULL	NAS Port the call came in on.
Calls	NASPortDNIS	varchar(20)	NULL	
Calls	NASPortType	tinyint	NULL	
Calls	ServerID	int	NULL	Server identifier
Calls	UserName	varchar(40)	NULL	Username of caller.

DNISGroups	Description	varchar(45)	NULL	Full description of the DNIS Group.
DNISGroups	DNISGroup	varchar(25)	NOT NULL	Name of the DNIS Group
DNISGroups	DNISGroupID	int	IDENTITY	Group identifier (IDENTITY)
DNISNumbers	DNISGroupID	int	NOT NULL	Related DNIS group identifier (foreign key from DNISGroup table)
DNISNumbers	DNISNumber	varchar(20)	NOT NULL	The DNIS number as reported by the Radius client
Licenses	Company	varchar(80)	NOT NULL	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.
Licenses	LicenseID	varchar(50)	NOT NULL	License key provided by IEA Software upon purchase
MapAttributes	Attribute	varchar(32)	NOT NULL	
MapAttributes	Description	varchar(255)	NULL	
MapAttributes	MapAttribute	varchar(32)	NOT NULL	Identifier of external attribute
MapAttributes	MapType	int	NOT NULL	Groups sets of attributes by their type. (ex LDAP Tacacs External auth)
MapAttributes	MapType	int	NOT NULL	
MapAttributes	RadAttributeID	int	NOT NULL	The Radius attribute mapped to
MapAttributes	RadVendorID	int	NOT NULL	Radius Vendor ID of mapped radius attribute
MapAttributes	ReplyType	smallint	NOT NULL	
MapValues	Description	varchar(255)	NULL	Description of external attribute value
MapValues	MapAttribute	varchar(32)	NOT NULL	Identifier of external attribute
MapValues	MapType	int	NOT NULL	Identifier of type of external attribute
MapValues	RadValue	int	NOT NULL	Radius attribute value (number)
MapValues	Value	varchar(32)	NOT NULL	Attribute value (number)
MasterAccounts	Active	smallint	NOT NULL	Account active flag 0 -- not active will not be authenticated 1 - active
MasterAccounts	CancelDate	datetime	NULL	Date the account will become non- active or terminated
MasterAccounts	Comments	text	NULL	Account comments
MasterAccounts	CreateDate	datetime	NULL	Date the account was created
MasterAccounts	CustomerID	int	IDENTITY	Customer identifier (IDENTITY)

MasterAccounts	FirstName	varchar(25)	NULL	Customer first name
MasterAccounts	LastModifyDate	datetime	NULL	Date the master account record was last modified
MasterAccounts	LastModifyUser	varchar(32)	NULL	Username that last modified the account record (if available)
MasterAccounts	LastName	varchar(25)	NULL	Customer last name
MasterAccounts	Operator	varchar(32)	NULL	Operator that created the account
MasterAccounts	OverDue	smallint	NULL	How many days overdue to allow for all accounts.
MasterAccounts	StartDate	datetime	NULL	Date the account became or will become active
RadATConfigs	AccountTypeID	int	NOT NULL	Associated Account type (related AccountTypeID from AccountType table).
RadATConfigs	Data	varchar(255)	NULL	Used for string IP address or date attribute types
RadATConfigs	LastModifyDate	datetime	NULL	Date record last modified/updated
RadATConfigs	LastModifyUser	varchar(32)	NULL	User that last modified/updated this record
RadATConfigs	RadATConfigID	int	IDENTITY	RadATConfig identifier (IDENTITY)
RadATConfigs	RadAttributeID	int	NOT NULL	Associated Radius attribute (related RadAttributeID from RadAttributes table).
RadATConfigs	RadCheck	smallint	NULL	attribute type 0 denotes a normal reply attribute non-zero denotes this is a check attribute
RadATConfigs	RadVendorID	int	NOT NULL	If this attribute is a vendor specific attribute (radattribute = 26) then this denotes a vendor id. Otherwise the value should be NULL or 0
RadATConfigs	Tag	int	NULL	For attributes supporting it tag values allow grouping multiple attributes within a single radius response.
RadATConfigs	Value	int	NULL	Used for integer attribute types.
RadAttributes	AliasAttributeID	int	NULL	Radius attribute (from RadAttributes table) of similar Radius attribute for logging of accounting data.
RadAttributes	AliasVendorID	int	NULL	VendorID of AliasAttributeID
RadAttributes	Name	varchar(40)	NOT NULL	Name of the radius attribute
RadAttributes	RadAttributeID	int	NOT NULL	Radius Attribute identifier (IDENTITY)
RadAttributes	RadAttributeType	int	NOT NULL	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
RadAttributes	RadVendorID	int	NOT NULL	If this attribute is a vendor specific attribute (radattribute = 26) then this denotes a vendor id. Otherwise the value should be NULL or 0.
RadAttributes	ReplyType	int	NULL	Reply type 0 Accounting Only 1 Reply only 2 Check only 3 Check & Reply
RadConfigs	AccountID	int	NOT NULL	Associated subaccount (related AccountID from SubAccounts table).
RadConfigs	Data	varchar(255)	NULL	Used for string ip address or date attribute types
RadConfigs	LastModifyDate	datetime	NULL	Date this record was last updated
RadConfigs	LastModifyUser	varchar(32)	NULL	User that last modified this record
RadConfigs	RadAttributeID	int	NOT NULL	Associated Radius attribute (RadiusAttributeID from RadAttributes table).
RadConfigs	RadCheck	smallint	NULL	attribute type 0 denotes a normal reply attribute non-zero denotes this is a check attribute
RadConfigs	RadConfigID	int	IDENTITY	RadConfig identifier (IDENTITY)
RadConfigs	RadVendorID	int	NOT NULL	If this attribute is a vendor specific attribute (radattribute = 26) then this denotes a vendor id. Otherwise the value should be NULL or 0.
RadConfigs	Tag	int	NULL	For attributes supporting it tag values allow grouping multiple attributes within a single radius response.
RadConfigs	Value	int	NULL	Used for integer attribute types
RadDestTypes	RadDestType	varchar(64)	NOT NULL	Destination type label
RadDestTypes	RadDestTypeID	int	NOT NULL	Destination type identifier (IDENTITY)
RadFilterGroups	Description	varchar(255)	NULL	Filter group description
RadFilterGroups	DestData	varchar(255)	NULL	Destination data has two separate uses depending on the selected destination type. It is used to send a reply-message when the destination type is NAK. Or it can be used to supply parameters for the source specific destination type. See source specific above for details.
RadFilterGroups	DestRadFilterGroupID	int	NULL	Destination RadFilterGroupID

	D			
RadFilterGroups	RadDestTypeID	int	NOT NULL	Destination type identifier 1 = Filter Replace 2 = Filter Merge 3 = Nak 4 = Ignore 5 = Source Specific
RadFilterGroups	RadFilterGroup	varchar(64)	NOT NULL	Name of the current filter group
RadFilterGroups	RadFilterGroupID	int	IDENTITY	Filter group identifier (IDENTITY)
RadFilterGroups	RadSourceTypeID	int	NOT NULL	Source type identifier 1 = Disable or Chain Dest 10 = Auth In 11 = Auth Out 12 = Auth Proxy Out 13 = Auth Proxy Req+Resp 20 = Acct In 21 = Acct Out 22 = Acct Proxy Out
RadFilterGroups	SortOrder	smallint	NOT NULL	Controls the order in which filter groups are searched and processed. Note that multiple filter groups can be matched ('Filter Replace' or 'Filter Merge' destination types) and applied per request.
RadFilters	Data	varchar(255)	NULL	Contains values used by filters for matching setting or replacing data. This field can contain variables in the form of \$myvariablename. \$myvariablename will match the name of any source RADIUS attribute present with non-alphanumeric stripped out of the name. (For example 'Framed-Netmask' becomes '\$FramedNetmask') There is an additional variable '\$useronly' containing the domain stripped version of the RADIUS User-Name attribute. If \$myvariablename does not match an existing source attribute the string '\$myvariablename' is used unmodified.
RadFilters	RadAttributeID	int	NULL	When filter type is 'Radius Attribute' Vendor ID and Attribute ID indicate the RADIUS attribute being searched or replaced.
RadFilters	RadFilterGroupID	int	NOT NULL	Filter group identifier
RadFilters	RadFilterID	int	IDENTITY	RADIUS filter identifier (IDENTITY)
RadFilters	RadFilterTypeID	int	NULL	Filter type identifier 1 = Client IP 2 = Host IP 3 = Radius Attribute 4 = Destination IP
RadFilters	RadMergeTypeID	int	NULL	Merge type identifier 1 = Delete 2 = Delete matching 3 = Add 4 = Replace value 5 = Add or replace value
RadFilters	RadSearchTypeID	int	NOT NULL	Search type identifier 1 = String 2 =

				Substring 3 = Equal 4 = Less than 5 = Greater than 6 = Ends with 7 = Starts with 8 = Any value
RadFilters	RadVendorID	int	NULL	When filter type is 'Radius Attribute' Vendor ID and Attribute ID indicate the RADIUS attribute being searched or replaced. VendorID is zero for standard RADIUS attributes greater than 0 for VSAs.
RadFilterTypes	RadFilterType	varchar(64)	NOT NULL	Filter type label
RadFilterTypes	RadFilterTypeID	int	NOT NULL	Filter type identifier (IDENTITY)
RadIPAccountTypes	AccountTypeID	int	NULL	Associated with Account type (related AccountTypeID from AccountType table).
RadIPAccountTypes	RadIPAccountTypeID	int	NOT NULL	RadIPAccountType identifier (IDENTITY)
RadIPAccountTypes	RadIPGroupID	int	NULL	Associated RadIP Group (related RadIPGroup from RadIPGroup table).
RadIPAccountTypes	ServerGroupID	int	NOT NULL	Associated Server Group (related ServerGroupID from ServerGroup table).
RadIPAddresses	IPAddress	varchar(16)	NOT NULL	Associated IPAddress
RadIPAddresses	LastUsed	datetime	NULL	Date this IP last checked out
RadIPAddresses	NASIdentifier	varchar(16)	NULL	If the address is checked out this contains the last IPv6 IPv4 or hostname of RADIUS client this address was allocated to. Also see NASPort
RadIPAddresses	NASPort	varchar(10)	NULL	NAS Port associated with server/port.
RadIPAddresses	RadIPGroupID	int	NOT NULL	Associated Radius IP Group (related RadIPGroupID from RadIPGroup table).
RadIPAddresses	State	int	NOT NULL	Address checkout state 0 Available 1 Auth In Use 2 Acct In Use
RadIPGroups	RadIPGroup	varchar(32)	NOT NULL	Name of RadIPGroup
RadIPGroups	RadIPGroupID	int	IDENTITY	RadIPGroup Identifier (IDENTITY)
RadLogMsgs	Description	varchar(50)	NOT NULL	Description of Log Message
RadLogMsgs	RadLogMsgID	int	NOT NULL	Log Message Identifier (see ODBC logging)

RadLogMsgs	Severity	int	NOT NULL	Error severity of associated Log Message
RadLogs	CallerID	varchar(30)	NULL	The associated Caller ID of log entry
RadLogs	Data	varchar(50)	NULL	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.
RadLogs	LogDate	smalldatetime	NOT NULL	The log message date
RadLogs	NASIdentifier	varchar(64)	NULL	The associated NAS Identifier of log entry
RadLogs	NASPort	varchar(10)	NULL	The associated NAS Port of log entry
RadLogs	RadLogMsgID	int	NOT NULL	Log Message Identifier (type of log message)
RadLogs	UserName	varchar(40)	NOT NULL	The associated username (if exists) of log entry
RadMergeTypes	RadMergeType	char(64)	NOT NULL	Merge type label
RadMergeTypes	RadMergeTypeID	int	NOT NULL	RADIUS merge type identifier (IDENTITY)
RadProxyAttribute Groups	Description	varchar(255)	NULL	Description of the proxy group
RadProxyAttribute Groups	Priority	int	NOT NULL	It is possible that more than one attribute group can match a single request. Since a request can be proxied to only one server this determines how salient a particular group is over another. Please note that the lowest priority group takes precedence.
RadProxyAttribute Groups	ProxyGroupName	varchar(32)	NOT NULL	Identifying name of the Proxy group
RadProxyAttribute Groups	RadProxyAttributeGroupID	int	IDENTITY	Group Identifier (IDENTITY)
RadProxyAttribute Groups	RadRoamServerID	int	NULL	Radius Roam Server identifier (IDENTITY)
RadProxyAttributes	RadAttributeID	int	NOT NULL	Related Radius attribute (RadAttributeID from RadAttribute table)
RadProxyAttributes	RadProxyAttributeGroupID	int	NULL	Group Identifier (IDENTITY)

RadProxyAttributes	RadProxyAttributeID	int	IDENTITY	Identifier of proxied attribute (IDENTITY)
RadProxyAttributes	RadVendorID	int	NOT NULL	Related Radius attribute vendor
RadProxyAttributes	SearchType	smallint	NOT NULL	type of rules used in searching for matching attribute/values 1 string 2 substring 3 equal 4 less than 5 greater than
RadProxyAttributes	String	varchar(253)	NOT NULL	Value to search on
RadRejects	Data	varchar(255)	NULL	Used for string IP address or date attribute types.
RadRejects	RadAttributeID	int	NOT NULL	Associated Radius attribute (related RadAttributeID from RadAttribute table).
RadRejects	RadRejectID	int	IDENTITY	RadReject identifier (IDENTITY)
RadRejects	RadVendorID	int	NOT NULL	If this attribute is a vendor specific attribute (radattribute = 26) then this denotes a vendor id. Otherwise the value should be NULL or 0
RadRejects	Value	int	NULL	Used for integer attribute types.
RadRoamDomains	AccountTypeID	int	NULL	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 account type.
RadRoamDomains	Domain	varchar(32)	NOT NULL	Roam domain in the login (user@domain).
RadRoamDomains	Priority	int	NOT NULL	The Roam Server's priority in this domain
RadRoamDomains	RadRoamDomainID	int	IDENTITY	Rad Roam Domain identifier (IDENTITY)
RadRoamDomains	RadRoamServerID	int	NOT NULL	Which Rad Roam Server this entry is associated with (RadRoamServerID from RadRoamServer table).
RadRoamServers	AcctPort	int	NULL	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.
RadRoamServers	AuthPort	int	NULL	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.
RadRoamServers	IPAddress	varchar(64)	NULL	IP address of the Roam Server
RadRoamServers	RadRoamServerID	int	IDENTITY	Radius Roam Server identifier (IDENTITY)
RadRoamServers	RateMax	int	NULL	Maximum number of requests per second this roam server is allowed to receive.
RadRoamServers	RateTarget	int	NULL	Target number of proxy requests to send to this roam server per second.
RadRoamServers	Retries	int	NOT NULL	Number of retries (not currently used)
RadRoamServers	Secret	varchar(16)	NOT NULL	Shared Secret for requests going to roam server.
RadRoamServers	Server	varchar(32)	NOT NULL	Name of the Roam Server
RadRoamServers	StripDomain	smallint	NOT NULL	Strip the domain from the username before sending request.
RadRoamServers	Timeout	int	NOT NULL	Number of seconds to wait for a reply.
RadRoamServers	TreatAsLocal	smallint	NOT NULL	Do not proxy domain from the username before sending request.
RadSearchTypes	RadSearchType	varchar(64)	NOT NULL	Search type label
RadSearchTypes	RadSearchTypeID	int	NOT NULL	RADIUS search type identifier.
RadSourceTypes	RadSourceType	varchar(64)	NOT NULL	Source type label
RadSourceTypes	RadSourceTypeID	int	NOT NULL	Source type identifier (IDENTITY)
RadTriggers	AccountID	int	NOT NULL	Trigger associated to this subaccount id
RadTriggers	Directory	varchar(128)	NULL	Working directory for the program or file
RadTriggers	FileName	varchar(64)	NOT NULL	Executable program or file to run
RadTriggers	Parameters	varchar(64)	NULL	parameter(s) for the program or file
RadTriggers	RadTriggerID	int	IDENTITY	Trigger identifier (IDENTITY)
RadTriggers	TriggerType	int	NULL	Type of trigger (currently not used)
RadValues	Name	varchar(40)	NOT NULL	Attribute value name
RadValues	RadAttributeID	int	NOT NULL	Associated radius attribute (RadAttributeID from RadAttributes table).
RadValues	RadVendorID	int	NOT NULL	If this attribute is a vendor specific attribute (radattribute = 26) then this denotes a vendor id. Otherwise the value should be NULL or 0

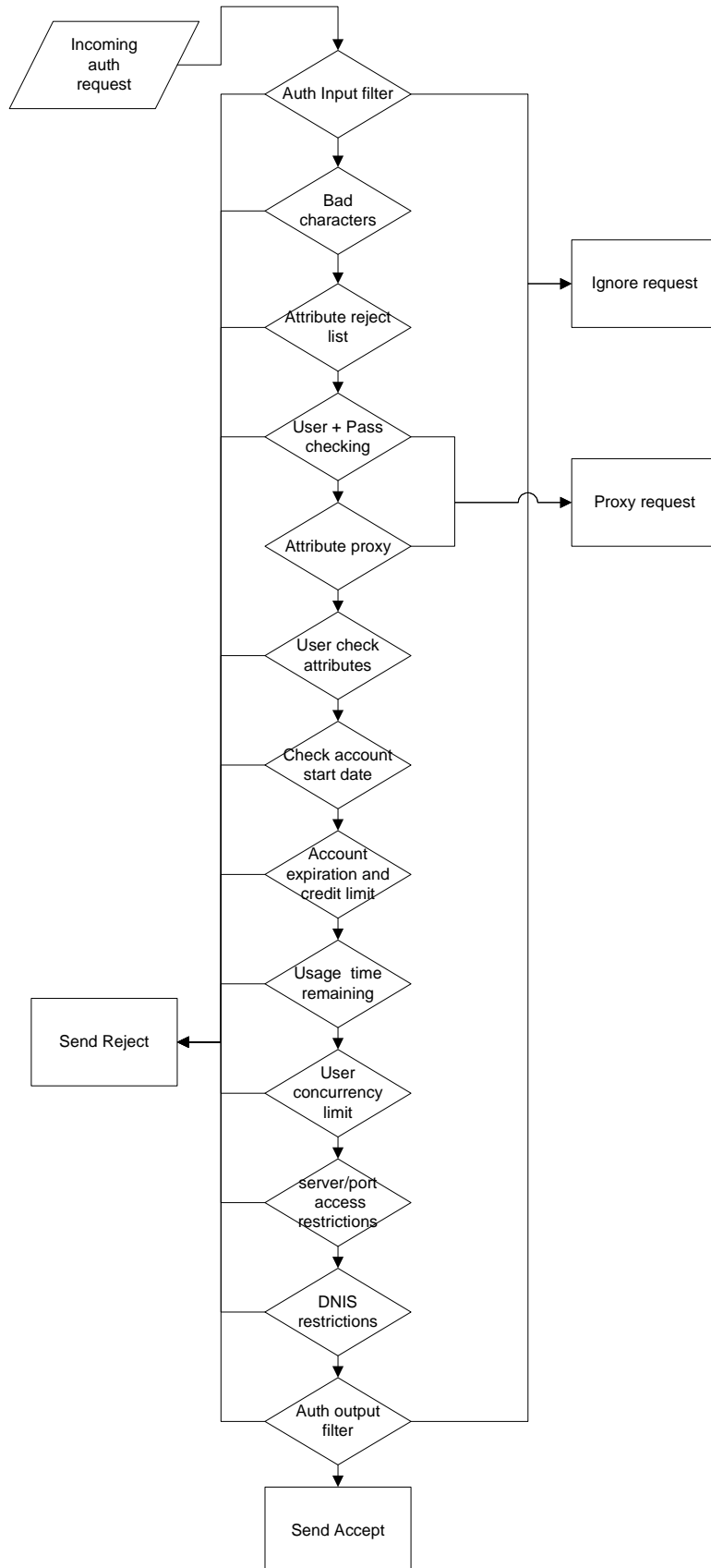
RadValues	Value	int	NOT NULL	Attribute value number
RadVendors	Name	varchar(32)	NOT NULL	Name of vendor
RadVendors	RadVendorID	int	NOT NULL	RadVendor identifier (industry/vendor specified)
ServerAccess	AccountTypeID	int	NULL	What Account type this entry is associated with (related AccountTypeID from AccountType table).
ServerAccess	MaxSessionLength	int	NULL	The maximum session length allowed.
ServerAccess	Port	varchar(10)	NULL	Which port that this record is associated with (related Port from ServerPorts table).
ServerAccess	ServerAccessID	int	IDENTITY	Server Access identifier. (IDENTITY)
ServerAccess	ServerID	int	NULL	What Server this entry is associated with (related ServerID from Servers table).
ServerAccess	StartTime	int	NULL	The start time allowed to login in minutes from midnight
ServerAccess	StopTime	int	NULL	The stop time allowed to login in minutes from midnight.
ServerGroups	ServerGroup	varchar(32)	NOT NULL	Server Group name (description).
ServerGroups	ServerGroupID	int	IDENTITY	Server Group identifier (IDENTITY)
ServerPorts	AccountID	int	NULL	The RadiusNT subaccount id of the last user of the port (if available).
ServerPorts	AcctSessionID	varchar(32)	NULL	The NAS AccountSessionID value of the last user on the port.
ServerPorts	AcctStatusType	smallint	NULL	The status of the last user on the port.
ServerPorts	CallDate	smalldatetime	NULL	The call date of the last user on the port.
ServerPorts	CallerID	varchar(20)	NULL	The CallerID of the last user of the port.
ServerPorts	ConnectInfo	varchar(32)	NULL	The Connect Information from the NAS for the last user of the port.
ServerPorts	FramedAddress	varchar(64)	NULL	The Framed Address of the last user on the port.
ServerPorts	IPAddress	varchar(64)	NULL	The IP address of the last user on the port.
ServerPorts	MaxSessionTime	int	NULL	The maximum session time allowed

				on the port.
ServerPorts	NASIdentifier	varchar(64)	NOT NULL	The IP Address or NAS-Identifier field if NAS-IP or NAS-IPv6 is not available. Specifies the address or hostname of the RADIUS client initiating an accounting request.
ServerPorts	Port	varchar(10)	NOT NULL	The port number.
ServerPorts	ServerID	int	NOT NULL	Which server this port is associated with (related serverid from Servers table).
ServerPorts	SNMPUser	varchar(64)	NULL	SNMP Object Identifier (OID) string for the SNMP concurrency checking.
ServerPorts	UserName	varchar(40)	NULL	The last username that used the port.
Servers	Comments	text	NULL	Optional comments regarding the server
Servers	Community	varchar(16)	NULL	SNMP Community for the server.
Servers	IPAddress	varchar(64)	NOT NULL	IP address of RADIUS client
Servers	RadRoamServerID	int	NULL	Radius Roam Server identifier (IDENTITY)
Servers	Secret	varchar(16)	NULL	The Shared Secret for the RADIUS client
Servers	Server	varchar(25)	NOT NULL	RADIUS client name of server
Servers	ServerGroupID	int	NULL	Associated Server Group identifier (foreign key from ServerGroup table)
Servers	ServerID	int	IDENTITY	Server identifier (IDENTITY)
Servers	ServerType	int	NULL	Type of server
ServerTypes	Model	varchar(32)	NULL	Server model
ServerTypes	ServerType	int	NOT NULL	Server Type identifier
ServerTypes	SNMPType	int	NULL	Associated SNMP Type
ServerTypes	SNMPUser	varchar(64)	NULL	Associated SNMP user
ServerTypes	Vendor	varchar(32)	NOT NULL	Vendor identifier
SubAccounts	AccountID	int	IDENTITY	Subaccount identifier (IDENTITY)
SubAccounts	AccountTypeID	int	NOT NULL	The account type of the service
SubAccounts	Active	smallint	NOT NULL	Subaccount active flag 0 -- not active will not be authenticated 1 - active
SubAccounts	CustomerID	int	NOT NULL	Associated Master account identifier
SubAccounts	Email	varchar(64)	NULL	the email address of the subaccount user
SubAccounts	ExpireDate	datetime	NULL	The date this subaccount will expire. If NULL the subaccount will not

				expire.
SubAccounts	Extension	int	NULL	An extension in days allowed from the expiration date.
SubAccounts	FirstName	varchar(25)	NULL	The first name of the subaccount user
SubAccounts	LastModifyDate	datetime	NULL	The date this record was last modified.
SubAccounts	LastModifyUser	varchar(32)	NULL	The username that last modified this record (if available)
SubAccounts	LastName	varchar(25)	NULL	The last name of the subaccount user
SubAccounts	LastUsed	datetime	NULL	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.
SubAccounts	Login	varchar(40)	NULL	The login id for the subaccount user
SubAccounts	LoginLimit	smallint	NULL	The number of concurrent logins allowed for this subaccount.
SubAccounts	Operator	varchar(32)	NULL	The operator which created this subaccount record.
SubAccounts	Password	varchar(32)	NULL	The password of the subaccount user
SubAccounts	TimeLeft	int	NULL	The login time left (minutes) for the subaccount. This should be set to NULL if the user has no time limitations.

Authentication Process

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



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 which 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 Account Type. This is where you place attributes for generic account 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 Account 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 features per platform

Feature	MS SQL	Sybase	Oracle	MySQL	PostgreSQL	Generic ODBC*
Database Procedures	Yes	Yes	Yes	No	Yes**	Yes
Proxy	Yes	Yes	Yes	Yes	Yes	Yes
Smart Caching	Yes	Yes	Yes	No	Yes	No
Concurrency control	Yes	Yes	Yes	Yes	Yes	Yes
IP Pooling	Yes	Yes	Yes	No	No	Yes
Dictionary	Yes	Yes	Yes	Yes	Yes	Yes
Server Access	Yes	Yes	Yes	Yes	Yes	Yes
Attribute Filtering	Yes	Yes	Yes	Yes	Yes	Yes

Calls	Yes	Yes	Yes	Yes	Yes	Yes
RADIUS Logs	Yes	Yes	Yes	Yes	Yes	Yes
Server Ports	Yes	Yes	Yes	Yes	Yes	Yes
Database install script	Yes	Yes	Yes	Yes	Yes	No
Emerald Express	Yes	Yes	No	No	No	No
Proxy Attributes	Yes	Yes	Yes	Yes	Yes	Yes
RADIUS Rejects	Yes	Yes	Yes	Yes	Yes	Yes
External cmd triggers	Yes	Yes	Yes	Yes	Yes	Yes
DNIS checking	Yes	Yes	Yes	Yes	Yes	Yes
Map Attributes	Yes	Yes	Yes	Yes	Yes	Yes

- * Depends on features supported by RDBMS.
- ** View based

Custom Queries

SQLRadGetServers – Provides a listing of RADIUS clients allowed to make RADIUS authentication or accounting requests.

Column	Type	Required	Description
ServerID	Int	No	Unique ID
Server	Char	No	Server name used in debug messages and name resolution
IPAddress	Char	Yes	IP Address of RADIUS client
Secret	Char	Yes	Shared secret between RADIUS server and client
RadRoamServerID	Int	No	If specified and server proxy is enabled all requests from this client are proxied to the specified roam server.

SQLConnectInit – Used to initialize environment data after the RADIUS server establishes a new connection to the database.

SQLConfigs – Any key used to configure RadiusNT/X listed when typing radius -v with the exception of ODBC database access can be stored in a database table. These options take precedence over those locally configured through the RadiusNT/X admin interface.

Column	Type	Required	Description
Key	Char	Yes	Name of registry key being configured
Value	Char	Yes	Key value

SQLAttributes – List of RADIUS attributes used by the RADIUS server and all NAS clients. If SQLAttribute fails to execute RadiusNT/X loads the dictionary file in the radius directory.

Column	Type	Required	Description
Name	Char	Yes	Attribute Name
AttributeID	Int	Yes	Attribute ID

VendorID	Int	Yes	Attribute Vendor ID
AttributeType	Int	Yes	Attribute Type: 0 = String 1 = Integer 2 = Ipv4 Address 3 = Datetime 4 = Ascend binary filter 5 = Ipv6 Address 10 = TAG String 11 = TAG Integer 12 = TAG Ipv4 Address 13 = TAG Datetime
AliasAttributeID	Int	No	Acct – aliases this attribute to appear as another in the Calls table (Attribute ID)
AliasVendorID	Int	No	Acct – aliases this attribute to appear as another in the Calls table (Attribute Vendor ID)

SQLValues – List of attribute values for attributes loaded through the SQLAttributes query

Column	Type	Required	Description
Name	Char	Yes	Value Name
Value	Int	Yes	Value
AttributeID	Int	Yes	Attribute ID
VendorID	Int	Yes	Attribute Vendor ID

SQLCheckOnline – Returns a single column containing the number of times the user is found to be online. Variables can be any request attribute and \$accountid.

SQLCheckOnlineSNMP – Returns the table below. Variables can be any request attribute and \$accountid

Column	Type	Required	Description
IPAddress	Char	Yes	IP Address of the Radius clients SNMP management interface
SNMPType	Int	No	4 appends current session-id, otherwise send SNMPUser unmodified
Community	Char	Yes	SNMP community name
SNMPUser	Char	Yes	SNMP OID of users session to query
AcctSessionID	Char	No	SessionID from current authentication request

SQLRadConfigs – Returns a list of user specific RADIUS attributes. If any attributes are returned from running this query then the attributes contained within the users Service type profile are ignored. The \$accountid variable must be used to limit query results to the current user.

Example: SELECT AttributeID, VendorID, Data, Value FROM RadConfigs WHERE AccountID=\$accountid

Column	Type	Required	Description
AttributeID	Char	Yes	Attribute ID
VendorID	Int	Yes	Attribute Vendor ID
Tag	Int	No	Grouping tag used with tagged datatypes
RadCheck	Int	No	If set 0 or NULL the attribute is a reply attribute, otherwise it is

			considered a check attribute
Data	Char	Yes	Attribute value (string)
Value	Int	Yes	Attribute value (numeric)

SQLRadATConfigs – Returns a set of attributes associated with a Service type. Any user with the corresponding Service type is given these attributes provided no user-specific attributes have been configured for them. The \$accounttype variable must be used to limit query results to the current Service type.

Example: SELECT AccountType, AttributeID, VendorID, Data, Value FROM AccountTypes WHERE AccountType=\$ accounttype

Column	Type	Required	Description
AccountType	Char	Yes	Service Type this attribute is associated with
AttributeID	Char	Yes	Attribute ID
VendorID	Int	Yes	Attribute Vendor ID
Tag	Int	No	Grouping tag used with tagged datatypes
RadCheck	Int	No	If set 0 or NULL the attribute is a reply attribute, otherwise it is considered a check attribute
Data	Char	Yes	Attribute value (string)
Value	Int	Yes	Attribute value (numeric)

SQLFilterGroups - [See RADIUS filtering](#)

Column	Type	Required	Description
RadFilterGroupID	Int	Yes	See filter groups
RadSourceTypeID	Int	Yes	See filter groups
RadDestTypeID	Int	Yes	See filter groups
DestRadFilterGroupID	Int	Yes	See filter groups
DestData	Char	Yes	See filter groups

SQLFilters – The variable \$RadFilterGroupID must be used as a parameter to only show filters associated with the requested filter group.

Example: SELECT * FROM RadGetFilters WHERE RadFilterGroupID = \$RadFilterGroupID

Column	Type	Required	Description
RadFilterTypeID	Int	Yes	See filters
VendorID	Int	Yes	See filters
AttributeID	Int	Yes	See filters
RadSearchTypeID	Int	Yes	See filters
RadMergeTypeID	Int	Yes	See filters
Data	Char	Yes	See filters

SQLRoamServers – RADIUS client list used to accept incoming responses from outgoing proxy servers.

Column	Type	Required	Description
Server	Char	No	Server hostname
IPAddress	Char	Yes	IP Address of roam server

Secret	Char	Yes	Shared secret of roam server
--------	------	-----	------------------------------

SQLRoamDomains – Download the list of roam domains. There should be two sets of results within a UNION one where Label is the Domain and another where it is used as a Roam Server ID. Results should be ordered by Label then Priority.

Column	Type	Required	Description
Label	Char	Yes	Domain and roam server ID
Server	Char	No	Roam server hostname
IPAddress	Char	Yes	Roam server IP Address
Secret	Char	Yes	Roam server shared secret
AccountType	Char	No	Replace response with service type attributes
AuthPort	Int	No	Roam server authentication port
AcctPort	Int	No	Roam server accounting port
Priority	Int	No	Roam server try order
Timeout	Int	No	Request timeout before retry/fail in seconds
Retries	Int	No	Number of retries allowed
StripDomain	Int	No	1 strip auth, 2 strip acct, 3 strip auth + acct
TreatAsLocal	Int	No	Don't proxy handle request as if it were local
RateTarget	Int	No	Ideal proxy forwarding rate in requests/sec
RateMax	Int	No	Maximum proxy forwarding rate in requests/sec

SQLDNIS – Used to provide DNIS based access control when the 'DNIS Checking' option is enabled in the advanced section of RadiusNT/X admin.

Column	Type	Required	Description
AccountType	Char	Yes	Service Type DNIS number is associated with
DNISNumber	Char	Yes	Number

SQLServerAccess – Provides NAS Server + port access control when the 'Server port access' option is enabled in the advanced section of RadiusNT/X admin.

Column	Type	Required	Description
StartTime	Int	No	Start time in minutes past midnight, NULL for midnight
StopTime	Int	No	Stop time in minutes past midnight, NULL for midnight
IPAddress	Char	No	Address of NAS, NULL for any
NASPort	Char	No	NAS Port, NULL for any
AccountType	Char	No	Service Type, NULL for any
MaxSessionLength	Int	No	Maximum session length, NULL for unlimited

SQLPoolConfigs – Allows additional attributes to be sent to the user such as an IP address allocated from a pool. The following variables are available as parameters: \$NASIdentifier, \$NASPort, \$ServerID, \$AccountID and any RADIUS request attribute.

Example: SELECT AttributeID, VendorID, Value, Data FROM Pool WHERE AccountID=\$AccountID AND NASIdentifier = '\$NASIdentifier' AND NASPort = '\$NASPort'

Column	Type	Required	Description
AttributeID	Int	Yes	Attribute ID

VendorID	Int	Yes	Attribute Vendor ID
Value	Int	Yes	Numeric value
Data	Char	Yes	String value, also serves as a access-reject reply message when AttributeID, VendorID and Value are set to '0'.

SQLRejects – Download a list of reject attributes. If any attribute and value matches a reject attribute the authentication request is rejected.

Column	Type	Required	Description
AttributeID	Int	Yes	Attribute ID
VendorID	Int	Yes	Attribute Vendor ID
Value	Int	Yes	Numeric value to match for request to be rejected
Data	Char	Yes	String value to match for request to be rejected

SQLCMDTriggers – Calls a program for the user after successful authentication ordered by the order multiple programs should execute.

Column	Type	Required	Description
FileName	Char	Yes	Program to execute
Parameters	Char	No	Program parameters
Directory	Char	No	Program working directory

SQLRadGetUser – Authenticate a user. Any request attribute and \$login can be used in the query. The server can test multiple accounts with the same login until it finds one that authenticates (matching user + password) before giving up. Optionally a second result set is returned containing custom reply attributes.

Column	Type	Required	Description
Login	Char	Yes	Login username
AccountID	Int	Yes	Unique ID for this account
Password	Char	Yes	Account password
Active	Int	No	Is this account active? 0 = No, 1 = Yes
Domain	Char	No	Domain this account is associated with
AccountType	Char	No	Service type profile associated with this account. Used to set common attributes for
LoginLimit	Int	No	Maximum number of concurrent logins for this account. Concurrency control must be enabled in order for this limit to be enforced.
TimeLeft	Int	No	Maximum session time in seconds, null for unlimited. Time banking must be enabled in order for this limit to be enforced.
ExpireDate	Datetime	No	Account expiration date
StartDate	Datetime	No	Account start date
OverLimit	Int	No	Is the account over its credit limit? 0 = No, 1 = Yes
BadAccountType	Char	No	An alternate service type profile used to ACK a request instead of responding with a NAK when an authentication request is bad. If not specified then all authentication requests which fail will be rejected.
BadAck	Int	No	If specified BadAck controls the types of authentication failures, which should be acknowledged using the BadAccountType, profile. BadAck is a bit mask of the

			<p>following values:</p> <p>1 = Bad login/password 2 = Account expired or over credit limit 4 = Over user/group concurrency limit 8 = No time remaining 16 = Account inactive 32 = Access denied, (Port, DNIS, check...etc)</p> <p>Add the options you'd like together. If the BadAck column is not specified then the default value is Account expired(2) and(+) No time remaining(8). (=10)</p>
--	--	--	--

Second result set (Optional)

Column	Type	Required	Description
AttributeID	Int	Yes	Attribute ID of the reply attribute to send
VendorID	Int	Yes	Attribute Vendor ID of the reply attribute to send
Data	Char	Yes	String data to send in the Access-Accept reply. Or reject the auth request by setting AttributeID, VendorID and Value to 0. In this case Data becomes the reply-msg sent in the Access-Reject.
Value	Int	Yes	Numeric value to send in the reply

SQLProxyAttributes – Downloads attribute proxy rules. If a proxy group is matched the request is redirected to the specified roam server. Results must be ordered by Priority and RadProxyAttributeGroupID. All attribute match conditions for a given RadProxyAttributeGroupID must match in order for a request to be proxied to the roam server.

Column	Type	Required	Description
RadProxyAttributeGroupID	Int	Yes	Proxy group the rule is a part of
RadRoamServerID	Int	Yes	Roam server to redirect requests
String	Char	Yes	The value being matched
SearchType	Int	Yes	The type of search operation (RadSearchTypes) 1 = String 2 = Substring 3 = Equal 4 = Less than 5 = Greater than 6 = Ends with 7 = Starts with
AttributeID	Int	Yes	Attribute ID of the Attribute being matched
VendorID	Int	Yes	Attribute Vendor ID of the Attribute being matched

SQLMapAttributes – Used to map generic Attribute names with RADIUS attributes to allow mapping of data from external sources such as LDAP directories.

Column	Type	Required	Description
MapAttribute	Char	Yes	Mapped attribute name
AttributeID	Int	Yes	RADIUS Attribute ID
VendorID	Int	Yes	Radius Attribute Vendor ID
MapType	Int	Yes	ID of what RADIUS attributes are being mapped to. Currently:

			0 = RADIUS 1 = LDAP 2 = TACACS
--	--	--	--------------------------------------

SQLMapValues – Used to map generic Attribute value names with RADIUS attribute values to allow mapping of data from external sources such as LDAP directories.

Column	Type	Required	Description
MapAttribute	Char	Yes	Mapped attribute name
Value	Char	Yes	Mapped attribute value
RadValue	Int	Yes	Radius attribute value ID
MapType	Int	Yes	ID of what RADIUS attributes are being mapped to. Currently: 0 = RADIUS 1 = LDAP 2 = TACACS

ODBCTable – Used to specify the name of the default calls table. If ODBCTable is not specified a table name of 'Calls' is used.

PortsTable – Used to specify the name of the default server ports table. If PortsTable is not specified a table name of 'ServerPorts' is used.

Chapter 9 – ADVANCED FEATURES

RadiusNT/X has several advanced features, most of which are only available when running 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 maintain a list of who is currently on-line. For this feature to work, you **must** add records into the ServerPorts table that match the ServerID from the Servers table, **and** the Port column which matches the NAS-Port attribute in the accounting packet. If need be, you can run RadiusNT/X in -x15 debug mode to view examples of the NAS-Port numbers. RadiusNT/X only **updates** the records of the ServerPorts table, and will not **create** them.

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 gone, 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 in the advanced section of RadiusNT/X Configuration 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 an Account 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 in the Advanced section of RadiusNT/X Configuration Administrator and then restart RadiusNT/X.

DNIS Access

Dialed Number Identification Service (DNIS) Access allows you to limit the telephone numbers an Account 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 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 in after dialing that telephone number. Please note that DNIS Access is **not** enabled by default. You **must** enable DNIS Access in the Advanced section of the RadiusNT/X Configuration 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 Reject List in the Advanced section of RadiusNT/X Configuration 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 what the error is. 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 in the database, 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 and proxy clients 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.
Reconfig	Reload server configuration
RefreshServers	Reload Servers table or clients file.

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. RadiusNT/X also provides its own IP address pooling facility. This works by relying on 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.

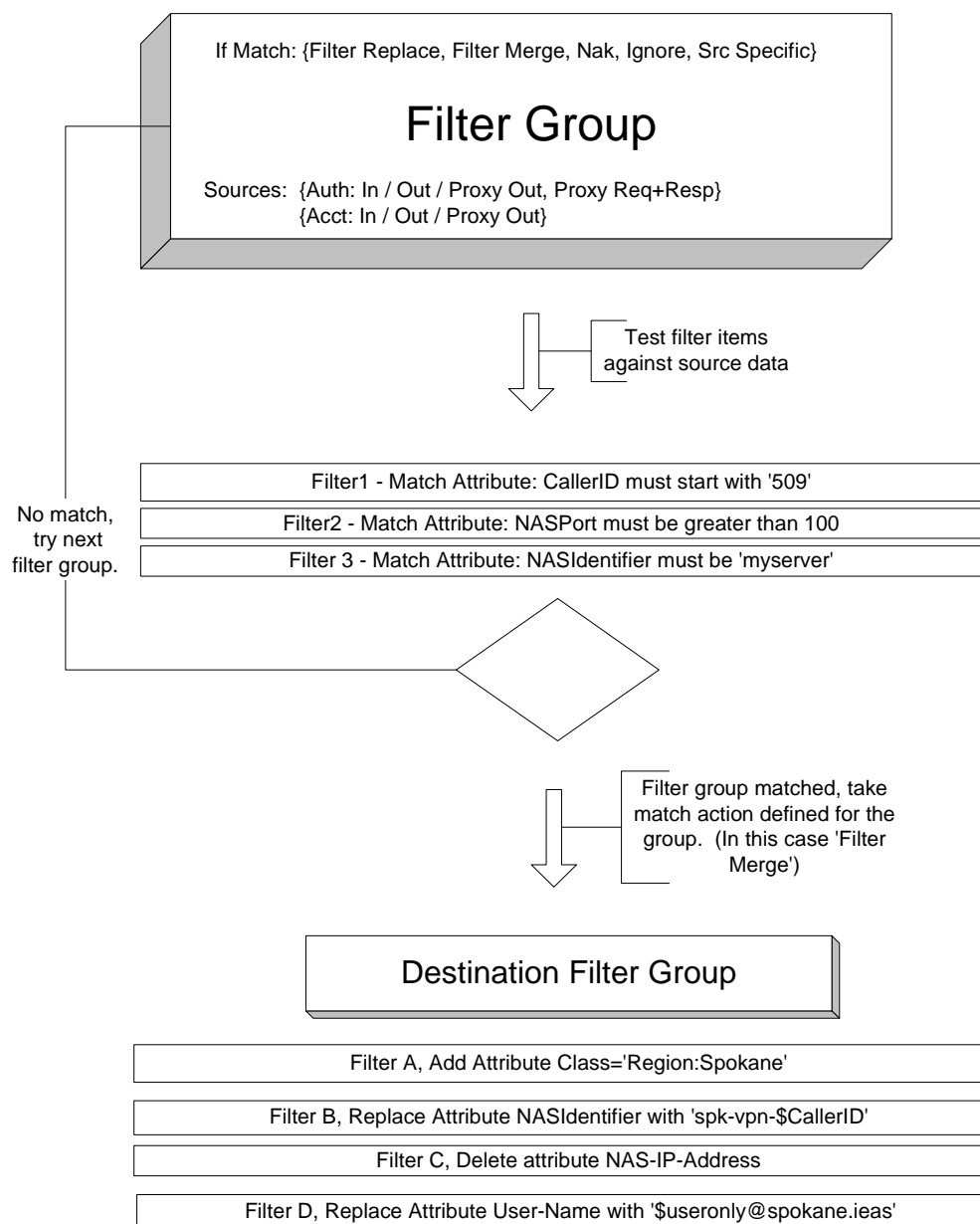
RADIUS Filtering

In some situations to support unique features of various NAS hardware, limit access or enforce policy in roaming environments the RADIUS server may need to add, alter or remove attributes going in, out or passing through the server. RADIUS filtering allows the flexibility to support many of these situations. The use of filtering should not be taken lightly and must be carefully thought out. Applying too many filter groups can make it very difficult to understand or troubleshoot the outcome of filtering actions.

Filtering is accomplished with Filters and Filter Groups.

Filter Groups define the source of the attributes to match and the action to take when there is a match.

Filters define a list of rules used in matching filter groups to attributes. Each filter is associated with a filter group.



Filter Groups (RadFilterGroups table)

Filter Group (RadFilterGroup) is the name of the filter group.

Description (Description) is an optional detailed description of the group.

Filter source (RadSourceTypes) define what is being filtered. (See below)

ID	Option	Description
1	Disable or Chain Dest	Group can only be used as a destination filter group.

10	Auth In	Modifies incoming authentication requests before being processed by RadiusNT/X.
11	Auth Out	Modifies outgoing authentication responses after being processed by RadiusNT/X.
12	Auth Proxy Out	Modifies outgoing proxy authentication REQUESTS after being processed by RadiusNT/X.
13	Auth Proxy Req+Resp	This is a special case for authentication proxy that uses the authentication request attributes to match the filter group – however the authentication response is actually modified.
14	Auth Req+Resp	This is a special case for authentication requests that uses the authentication request attributes to match the filter group – however the authentication response is actually modified.
15	Auth Proxy Resp	Modifies the outgoing proxy authentication RESPONSE after being processed by RadiusNT/X. (Requires RadiusNT/X 5.0.46+)
20	Acct In	Modifies incoming accounting requests before being processed by RadiusNT/X. Destination data sets an alternate local accounting table other than the default “Calls” table.
21	Acct Out	Reserved for future use.
22	Acct Proxy Out	Modifies outgoing proxy accounting REQUESTS after being processed by RadiusNT/X.

Filter destination (FilterDestTypes) define what action to take when a filter group matches. (See below)

ID	Option	Description
1	Filter Replace	Removes all source attributes before applying destination filters. Note that certain RADIUS attributes normally are excluded
2	Filter Merge	Uses the merge settings of individual destination filters to specify how the source attributes should be modified.
3	Nak	Sends an authentication NAK to the request optionally sending destination data (DestData) as the reply-message. If NAK is used with an accounting request – the request is ignored.
4	Ignore	Drops the request without responding. Ignore is not enforced for proxy sources.
5	Source Specific	Source specific is used in conjunction with destination data (DestData) to specify custom behavior specific to a source. When the ‘Acct Out’ source is used Destination data becomes the name of an alternate table to log calls. (Different from the default “Calls” table)

Destination filter group (DestRadFilterGroupID) is the filter group containing filters responsible for altering attributes. This is used only where filter destination type is set to ‘Filter Replace’ or ‘Filter Merge’, otherwise its ignored.

Destination data (DestData) has two separate uses depending on the selected destination type. It is used to send a reply-message when the destination type is NAK. Or it can be used to supply parameters for the source specific destination type. See source specific above for details.

Sort order (SortOrder) controls the order in which filter groups are searched and processed. Note that multiple filter groups can be matched (‘Filter Replace’ or ‘Filter Merge’ destination types) and applied per request.

Each subsequent change in the attributes used for matching is visible to the filtering system allowing multiple filter groups to modify attributes in a way that may effect or interfere with the operation of another. However no further filter processing is done after a filter group with either a Nak or Ignore destination type

is matched. Filter groups are processed in reverse order as the result set returned by the RadGetFilterGroups stored procedure or equivalent query.

Filters (RadFilters table)

Filter group (RadFilterGroupID). Filter group the filter is associated with.

Filter type (RadFilterTypeID) Type of data being filtered. (See below)

ID	Option	Description
1	ClientIP	IP Address of the RADIUS client initiating the request
2	HostIP	IP Address if the RADIUS server
3	Radius Attribute	RADIUS source attribute
4	DestinationIP	IP Address of RADIUS server the request is being proxied to

Radius Vendor ID (RadVendorID). When filter type is 'Radius Attribute' Vendor ID and Attribute ID indicate the RADIUS attribute being searched or replaced. VendorID is zero for standard RADIUS attributes, greater than 0 for VSAs.

Radius Attribute ID (RadAttributeID). When filter type is 'Radius Attribute' Vendor ID and Attribute ID indicate the RADIUS attribute being searched or replaced.

Radius search types (RadSearchTypeID). When using a filter to match data, search type specifies which match operation to use. (See below) Search types only apply when using a Filter type of RADIUS Attribute. When using other filter types such as ClientIP, HostIP or DestinationIP matching is always done as an exact string match.

ID	Option	Description
1	String	Exactly match string
2	Substring	Match any portion of a string
3	Equal	Exactly match a numeric value
4	Less than	Is less than a numeric value
5	Greater than	Is greater than a numeric value
6	Ends with	Exactly match the ending portion of a string
7	Starts with	Exactly match the starting portion of a string
8	Any value	Match any value including null

Radius merge types (MergeTypeID). When using RADIUS filters to filter data, merge type specifies which filtering operation to use. (See below)

ID	Option	Description
1	Delete	Delete any source attribute matching Vendor ID and Attribute ID
2	Delete matching	Delete only source attributes matching Vendor ID, Attribute ID and contain a matching value (Data)
3	Add	Add a new source attribute containing VendorID, AttributeID and the contents of Data as the attribute value.
4	Replace value	For every source attribute matching Vendor ID and Attribute ID replace its current value with the contents of Data.
5	Add or replace value	For every source attribute matching Vendor ID and Attribute ID replace its current value with the contents of Data or add a new source attribute containing VendorID, AttributeID and Data if no matching source attributes are found.
6	Add attributes from query	The data field contains an SQL query that retrieves attributes from the authentication database and adds them to the response. The result set returned

		by this query must contain the following three columns "AttributeID", "VendorID", and "Data". If this query fails for any reason the authentication request is rejected.
--	--	--

Data (Data). Contains values used by filters for matching, setting or replacing data. This field can contain variables in the form of \$myvariablename. \$myvariablename will match the name of any source RADIUS attribute present with non-alphanumeric stripped out of the name. (For example 'Framed-Netmask' becomes '\$FramedNetmask') There is an additional variable '\$useronly' containing the domain stripped version of the RADIUS User-Name attribute. If \$myvariablename does not match an existing source attribute the string '\$myvariablename' is used unmodified.

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.

To achieve Server Based Proxy, begin by selecting the Server Based Proxy option in 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 does **not** process the request locally. In addition, the StripDomain and TreatAsLocal options are not applicable in this case.

Modifying Return Attributes

If the AccountType field in the RadRoamDomains table is **not** NULL, then RadiusNT/X will return the set of attributes associated with that particular AccountType 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 tries should be sent to the primary server and the interval between retries. Once the primary server has been identified as down, RadiusNT/X 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 each. 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.radiusAuthSe  
rv.radiusAuthServIdent.0 = "RadiusNT 2.5.116"
```

```
radius.radiusAuthentication.radiusAuthServMIB.radiusAuthServMIBObjects.radiusAuthSe  
rv.radiusAuthServUpTime.0 = 119192
```

```
radius.radiusAuthentication.radiusAuthServMIB.radiusAuthServMIBObjects.radiusAuthSe  
rv.radiusAuthServResetTime.0 = 119192
```

```
radius.radiusAuthentication.radiusAuthServMIB.radiusAuthServMIBObjects.radiusAuthSe  
rv.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 Request	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) 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
Lucent	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.
Lucent	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).
Cisco	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.
Ascend	Max 4xxx	.1.3.6.1.4.1.529.12.3.1.4.	5, 6, 7, 8	ServerType must be set to 5-8 for this to work.
3Com	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.
Nortel	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 RadCheckOnlineSNMP 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.

Server Types

RadiusNT/X uses the ServerType field in the Servers Table to track the types of servers. 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
Generic	Starts at 0	0	Use SNMPUser as OID
Generic	Starts at 0	1	Use SNMPUser as OID
Lucent	Portmaster 2	2	Use SNMPUser as OID
Lucent	Portmaster 3	3	Use SNMPUser as OID
Lucent	Portmaster 4	4	Use SNMPUser as OID
Ascend	MAX 40xx/60xx T1	5	Add ASID To SNMPUser
Ascend	MAX 40xx/60xx E1	6	Add ASID To SNMPUser
Ascend	MAX 1800	7	Add ASID To SNMPUser
Ascend	MAX TNT	8	Add ASID To SNMPUser
Cisco	AS 5x00	9	Use SNMPUser as OID
3Com	Total Control	10	Use SNMPUser as OID
Computone	Power Rack	11	Use SNMPUser as OID
Microcom	6000	12	Use SNMPUser as OID
3Com/USR	HiPer ARC	13	Use SNMPUser as OID
Nortel	5399	14	Use SNMPUser as OID

Smart Cache

A new feature, starting with RadiusNT/X 3.0, is the inclusion of a Smart Cache engine that is very flexible and powerful. The following section describes various aspects and behaviors of the Smart Cache so that you can tune it to meet your specific needs.

The primary feature of the Smart Cache is the ability to maintain operations in the event of a database (or connection to the database) failure. This feature allows RadiusNT/X to continue operating until the problem can be fixed. It also includes the ability to have 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.

Smart Cache's next feature is the ability to off-load redundant processing from the database to the local servers. This removes a large strain from the database as the number of requests and users grow. You can define the maximum interval for how often the cache information is refreshed, but in most cases it will intelligently update itself as needed before those 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 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 Radius 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	Search string
Netscape LDAP/Messaging Server	(uid=\$login)
Microsoft Active Directory	cn=\$login,cn=users,dc=\$domain
Novell NDS	(cn=\$login)
posixAccount* objectClass	(&(uid=\$login)!(shadowInactive=1))
Generic	(&(uid=\$login)(ou=\$domain))

Chapter 11 – ENTERPRISE VERSION FEATURES

When RadiusNT/X is run with either an Enterprise license, additional features become available. 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 IPAddress, 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

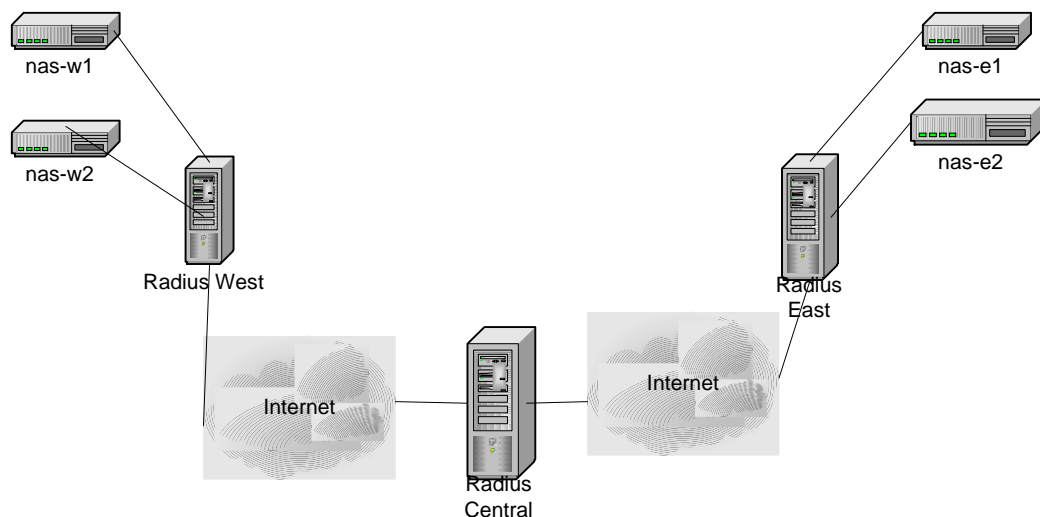
The EXT_USER structure in the Auth API includes a field for specifying the type of mapping that should be done. The available types are:

- 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, so does the need to store and forward accounting data among RADIUS proxies.

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 request was received:



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.

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, click the save button from within the RadiusNT/X administrator or you can use the *reload* user entry with Radlogin. This signals RadiusNT/X to reload the *users* file without restarting the service.

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}teH0wLlpW0gyQ). 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/odbc>

- *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.

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/cgi-bin/search/search.pl?searchPhrase=configuring+radius>

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. <div><div><div>1 Login</div><div>2 Framed</div><div>3 Callback Login</div></div><div><div>4 Callback Framed</div><div>5 Outbound</div><div>6 Administrative</div></div><div><div>7 NAS Prompt</div><div>8 Authenticate Only</div><div>9 Callback NAS Prompt</div></div></div>

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

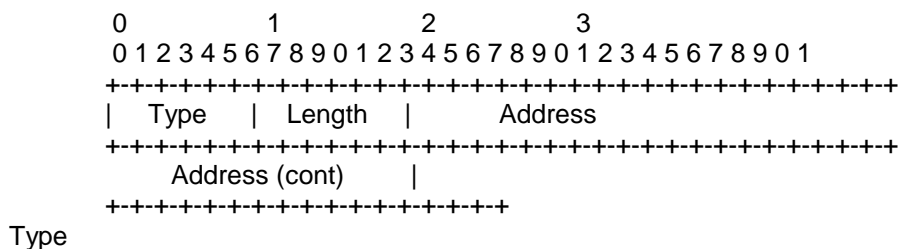
The Value field is four octets.

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

5.8. Framed-IP-Address

This attribute indicates the address to be 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.

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



8 for Framed-IP-Address.

Length

6

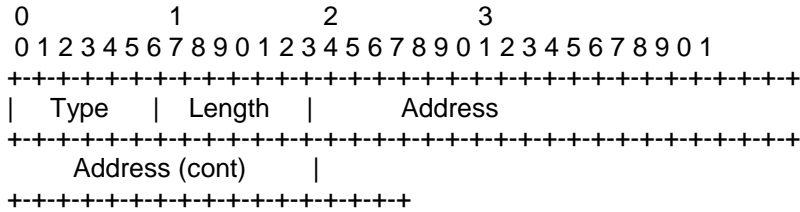
Address

The Address field is four octets. The value 0xFFFFFFFF indicates that the NAS should allow the user to select an address (e.g. Negotiated). The value 0xFFFFFFF0 indicates that the NAS should select an address for the user (e.g. Assigned from a pool of addresses kept by the NAS). Other valid values indicate that the NAS should use that value as the user's IP address.

5.9. Framed-IP-Netmask

This attribute indicates the IP netmask to be configured for the user when the user is a router to a network. 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 netmask, but the server is not required to honor the hint.

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



Type

9 for Framed-IP-Netmask.

Length

6

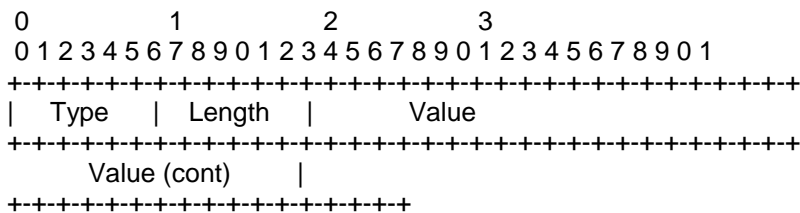
Address

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.

```

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

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.

```

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

12 for Framed-MTU.

Length

6

Value

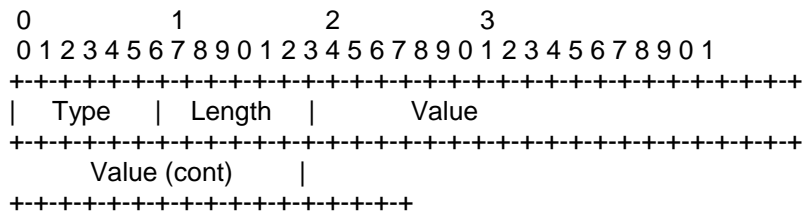
The Value field is four octets. Despite the size of the field, values range from 64 to 65535.

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.

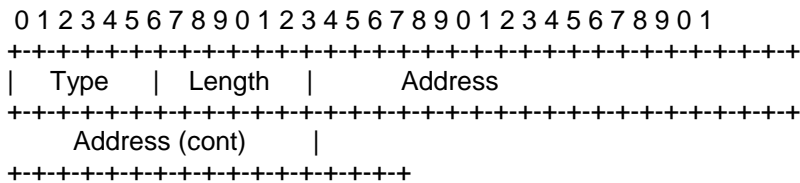
- 0 None
- 1 VJ TCP/IP header compression [5]
- 2 IPX header compression

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

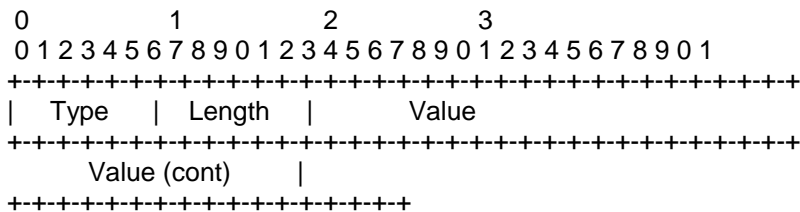
Address

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

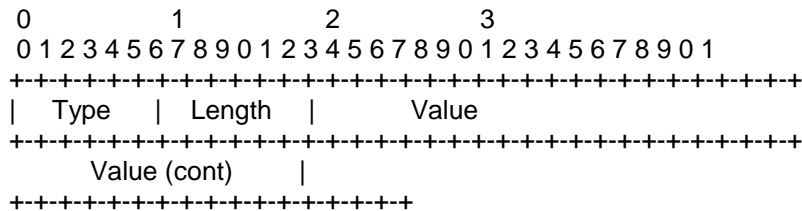
The Value field is four octets.

- 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.

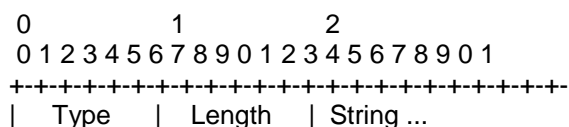
When used in an Access-Accept, it is the success message.

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

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.

```

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

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.

```

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

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

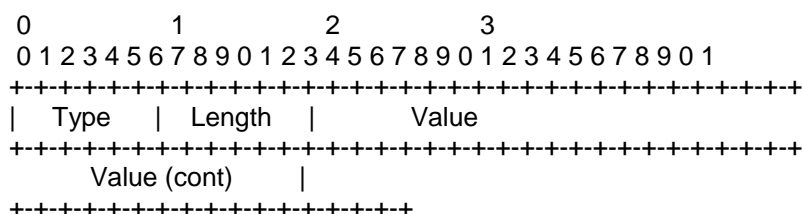
followed by a space, a gateway address in dotted quad form, a space, and one or more metrics separated by spaces. For example, "192.168.1.0/24 192.168.1.1 1 2 -1 3 400". The length specifier may be omitted in which case it should default to 8 bits for class A prefixes, 16 bits for class B prefixes, and 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 0xFFFFFFFF 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.

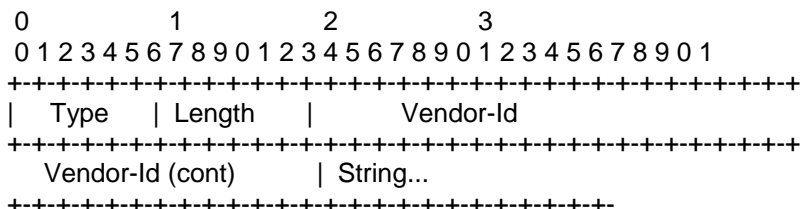
The codification of the range of allowed usage of this field is outside the scope of this specification.

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

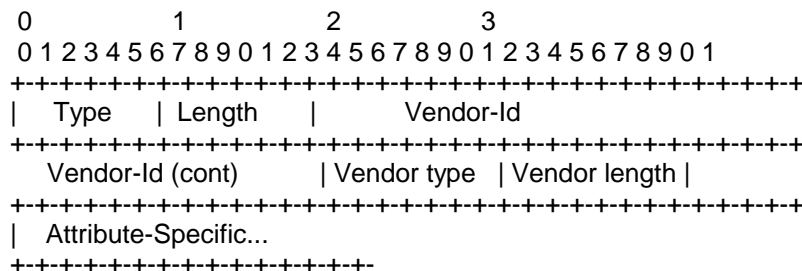
The high-order octet is 0 and the low-order 3 octets are the SMI Network Management Private Enterprise Code of the Vendor in network byte order, as defined in the Assigned Numbers RFC [3].

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.

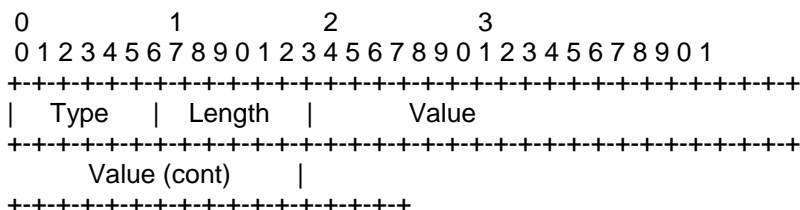
It **SHOULD** be encoded as a sequence of vendor type / vendor length/value fields, as follows. The Attribute-Specific field is dependent on the vendor's definition of that attribute. An example encoding of the Vendor-Specific attribute using this method follows:



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

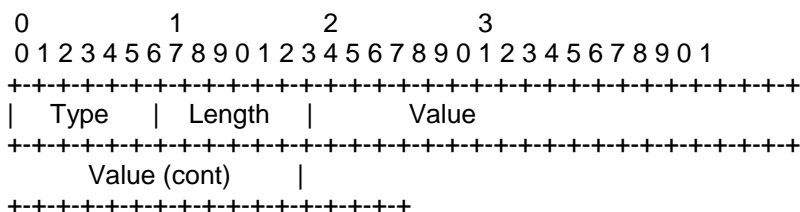
Value

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.



Type

28 for Idle-Timeout.

Length

6

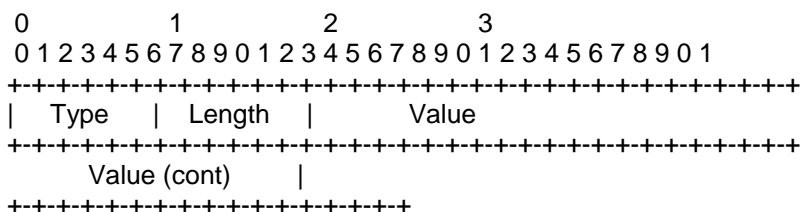
Value

The field is 4 octets, containing a 32-bit unsigned integer with the maximum number of consecutive seconds of idle time this user should be permitted before being disconnected by the NAS.

5.29. Termination-Action

This attribute indicates what action the NAS should take when the specified service is completed. It is only used in Access-Accept packets.

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



Type

29 for Termination-Action.

Length

6

Value

The Value field is four octets.

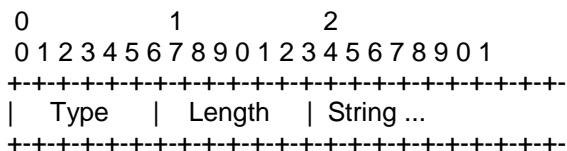
- 0 Default
- 1 RADIUS-Request

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.



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.

```

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

36 for Login-LAT-Group.

Length

34

String

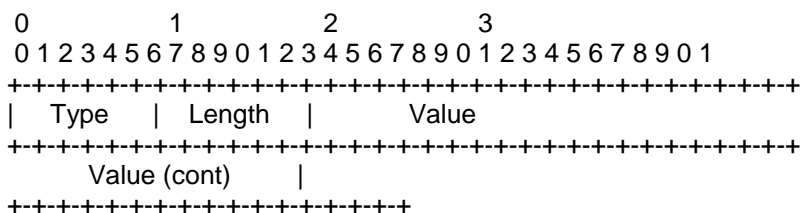
The String field is a 32 octet bit map, most significant octet first. A robust implementation SHOULD support the field as undistinguished octets.

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.



Type

37 for Framed-AppleTalk-Link.

Length

6

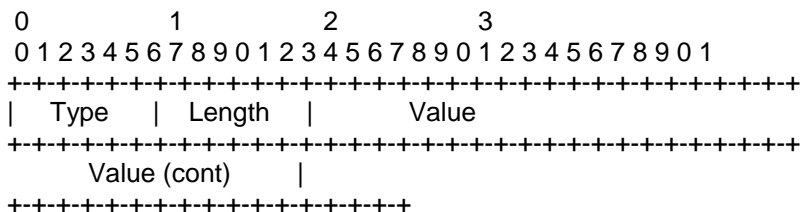
Value

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.



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.

```

      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 4
      +---+---+---+---+---+---+---+---+---+---+---+---+---+---+
      | Type   | Length | String ...
      +---+---+---+---+---+---+---+---+---+---+---+---+---+---+
```

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.

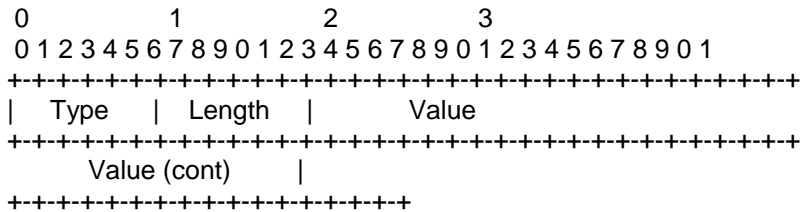
Below, you will find information from the RADIUS RFC 2139.

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.

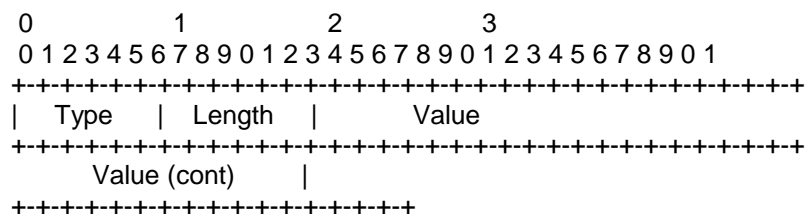
- 1 Start
- 2 Stop
- 7 Accounting-On
- 8 Accounting-Off

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.

```

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

46 for Acct-Session-Time.

Length

6

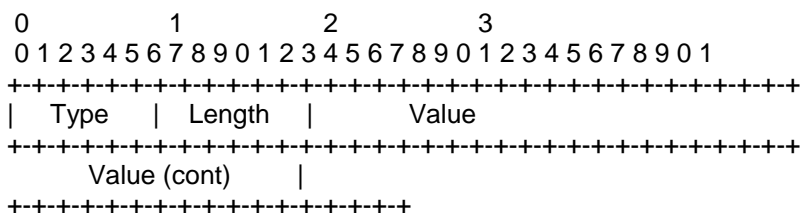
Value

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.



Type

47 for Acct-Input-Packets.

Length

6

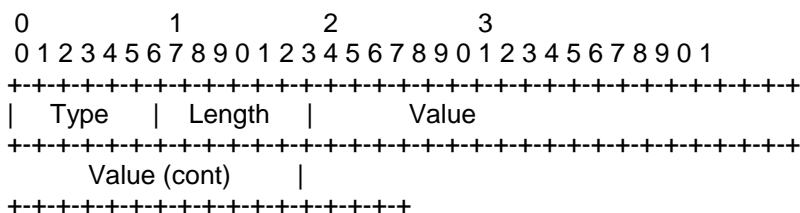
Value

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.



Type

48 for Acct-Output-Packets.

Length

6

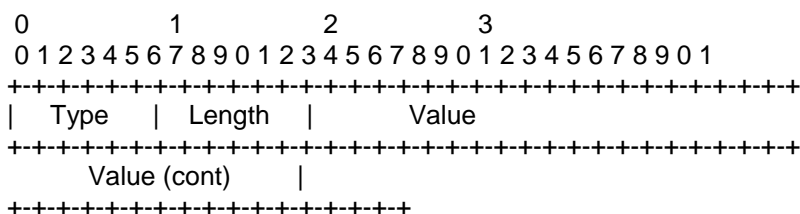
Value

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.

```

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

60 for CHAP-Challenge.

Length

>= 7

String

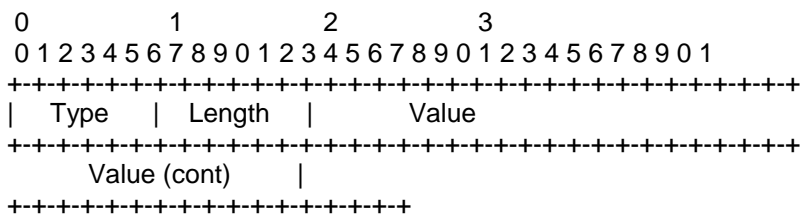
The String field contains the CHAP Challenge.

5.41. NAS-Port-Type

This attribute indicates the type of the physical port of the NAS which is authenticating the user. It can be used instead of, or in addition to, the NAS-Port (5) attribute. It is only used in Access-Request packets.

Either NAS-Port (5) or NAS-Port-Type or both SHOULD be present in an Access-Request packet, if the NAS differentiates among its ports.

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



Type

61 for NAS-Port-Type.

Length

6

Value

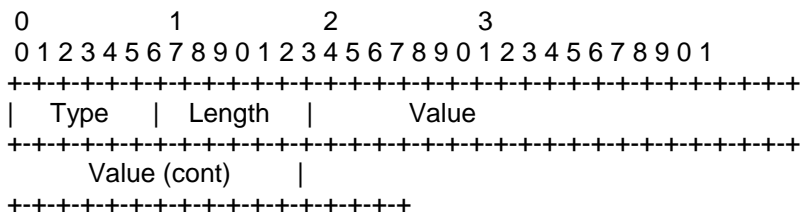
The Value field is four octets. "Virtual" refers to a connection to the NAS via some transport protocol, instead of through a physical port. For example, if a user telnetted into a NAS to authenticate himself as an Outbound-User, the Access-Request might include NAS-Port-Type = Virtual as a hint to the RADIUS server that the user was not on a physical port.

- 0 Async
- 1 Sync
- 2 ISDN Sync
- 3 ISDN Async V.120
- 4 ISDN Async V.110
- 5 Virtual

5.42. Port-Limit

This attribute sets the maximum number of ports to be provided to the user by the NAS. This attribute MAY be sent by the server to the client in an Access-Accept packet. It is intended for use in conjunction with Multilink PPP [7] or similar uses. It MAY also be sent by the NAS to the server as a hint indicating how many ports are desired for use, but the server is not required to honor the hint.

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



Type

62 for Port-Limit.

Length

6

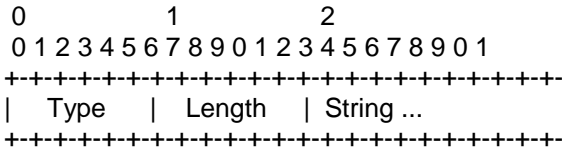
Value

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 which attributes may be found in which kinds of packets, and in what quantity:

RFC 2138 - RADIUS Authentication

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.

Configuring ODBC

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.

RadiusNT/X's ODBC layout is based on the database layout of Emerald, the Internet Management Suite.

To configure an ODBC DSN for RadiusNT/X, follow the steps in [Chapter 1 – ODBC Settings](#).

To finish the test, you will also need to create a Master Billing Record (MBR) with associated Service within the Emerald client.

For all others, please use the database interface to add entries to the Servers table. These should reflect the information you would have entered in the *Clients* file for text mode. The three fields that are required are **Name**, **IP Address**, and **Secret**; all other fields are informational only. For the Calls Online feature to function properly, you will also need to populate the ServersPorts table.

Next, start RadiusNT/X. You do this by accessing a DOS Command Prompt and then changing to the directory where RadiusNT/X is installed. Execute the following command to start RadiusNT/X in full debug mode:

```
radius -x15 (Windows)
./radiusd -x15 (UNIX)
```

If everything is configured correctly, a "waiting for requests" line will be returned. At this point you can minimize the window and continue on to the Terminal Server Configuration section. RadiusNT will return an error message if something is not configured correctly. If this occurs, please go back and check the directions again, carefully.

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. It **must** be pointed to the Emerald database you created.
3. Specified correct login information in the RadiusNT Administrator to allow RadiusNT to log in to the SQL Server.

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 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, then append the information to the detail file for that NAS.

If you do **not** want duplicate accounting, and only want the two authentication choices, you may specify an accounting directory that does not exist. RadiusNT 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.

Tables

Please note the following information pertains only to Emerald installations.

Accounting Manual Calls Update	RadiusNT/X will manually update the ServerPorts table. This is only needed for databases that do not have trigger support . The option is not needed with Emerald/SQL Server or an active database that can update the Calls Online view automatically.
Manual Service Update	In order for Time Banking to work, RadiusNT/X will manually update the user's time left information. This option is not needed with Emerald or an active database that can update the Subaccounts table automatically.

Master Accounts Table	*OverLimit	Money	If the Balance field is less than this field, the account will not 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.

Emerald Integration FAQs

- *When using RadiusNT/X with Emerald, what license and database information do I use?*

When using RadiusNT/X in conjunction with Emerald, there is no need to configure a license or database settings if Emerald has already been installed and configured on the system you will be using RadiusNT/X with. Otherwise you will need to configure an ODBC datasource in the RadiusNT administrator.

Note: If the version of Emerald is does not ship with RadiusNT/X you will need to install a separate RadiusNT/X license in the RadiusNT/X administrator. For example using Radius v5 with Emerald v4 requires a RadiusNT/X v5 license.

- *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.

See the SQL script callsdb_ms.sql located in your Emerald SQL folder for more information.

Glossary

Term	Definition
8	
802.1x	Standard for wireless authentication and encryption with EAP
A	
AAA	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.
Accounting	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
Application Program (or Programming) Interface (API)	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.
Attribute	Defined parameters used to identify a user or to configure a user's call session.
Authentication	A method of identifying a caller before accepting a call.
B	
Basic Rate Interface (BRI)	An ISDN interface that consists of two 64Kbps B channels (for voice and/or data) and one 16Kbps D channel (for signaling).
C	
Challenge-Handshake Authentication Protocol (CHAP)	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.
Client	A software program that is used to contact and obtain data from a Server software program on another computer.
Clients File	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.
D	
Dialed Number Identification Service (DNIS)	The DNIS shows the phone number the user dialed in order to access the telephony system.
Digital Subscriber Line (DSL)	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.
Domain Name Services (DNS)	A method of administering domain names to correlate to IP addresses, and vice versa, in a consistent and concise manner.

E	
Extensible Authentication Protocol (EAP)	A generic protocol that enables end clients to speak to the authentication server for the purpose of negotiating an authentication protocol and performing authentication.
F	
Firewall	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.
Frequently Asked Questions (FAQs)	FAQs are documents that list and answer the most common questions on a particular subject.
File Transfer Protocol (FTP)	A very common method of moving files between two systems.
H	
Host	Any computer on a network that is a repository for services available to other computers on the network.
I	
Internet Engineering Task Force (IETF)	An group of international network designers, operators, vendors and researchers who work together to develop new Internet standards and specifications.
Intranet	A private network ,inside a company or organization, that uses Internet services and protocols for internal use.
IP Address	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.
IP	Internet Protocol - An addressing standard used on TCP/IP networks.
Integrated Services Digital Network (ISDN)	A way to move more data over existing regular phone lines at speeds of roughly 128,000 bits-per-second.
L	
Login	Noun: The account name used to gain access to a computer system. Verb: (Log In) The act of entering into a computer system.
M	
Maximum Transmission Unit (MTU)	The largest frame or packet that can be sent through a segment of an IP network without fragmentation.
Microsoft Challenge-Handshake authentication protocol	A CHAP protocol compatible with password encryption used in most Microsoft operating systems.
N	
Name Server	A server that resolves host names into network addresses.
Network Access Server(s) (NAS)	A server dedicated to authenticating users that log on.
Network	Two or more computers connected so that they can share resources. If you connect 2 or more networks, you have an internet.
O	
Open DataBase Connectivity (ODBC)	An interface used by Windows application programs to gain access to databases.
P	
Port	A number assigned to an application running in a server. The number is used to link the incoming data to the correct service.
Practical Extraction and Report Language (Perl)	An interpreted language developed by Larry Wall that is freely distributed on the Internet. It includes object-oriented programming

	facilities.
Protocols	Formal sets of communication rules and standards.
Protected-EAP (PEAP)	A secure EAP channel established between the end client and authentication server.
R	
Relational DataBase Management System (RDBMS)	A database organization method that links files as required. The software controls the organization, storage, retrieval, security and integrity of data in a database.
Request For Comments (RFC)	The name of the result and the process for creating a standard on the Internet.
Roaming	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.
Router	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.
S	
Secret	A code used to gain access to a locked system. Also known as a password.
Server	A computer or a software package that provides a specific kind of service to client software running on other computers.
Shared Secret	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.
SNMP	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 http://www.ietf.org/ .
Structured Query Language (SQL)	A specialized programming language for sending queries to databases.
T	
Transmission Control Protocol (TCP)	The standard that is responsible for reliable end-to-end communications for transmitting datagrams across Internet networks.
Trigger	An SQL procedure that is executed when a record is added, updated or deleted. It is used to maintain referential integrity in the database. A trigger may also execute a stored procedure.
U	
User	A person who dials into a NAS for negotiation.
Users File	A text file that contains authentication and authorization information in the form of attributes and values for each user who connects to the network.
User Datagram Protocol (UDP)	The standard that is responsible for unreliable end-to-end communications for transmitting data across IP networks.