RadiusNT & RadiusX

The Ultimate RADIUS Servers

For Windows NT, Linux, Solaris & Cobalt Appliances

Version 3.0

IEA Software, Inc.

Administrative and Support Office
516 W. Riverside, Suite 201
Spokane, WA 99201
(509) 444-BILL
(509) 755-0705 fax

Sales Office
Santa Cruz, CA
(831) 459-9430
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 load, rent, lease or sublicense the Software or any copy to others for any purpose. RadiusNT or RadiusX may only be installed on a single WindowsNT, Solaris, Linux or Cobalt Networks workstation or server. Additional servers may be purchased separately. You agree to use reasonable efforts to protect the Software from unauthorized use, modifications, reproduction, distribution and publication. You are not permitted to make any uses or copies of the Software that are not specifically authorized by the terms of this License Agreement. Your adherence to this License Agreement will allow IEA Software, Inc. to continue developing innovative and useful products and providing a high level of customer service and support. If you do not comply with the terms of this License Agreement, your license will be revoked.

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

Trademarks IEA Software, Inc., Emerald, RadiusNT, RadiusX and the associated logo(s) are registered trademarks. All images, photographs, animations, audio, video and text incorporated into the Software is owned by IEA Software, Inc., unless otherwise noted by Trademark.

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

Miscellaneous This License Agreement shall be construed, interpreted and governed by the laws of the State of Washington. Should any term of this License Agreement be declared void or unenforceable by any court of competent jurisdiction, enforcement of the remaining terms shall not be affected. Failure of either party to enforce any rights or to take action against the other party in the

event of any breach of this Licensing Agreement shall not be deemed a waiver of any subsequent enforcement of rights.

Limitations of Liability and Remedies In no event shall IEA Software, Inc. or its licensors be liable for any loss of profit or any other commercial damage, including but not limited to special, incidental, consequential or other damage, even if IEA Software, Inc. or its licensors are advised, in advance, or the possibility of such damages. IEA Software, Inc. and its licenser'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, the accompanying material. This Limited Warranty is void if failure of the Software has resulted from accident, abuse or misapplication. You may have other specific legal rights, which vary from state/jurisdiction to state/jurisdiction.

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

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

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

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

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

Trademarks

Emerald Management Suite, RadiusNT and *RadiusX* are trademarks of IEA Software, Inc.
Alpha AXP is a registered trademark of Digital Equipment Corporation. *Intel* is a registered trademark of Intel Corporation. *Transact-SQL* is a registered trademark and *DB-Library* is a trademark of Sybase, Inc.

Table Of Contents

Welcome

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

Preface

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

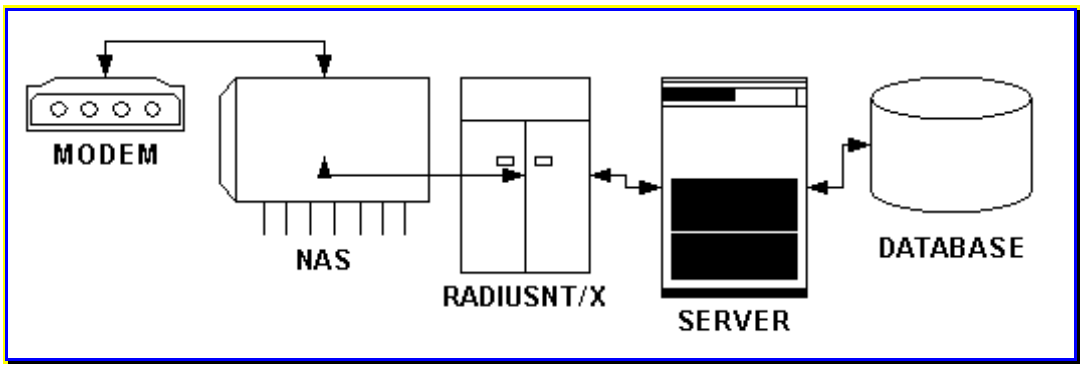
This document is not intended to delve into the technical aspects of RADIUS. You will find that technical reference materials exist in a variety of places. For RFC information, please check out the World Wide Web. A good starting point is the Internet Engineering Task Force (IETF) Web site at http://www.ietf.org.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

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

About RADIUS

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

The basic RADIUS design allows for a client such as a NAS or firewall to contact the RadiusNT/X server and send a message requesting authentication of a user who has requested access to a network. In response, RadiusNT/X searches its *clients* file for an entry that matches the request. If a match is found, RadiusNT/X searches the *users* file for a profile that matches the criteria (commonly a username and password). The server processes the request and replies back 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 have very similar characteristics to most UNIX RADIUS servers, including basic authentication and accounting capabilities. RadiusNT/X stand out among RADIUS servers though by providing a multitude of powerful features and enhanced options. The most striking features 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 other additional rules as configured by the RadiusNT/X Administrators.

RadiusNT and RadiusX Editions

There are two stand-alone editions of RadiusNT and RadiusX, Standard and Professional. In addition, RadiusNT/X works with version 2.5+ editions of the Emerald Management Suite. RadiusNT/X Professional includes advanced features that the Standard version does not include such as cache and proxy (see below). In addition, 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 lie in:

- 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 has a different Administrator
- RadiusX uses system password functions in place of a password file.
- RadiusX does not support NT Authentication
- RadiusX datasources are defined in the *odbc.ini* file versus the Windows ODBC Administrator

Differences are noted throughout the documentation. In addition, features and options available in only the Professional versions of the software are clearly noted. The following chart shows the options that are only available in the Professional editions. For more detailed information on each option, please see the Professional Features chapter.

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
Dual Mode Authentication	To authenticate based on an expiration date or a balance/limit combination
Unlimited Smart Cache	Unlimited number of smart cache entries for scaling
Advanced State Management	Store and recover authentication and accounting information

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, but rather just the text within the quotation marks.

System Requirements

RadiusNT runs on any Windows NT 4.0 and Windows 2000 workstation or server. It is administered from Windows NT either remotely or locally.

For RadiusNT, please use:

- Windows NT 4.0
- Service Pack 3 or higher
- 32MB of RAM or greater
- Pentium 100 or greater

RadiusX can also be administered remotely or locally.

For RadiusX, please use:

- Solaris 2.6 or higher, RedHat Linux 6.0 or higher
- 64MB of Ram or greater
- >30MB Disk space
- Perl 5.0 or higher

Both run with the below listed SQL databases. You need to have a working knowledge of your database. For the database, please use the following guidelines:

- Microsoft SQL Server 6.5 with SP3 or higher
- Microsoft SQL Server 7.0
- Sybase SQL Server 11.0 or higher
- Oracle Server 8.0 or higher
- Microsoft Access 7.0 or higher

Note: When using a database with the Linux version of RadiusX, Windows NT is required. Please use:

- Windows NT 4.0
- Service Pack 5 or higher
- 128MB of RAM
- Pentium 100 or greater

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

RadiusX for Cobalt runs on the Cobalt Qube2, RaQ2and RaQ3 systems. It is administered either remotely or locally.

Please use the following as a guideline for your system requirements.

- 64MB of RAM or greater
- 30MB of disk space
- Perl 5.0 or greater

RadiusX for Cobalt can authenticate against a password file, users file, or an ODBC database, please use the following guidelines:

- Microsoft SQL Server 6.5 with Service Pack 5 or higher
- Microsoft SQL Server 7.0
- Sybase SQL Server 11.0 or higher
- Oracle Server 8.0 or higher

Note: When using a database with RadiusX for Cobalt, Windows NT is required.

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 pertinent 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 (FAQs) and more.

- IEA Software hosts mailing lists for RadiusNT/X. These are user-supported lists and are a great resource for conversing with others who own the products. You can learn more about the mailing lists at http://www.iea-software.com/support/maillists/liststart. We host a searchable archive of the lists on our Web site as well.

- If you still require assistance, we have a variety of support contract options available via our Web site at http://www.iea-software.com/support.

Chapter 1 – INSTALLATION

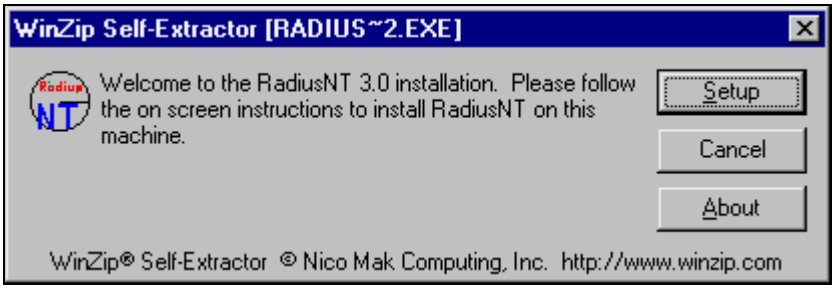
This chapter contains information on how to install and configure your RadiusNT and RadiusX servers. The instructions include information on configuration options that will differ depending on your organization's needs. Please read the ***readme.txt*** and ***changes.txt*** files included with your distribution for additional 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.

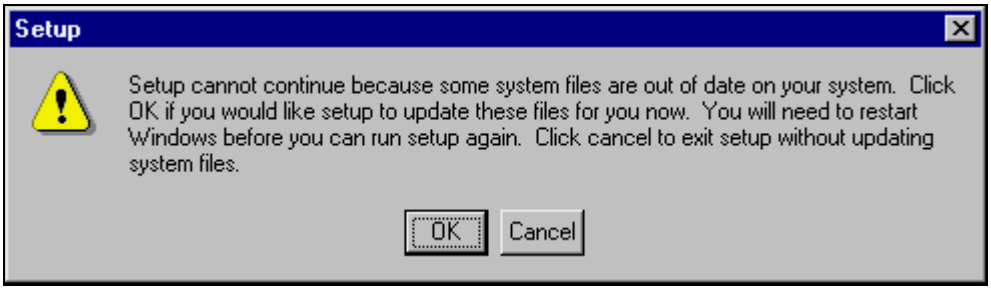
Installing RadiusNT

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 *RadiusNT3.exe* file and then click **OK** to begin the installation process. *RadiusNT3.exe* is a zipped executable file.
6. Click **Setup**.



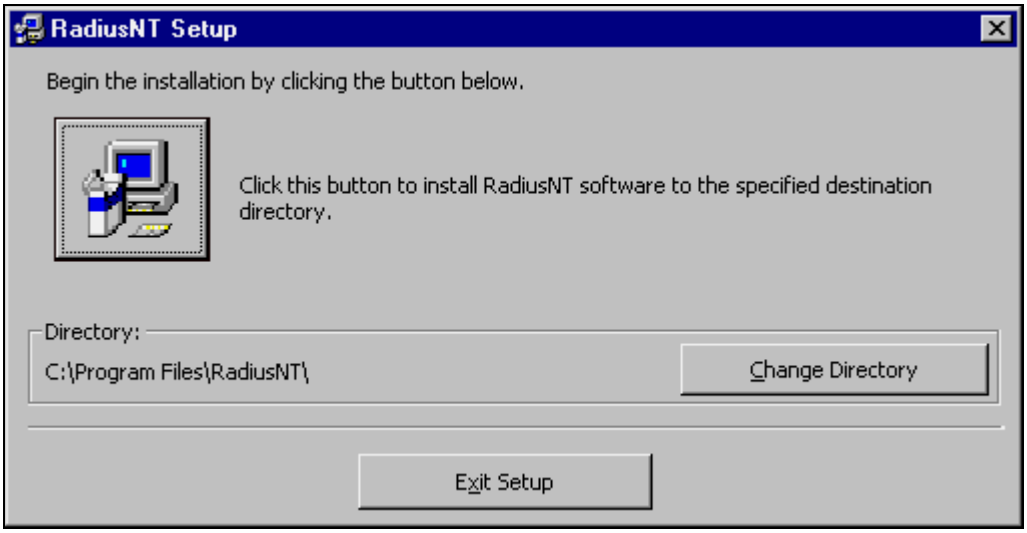
Please note that if some of your system files are out of date, RadiusNT will update the files and require you to restart Windows NT in order to proceed.



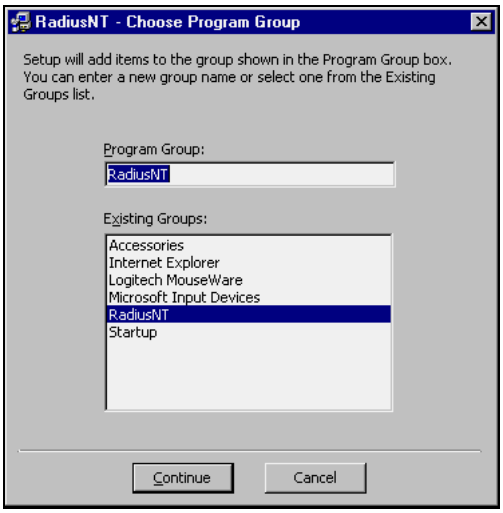
7. You will see the Welcome screen. Click **OK** to proceed.

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.



10. The installation program will check for necessary disk space and will then ask you to choose a Program Group to add items to. Accept the **RadiusNT** group and click **Continue**.



11. When the installation is successfully completed, you will receive a final confirmation screen. Click **OK** to finish.

Once the Setup program has finished, you can configure RadiusNT for your operating environment via the RadiusNT Administrator. Please note that in order 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.

Upgrading From an Earlier Version of RadiusNT

Before you upgrade to a newer version of RadiusNT/X, make sure you **backup** 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 new 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 Microsoft Access, the databases are compatible and no changes need to be made.

The RadiusNT 3.0 database schema includes several database changes that either add new functionality or correct previous issues.

If your currently using RadiusNT 2.5 /w SQL Server (**not emerald**) run rad25_up.sql to upgrade your database to Radius 3.0

If running Emerald 2.5 you should run emer25_up.sql to upgrade the Emerald database to be compatible with Radius 3.0. See Appendix B.

Both rad25_up.sql and emer25_up.sql are fully backwards compatible with Radius 2.5.

SQL Server

- Several stored procedures have been added for use during authentication and other areas to replace queries that RadiusNT manually built and executed. This allows for increased flexibility and adaptation when running against SQL Server. Please reference the SQL database section for a full list of the stored procedures.

Installing RadiusX for Cobalt (Raq2 & Raq3)

Please read the readme.txt and changes.txt files that came with your distribution for updated information.

General info:

To configure your odbc datasources run ./odbc_setup from the /usr/local/radius directory.

To configure the RadiusX server goto http://mycobaltserver/~admin/radius. Use your administrator login and password when prompted.

To run RadiusX execute /usr/local/radius/radiusd –x15

Details:

After you have downloaded the RadiusX for Cobalt distribution, please do the following to install RadiusX on your Cobalt appliance.

1. From the Cobalt server admin interface. Select 'Maintenance'. Next select the 'Install Software' option. Upload your RadiusX for Raq2 or Raq3 package (.pkg) file.

   RadiusX for Cobalt will be installed in the */usr/local/radius* directory. Please proceed to the RadiusNT/X documentation to continue your installation.

Please note that if you would like to configure RadiusX for Cobalt to connect to a remote database, you will need to follow the steps below.

1. Begin by creating a new database by running one of the install scripts located in the */usr/local/radius* directory from your database management software. Or, if you have an existing RadiusNT or Emerald database, locate it.

   Below is a list of install scripts and descriptions.

   rad25_up.sql - This script will upgrade an existing Microsoft SQL Server RadiusNT 2.5 database to a 3.0 database.

   emer25_up.sql – This script upgrades an exsiting Microsoft SQL Server Emerald 2.5 database to be compatible with Radius 3.0.

   radius.sql - This script is used to create a Radius v3 database for Microsoft SQL Server v6.5 and 7.0.

   rdius_sybase.sql - This script is used to create a Radius v3 database for Sybase Server v11.

   radius_oracle.sql - This script is used to create a Radius v3 database for Oracle version 8.

2. Next, create an ODBC Datasource called 'Emerald' on your Windows NT system, which points to the RadiusX for Cobalt database. **(Note: you can use a name other than Emerald, but the name you use must be consistent throughout.)**

3. **Raq2 users only**: Install the OpenRDA request server on your Windows NT system by running *odbcsrvr.exe*.

   - During the setup process, go to the 'Server Configuration' menu and enter 'Emerald' in the name field while leaving the other settings at their default values. Click Next.
   - In the 'Custom Database Info' menu, enter "Emerald" as your ODBC datasource. Click Next.
   - In the 'License Information' menu, enter "1960540" as the Server key and "01092321071" as the Client key. Click next.
   - Start the OpenRDA server via the Start Menu - Programs/OpenRDA/OpenRDA Server.

- ❖ Next, you will need to configure a Cobalt datasource. Begin by running *./odbc_setup* from the */usr/local/radius* directory on your Cobalt system. Edit an existing entry for 'Emerald', then modify the 'Address' option with the IPAddress of your OpenRDA server configured above.

4. **Raq3 users only**: Install the Sequlink request broker on your Windows NT or other compatible platform located on the IEA Software FTP site ftp://ftp.iea-software.com/RadiusX/Linux/sequlink. See the readme.txt file in this directory for further information on which files to download.

5. Now you will need to configure RadiusX for ODBC mode. Begin by running the RadiusX Administrator. Select 'General' / 'Database Mode' / select the ODBC option.

6. Next you'll need to specify a datasource and login information to your database. Select 'Authentication'. Enter your Authentication Datasource, database login and database password.

7. Finally, run RadiusX in debug mode from the */usr/local/radius* directory using *./radiusd -x15.*

Please refer to this documentation for further information regarding RadiusX.

Installing RadiusX for Solaris & Linux

Please follow the instructions below to install RadiusX for Solaris and Linux. Linux and Solaris specific steps will be labeled (**Solaris**) or (**Linux**) respectively.

1. Download the distribution archive for the Solaris or Linux RadiusX edition 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 rights 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**.

Next, un-tar the distribution (***radiusx3_solaris.tar.gz*** or ***radiusx3_linux.tar.gz***) into a temporary directory. Use the "**cd**" command to change to the directory where the files were expanded. This can be done by typing the following commands:

```
gzip –d radiusx_xxxxx.tar.gz
tar –xf radiusx_xxxxx.tar
```

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 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.sql*
- For a Sybase database, use radius_*sybase.sql*
- For a Oracle database, use radius_oracle.sql

Please refer to your database documentation to learn how to run the script. For MS SQL you can use the Enterprise Manager and for Sybase you can use the SQL Server Manager. You can also use the ISQL application.

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

Linux Installation

1. Run the Install application by typing "perl install.pl". This will install RadiusX to the /usr/local/radius directory. A log of this installation can be found in the file install.log.

Configuring database connections

Install the Sequlink request broker on your Windows NT or other compatible platform located on the IEA Software FTP site ftp://ftp.iea-software.com/RadiusX/Linux/sequlink. See the readme.txt file in this directory for further information on which files to download.

During the sequlink server installation if you are prompted for a serial number enter any number and continue with the install. It is safe to ignore any 30 day evaluation warnings. They do not apply.

run ./odbc_setup from the /usr/local/radius directory.

```
SequeLink Connect Administration Tool on Linux
(c)Copyright 1995-1998 INTERSOLV, Inc., All rights reserved


The following Data Source is selected : .
[1] Select a Data Source
[2] New
[7] About
[0] Cancel
```

2. Select an action [0]: ▌

Select 'New' data source and answer the following questions. Make sure the sequlink server you installed previously is running then select your newly created datasource and test it.

Now run the RadiusX Administrator by typing perl ./radadmn.pl from the /usr/local/radius directory.

Select 'Configuration' / 'Database Mode' – enable ODBC Mode.

Next, from the main menu select 'ODBC DSN' – Authentication Datasource. In this field enter the name of the data source you previously created from the ./odbc_setup program.

Next enter your database login and password by configuring the 'Auth Database Login' and 'Auth Database Password' options.

Exit the administrator and run ./radiusd –f to test your database connection. Radius returns Datasourcename = OK.

Solaris Installation

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

```
Welcome to IEA Software, Inc.  RadiusX v3.0 Installer.

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

1.   [Do not Install]      Microsoft SQL Server 6.5 & Sybase 11 ODBC
2.   [Do not Install]      Install Oracle 7 ODBC Drivers
3.   [Do not Install]      Oracle 8 ODBC Drivers

: 
```

2. You will be presented with three options. Select the component you want from the install list by typing the corresponding number (ex: 1 for Microsoft SQL Server 6.5 ODBC & Sybase 11 ODBC drivers). Once you have selected an option, you will note that the indicator changes from '**Do not Install**', to '**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. After you have selected the option(s) you want to install, continue to step 8.

3. Type "**C**" to continue, or "**Q**" to abort the install process.

4. Next, you will be prompted to enter your database server **network address**, **port number** (ex: the port that is used to communicate between RadiusX and the SQL or Sybase server**)**, **database login**, **database name** and **database password**. You will also need to confirm your password to ensure that it is correct. An example is shown below. Press the **Return** key when you have completed entering the needed information. You will be returned to the command prompt.

```
Welcome to IEA Software, Inc.  RadiusX v3.0 Installer.

The following questions set default values in:
ODBC configuration file (/usr/local/radius/odbc.ini)
RadiusX configuration file (/usr/local/radius/radiusd.ini)
These settings can be changed later by editing odbc.ini or
running radadmn.pl located in /usr/local/radius.

        SQL Server address (IP Address only for MSSQL/Sybase): 123.123.123.123
        Database Login: sa
        Database port number: 1433
        Database name: radiusx
        Database Password:      Confirm Password: 
```

Please note that the default values that you set are stored in the ODBC configuration file (*/usr/local/radius/odbc.ini*) and RadiusX configuration file (*/usr/local/radius/radiusd.ini*). These settings can be changed later by editing *odbc.ini* or running *radadmn.pl* located in /usr/local/radius.

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. In order 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

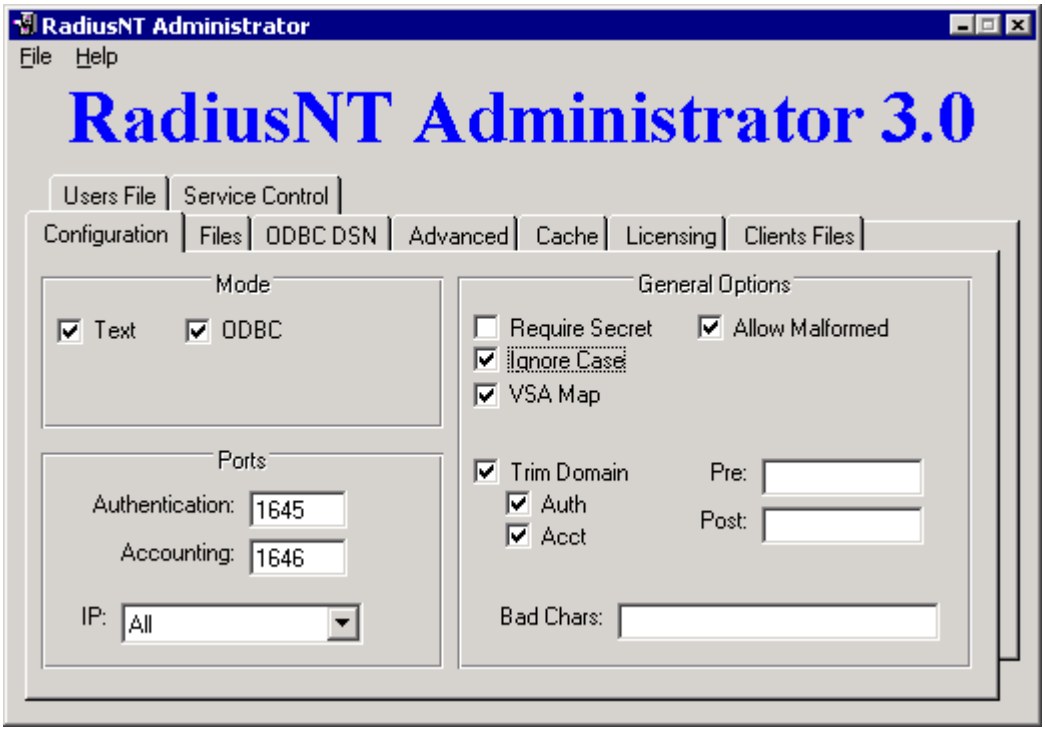
	items such as file permission errors or disk space.

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 Administrator (*radadmn.exe*) has nine different areas: Configuration, Directories, ODBC Security, Licensing, Service Control, cache, Clients and Users. To move between each area, click on the corresponding tab along the top of the Administrator window. You can use the Tab key and mouse to move between options. Please remember to fill out your **license information** on the Licensing tab in order for RadiusNT to function.



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 available in the RadiusNT and RadiusX Administrators in the Configuration section. Please note that some options are explained in finer detail in later sections

RadiusX Administrators

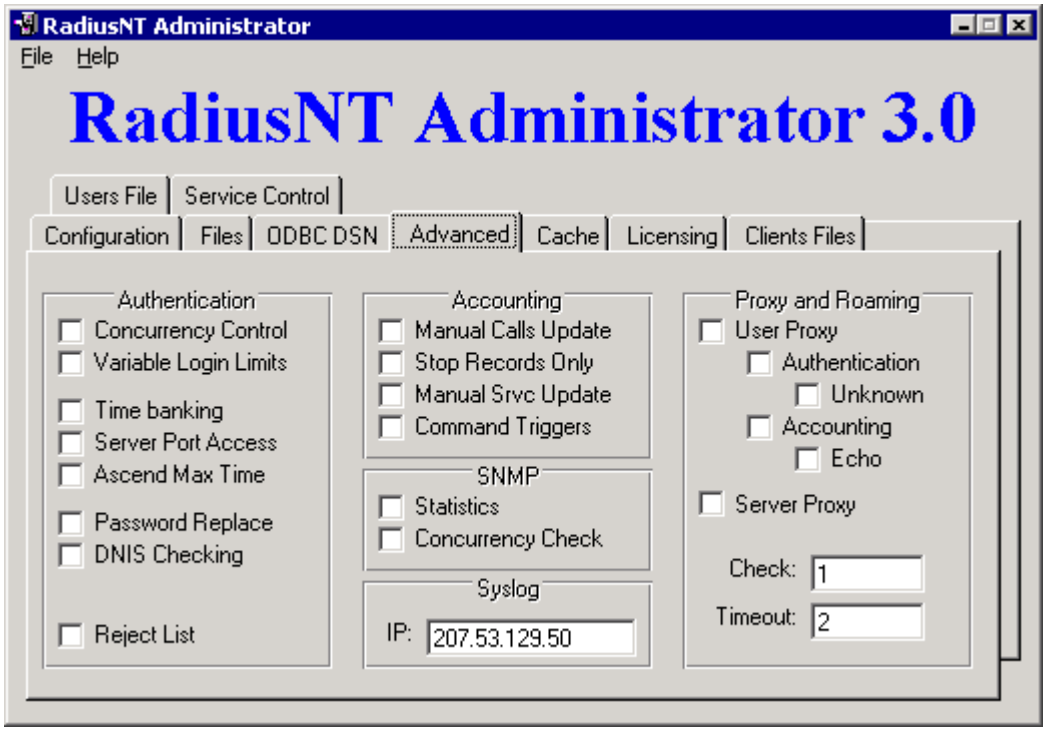
There are two RadiusX Administrators available to assist you in your configuration needs; a text-based Administrator and a Web-based Administrator. When you completed the RadiusX installation, the RadiusX text-based Administrator was automatically created in the /usr/local/radius directory. Please note that if you would rather use the RadiusX Web-based Administrator, **extra installation steps** need to be taken prior to usage. These instructions are listed below in the RadiusX Web-based Administrator section.

RadiusX Text-based Administrator

If you would like to use the text-based RadiusX Administrator, perform the following steps.

1. Begin by changing to the ***/usr/local/radius*** directory.
2. Run the RadiusX text-based Administrator by typing "**perl *radadmn.pl***".

The RadiusX text-based Administrator (*radadmn.pl*) has five different areas: Advanced, Cache, Configuration, Licensing and ODBC DSN. To move between each area, type the corresponding number in the administrative menu. **Please remember** to fill out your **license information** in the Licensing section in order for RadiusX to function. Also, note that the *users* and *clients* files **must** be edited **outside** of the Administrator with a simple text editor.



You will find brief explanations of each option available in the RadiusNT and RadiusX text-based Administrators in the Configuration section below. Some options are explained in finer detail in later sections. Please note that the RadiusX Web-based Administrator menu options are explained in a later section.

RadiusX Web-based Administrator

The RadiusX 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. Before you begin the installation, please make sure that you have:

- Perl 5 or higher installed
- A Web server (such as Apache) that supports CGI

You can now proceed with installing the Web-based RadiusX Administrator. (Note: This applies only to Solaris and Linux versions of RadiusX. The admin interface is automatically installed on the Cobalt Raq2 and Raq3)

1. Begin by creating ***/web*** and ***/cgi*** directories for the RadiusX web-based Administrator's .html files.

2. Change to the ***/webadmin*** directory.

3. Run the *webinstall.pl* Perl script by typing "**perl webinstall.pl**".

4. You will be prompted to identify the directories, which you created above.

   HTML directory to install Radius Admin web files:
   CGI directory to install Radius admin cgi files:
   HTML realitive path to the html directory (ex http.../radadmn):
   CGI realitive path to the cgi-bin directory (ex http.../cgi-bin):

5. Next, set the permissions you would like associated with the HTML and CGI files as well as program access. This step will vary depending on your Operating System(OS) and Web Server and will need to be set within the OS and Web Server.

Please note that the RadiusX web-based Administrator program (*radadmn.pl*), located in your specified */cgi* directory, **requires** read/write access to the radius configuration file (*/usr/local/radius/radiusd.ini*).

Quick Tip!	If you are running Apache or NCSA httpd, it is possible to password protect this program by creating an ***.htaccess*** file in your */cgi* directory. Please see your server's documentation for complete information.

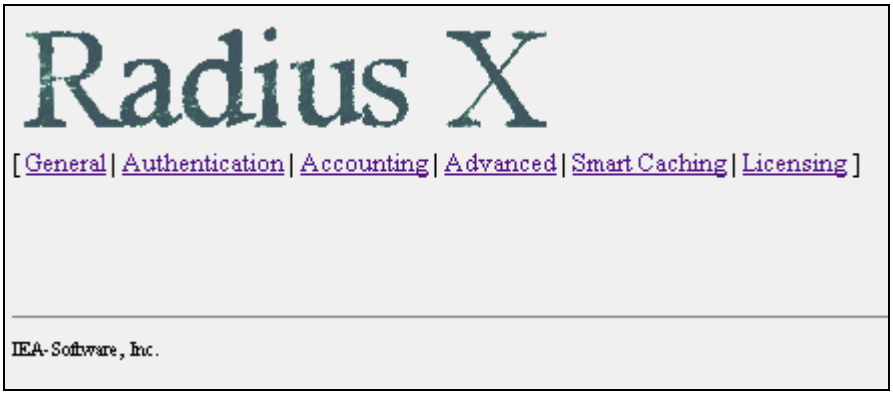
During the installation, a file named ***index.html*** was created in your specified **/html** install directory. To use the web-based RadiusX Administrator, perform the following step.

1. Open your preferred Web browser application.

2. Open the ***index.html*** file located in your specified /html install directory.

Please note that you **may** be required to login to the Web site if permissions were set accordingly.

The RadiusX Web-based Administrator (*index.html*) has six different areas: General, Authentication, Accounting, Advanced, Smart Caching and Licensing. To move between each area, simple click on the associated menu item. Please remember to fill out your **license information** on the Licensing section in order for RadiusX to function. Also, note that the *users* and *clients* files must be edited **outside** of the Administrator with a simple text editor. Please refer to the RadiusX Web-based Administrator configuration section below as it differs slightly from the RadiusNT and RadiusX text-based Administrator menu options.

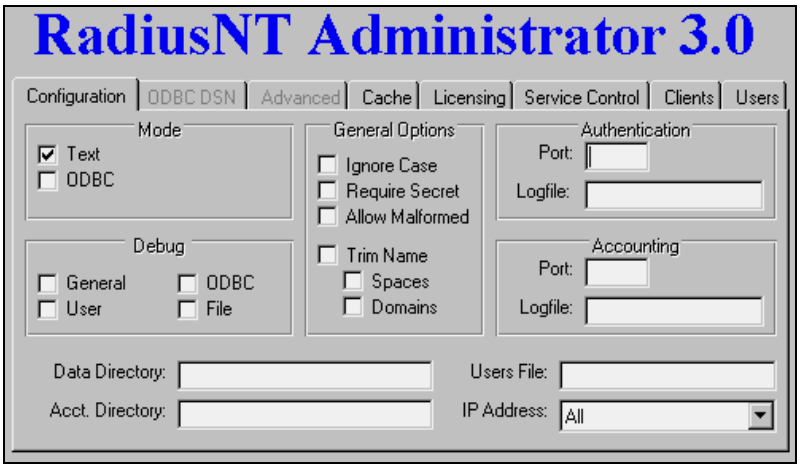


Configuration Options for RadiusNT GUI and RadiusX Text-based Administrators

The configuration of RadiusNT/X should be performed primarily through the RadiusNT/X Administrators. The tables below display detailed information about the options available. You will find brief explanations of each option available in the RadiusNT and RadiusX text-based Administrators here. Please note that some options are explained in finer detail in later sections. In addition, **please note that some menu options are different for the Web-based RadiusX Administrator.** Please refer to the RadiusX Web-based Administrator section for further information.

Configuration Menu Options

RadiusNT Administrator Configuration Menu



RadiusX Text-based Administrator Configuration Menu

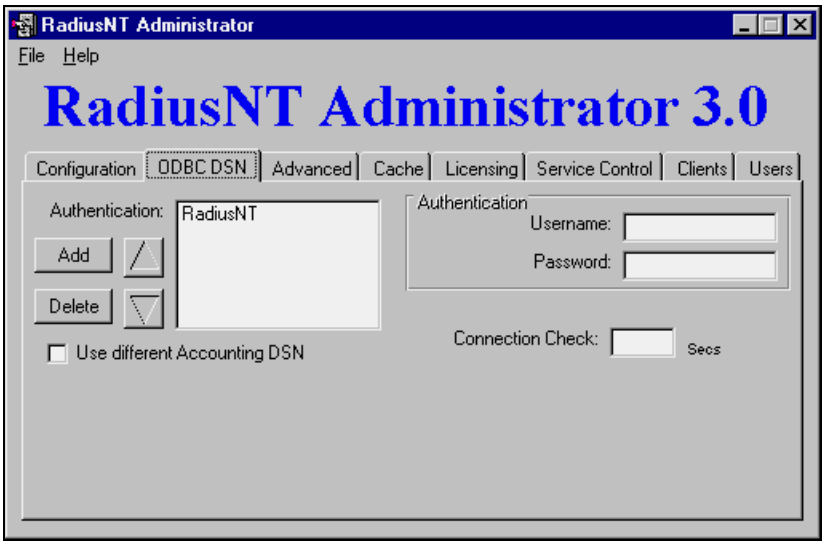
```
IEA Software, Inc.
RadiusX Administrator v1.0
--
Configuration
--
1.      Accounting
2.      Authentication
3.      General Options
4.      Main Menu
5.      Accounting Directory
6.      Data Directory
7.      Debug
8.      IP Address
9.      Database Mode
10.     Users File
```

Option	Description
Mode	
Text	RadiusNT/X will read the users, clients and dictionary file to retrieve all standard information. If ODBC mode is enabled as well as text mode, the only text file which will be read is the *users* file. Accounting information will be stored in the database **and** in the detail files. All other configuration (dictionary, clients, etc.) will be read from the ODBC database.
ODBC	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	

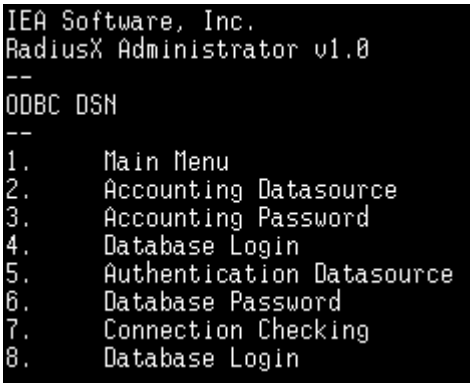
General	General information about the operation of RadiusNT/X, including requests.
User	User information during authentication (passwords, etc).
ODBC	ODBC information, including SQL statements.
File	File Information, including accounting and logging.
Authentication	
Ignore Case	By default, RadiusNT/X is case sensitive when authenticating a username and password. If this option is enabled, RadiusNT/X will make case in-sensitive compares for authentication. Note that CHAP authentication will **not** work if this option is selected.
Trim Name	When enabled, the Trim Name option will cause RadiusNT/X to trim spaces before and after a user's name. In addition, it will remove a DOMAIN\ prefix to a username. Please note that this is common on Windows NT Dial Up Networking (DUN) requests.
Port	This option allows you to specify the port RadiusNT/X will 'listen' for authentication requests on.
Accounting	
Require Secret	This option requires accounting packets to be 'signed'. This option is rarely needed, and should normally be left unchecked.
Allow Malformed	A RADIUS attribute with a length of two or less 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 greater.
Port	The Port option allows you to specify the port RadiusNT/X will 'listen' for accounting requests on.
Data Directory	The Data Directory option tells RadiusNT/X what directory to look in for configuration files (dictionary, users, clients, etc.) **if** Text Files mode is checked. This **must** be a fully qualified path in order for RadiusNT to run as a service. If you are using ODBC mode, this option directs RadiusNT/X where to write the log file.
Accounting Directory	If Text Files mode is selected, the Accounting Directory option tells RadiusNT/X in what directory to create the accounting directories (one per NAS) and detail log file (‘date’.log). This directory **must** already exist for RadiusNT/X to be able to save accounting information. To run RadiusNT as a service, it **must** be a fully qualified path.
Users File	If Text Files Mode is selected, the specified file is the file RadiusNT/X reads user's information from. This file **must** be present in the Data directory.

ODBC DSN Menu Options

RadiusNT Administrator ODBC DSN Menu



RadiusX Text-based Administrator ODBC DSN Menu

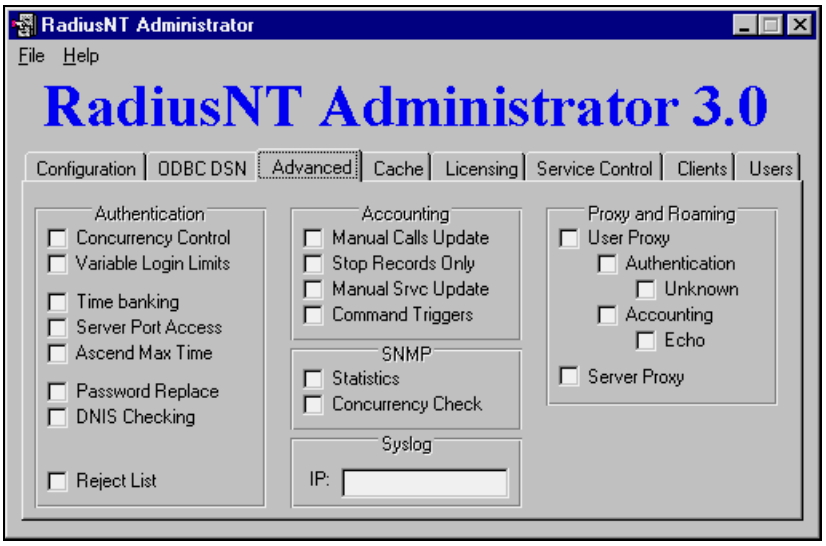


Option	Description
Authentication	
DSN	This specifies the ODBC DSN RadiusNT/X uses to connect to the ODBC database. Multiple DSNs can be specified (space separated) to fail-over to other database servers if the primary is not available. Other databases are tried in the order they're entered.
Username	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.
Verify	This option is used for verification of the password for the database user.
Check	You can use the Check button to verify that the DSN settings are correct.
Accounting	
DSN	This specifies the ODBC DSN RadiusNT/X uses to connect to the ODBC database. Multiple DSNs can be specified (space seperated) to failover to other database servers if the primary is not avaliable. 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.
Verify	This option is used for verification of the password for the database user.
Check	You can use the Check button to verify that the DSN settings are correct.
Use Different Accounting DSN	Check this option if you would like RadiusNT/X to use a different ODBC DSN or set of credentials for the accounting thread, rather than those specified by the authentication set.

Advanced Menu Options

RadiusNT Administrator Advanced Menu



RadiusX Text-based Administrator Advanced Menu

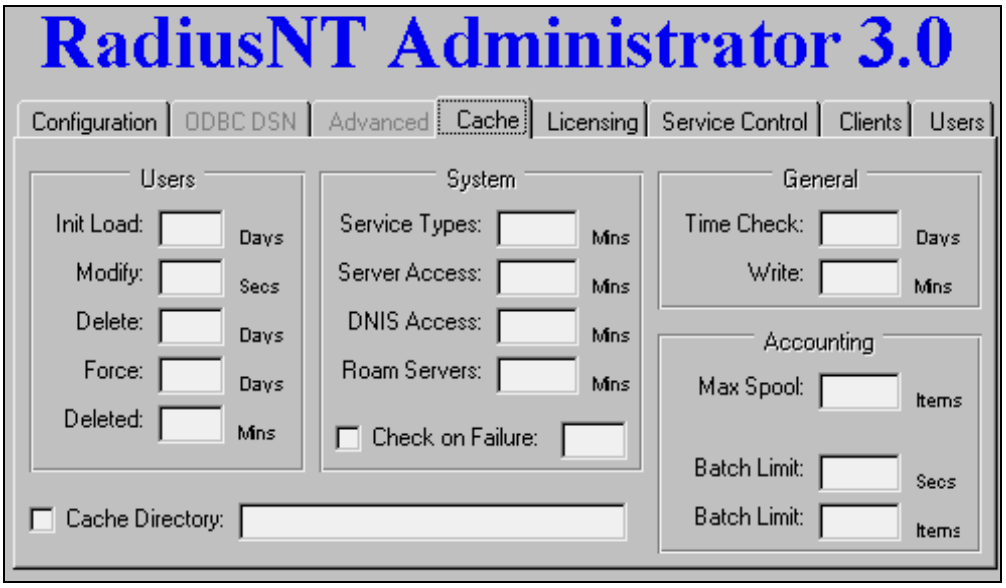
```
IEA Software, Inc.
RadiusX Administrator v1.0
--
Advanced
--
1.      Main Menu
2.      Agentx domain socket directory
3.      Authentication & Accounting
4.      Proxy and Roaming
5.      Proxy Identifier
6.      Proxy Timeout
7.      SNMP
8.      Syslog server configuration
```

Option	Description

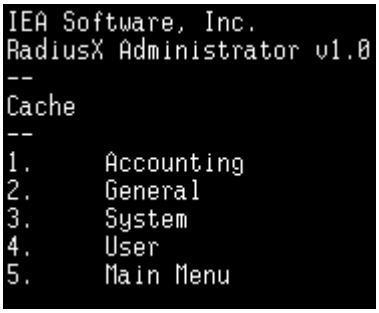
Authentication	
Concurrency Control	RadiusNT/X can restrict users from logging in more than one time if this option is enabled. If the Variable Login Limits option is not enabled, then the limit is set to one. On the other hand, if the Variable Login Limits option is enabled, then the limit is taken from the Login Limit field in the SubAccounts table.
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.
DNIS Checking	This enables the Dialed Number Identification Service (DNIS) checking option. Please see the Chapter 9 ODBC Advanced section for more details on DNIS checking and restrictions.
Reject List	This option enables Reject List checking. Please see the Chapter 9 ODBC Advanced section for more details on the Reject list option.
Accounting	
Manual Calls Update	RadiusNT/X will manually update the ServerPorts table. This is only needed for databases that do not have trigger support and the option is **not** needed with Emerald/SQL Server or an active database that can update the calls online 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 online.
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.
SNMP	
Statistics	This option enables SNMP statistics. See Chapter 9 for more information about SNMP. **(Professional version only)**
Concurrency Check	This option enables SNMP Concurrency verification See Chapter 9 for more information about SNMP. **(Professional version only)**
Proxy and Roaming	
User Proxy	This option enables User Based Proxy. See Chapter 9 for more information about Proxy. **(Professional version only)**
Server Proxy	This option enables Server Based proxy. See the Chapter 9 for more information about Proxy. **(Professional version only)**

Cache Menu Options

RadiusNT Administrator Cache Menu



RadiusX Text-based Administrator Cache Menu



Option	Description
Users	
Init Load	Number of days since the last successful authentication an account should be preloaded into the cache.
Modify	Interval to check for and update the cache database with new information on changed accounts (in seconds).
Delete	Number of days an account can remain in the cache without being requested before being removed.
Force	The number of days without a cache update to force account information to be updated.

Deleted	Interval (in minutes) to search for accounts that have been deleted in the database but still exist in the cache. If an account is marked inactive the most time a cached account can still successfully authenticate is based on the 'Modify' option. Otherwise if an account is simply removed the most time a cached account can successfully authenticate is based on this option.
Check on Failure	Query the database when a cached account would otherwise reject an authentication request. (In the case of an expired account, bad password or no time left in the time bank). This usually isn't necessary as account changes are regularly synchronized with the database.
Min Wait	Every specified number of seconds, a connection to every datasource available is checked. If the connection fails the datasoure is marked unavailable until the next check. **(Professional version only)**
General	
Time Check	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.
Write	If the write cache to disk option is checked, the 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. **(Professional version only)**
Accounting	
Max Spool (items)	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. 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. **(Standard edition limited to 500)**.
Max Batch (items)	The maximum number of items that can be sent in a single accounting batch. (See Max Batch time) **(Professional version only)**
Max Batch (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. **(Professional version only)**
System	
Service Type	Service type cache update interval (in minutes).
Server Access	Server-Access cache update interval (in minutes).
DNIS Access	DNIS cache update interval (in minutes).
Roam Servers	Roam Server cache update interval (in minutes).
Write Cache to Disk	Enable Accounting and 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. **(Professional version only)**

Licensing Info Menu

RadiusNT Administrator Licensing Menu

RadiusX Text-based Administrator Licensing Menu

Option	Description
Company Name	License Key Company Name
License Key	RadiusNT/X License Key

Service Control Menu

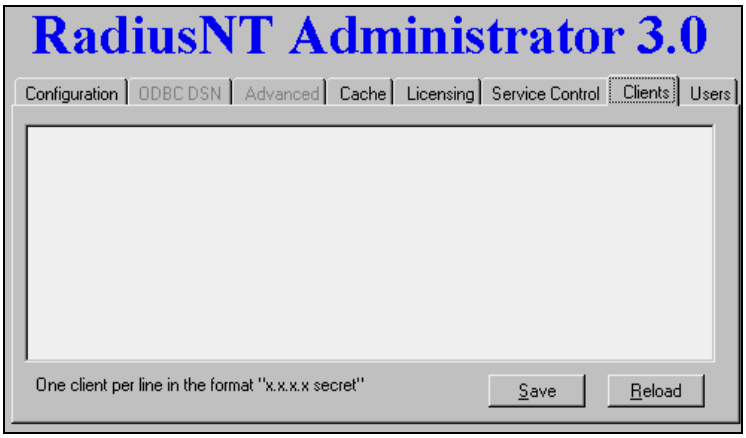
RadiusNT Administrator Service Control Menu

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.

Option	Description
Install Service	Install RadiusNT as a service. The radius.exe file **must** be in the same directory as the RadiusNT Administrator for this to option to be available.
Remove Service	Remove RadiusNT as a service. The radius.exe file **must** in the same directory as the RadiusNT Administrator for this to option to be available.

Clients Menu

RadiusNT Administrator Clients Menu

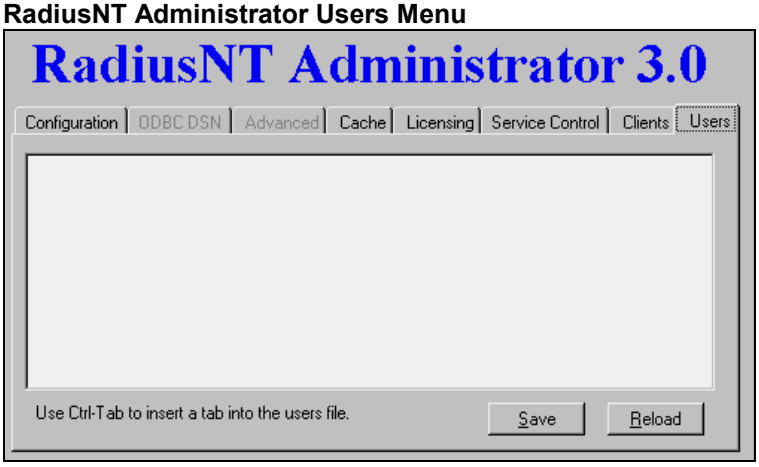


Please note that when using RadiusX, you **must** configure the *clients* file outside of the Administrator using any text editor.

Option	Description
Edit Window	Clients which can make requests to RadiusNT. See Chapter 2 below for more details about the *clients* file.
Save	Save the contents of the edit window to the *clients* file.
Load	Reload the *clients* file into the edit window

Users Menu

RadiusNT Administrator Users Menu



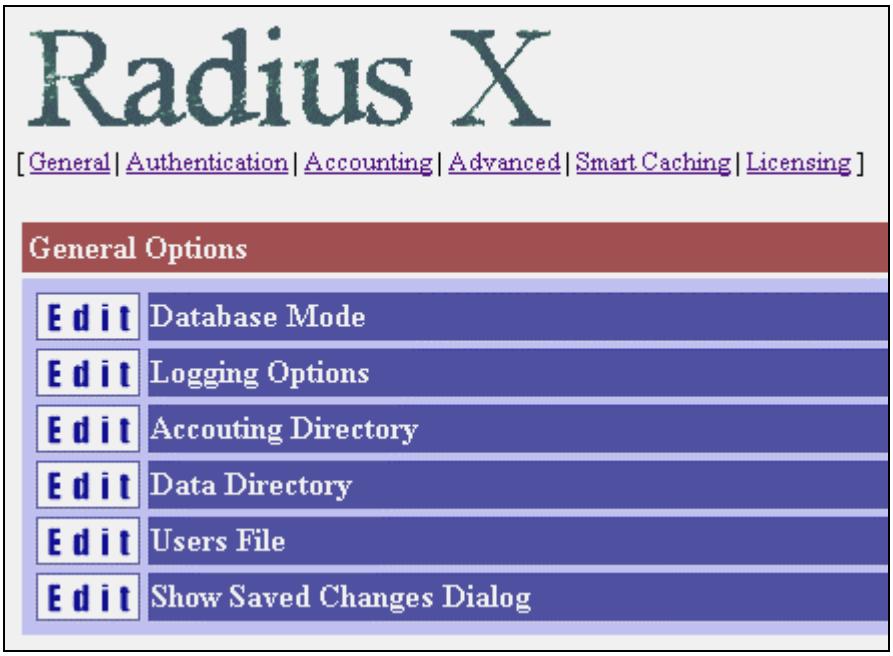
Please note that when using RadiusX, you **must** configure the *users* file outside of the Administrator using any text editor.

Option	Description
Edit Window	User list for RadiusNT to authenticate from. See Chapter2 for more details about the *users* file.
Save	Save the contents of the edit window to the *users* file.
Load	Reload the *users* file into the edit window

Configuration Options for RadiusX Web-based Administrator

Although very similar, the RadiusX Web-based Administrator configuration options have slightly different menus. Please refer to the following section if you are using the Web-based Administrator for RadiusX.

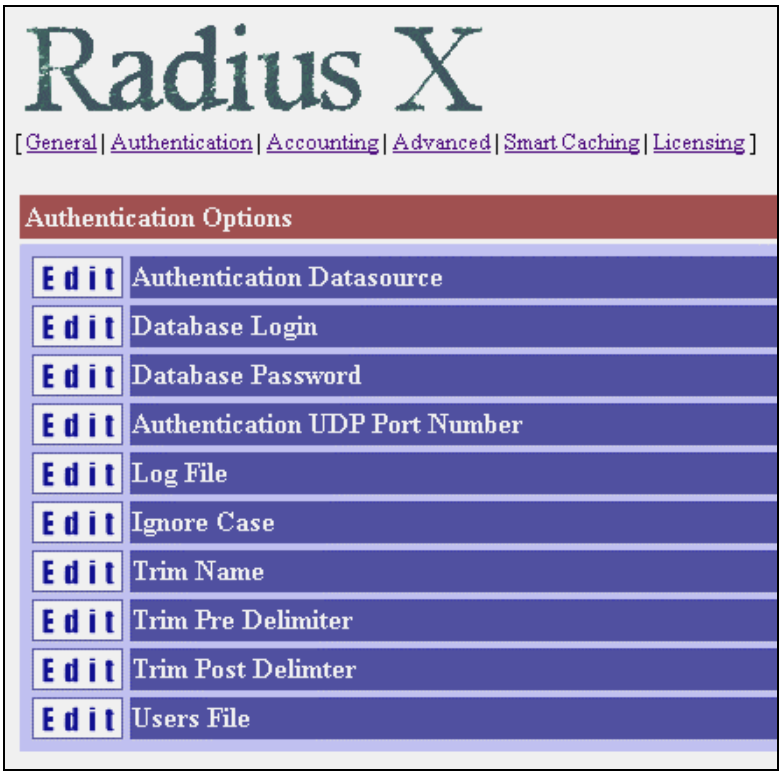
RadiusX Web-based Administrator General Menu



Option	Description
Database Mode	
Text	RadiusNT/X will read the users, clients and dictionary file to retrieve all standard information. If ODBC mode is enabled as well as text mode, the only text file which will be read is the *users* file. Accounting information will be stored in the database **and** in the detail files. All other configuration (dictionary, clients, etc.) will be read from the ODBC database.
ODBC	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.
Logging Options	
General	General information about the operation of RadiusNT/X, including requests.
User	User information during authentication (passwords, etc).
ODBC	ODBC information, including SQL statements.
File	File Information, including accounting and logging.
Accounting Directory	If Text Files mode is selected, the Accounting Directory option tells RadiusX in what directory to create the accounting directories (one per NAS) and detail log file ('date'.log). This directory **must** already exist for RadiusNT/X to be able to save accounting information. To run RadiusNT as a service, it **must** be a fully qualified path.

Data Directory	The Data Directory option tells RadiusX what directory to look in for configuration files (dictionary, users, clients, etc.) **if** Text Files mode is checked. This **must** be a fully qualified path in order for RadiusNT to run as a service. If you are using ODBC mode, this option directs RadiusX where to write the log file.
Users File	If Text Files Mode is selected, the specified file is the file RadiusNT/X reads user's information from. This file **must** be present in the Data directory.
Show Saved Changes Dialog	When you select this option after making changes you will be prompted with a 'Configuration Saved' message. You are then given the option of going back to the previous menu or restarting the RADIUS server.

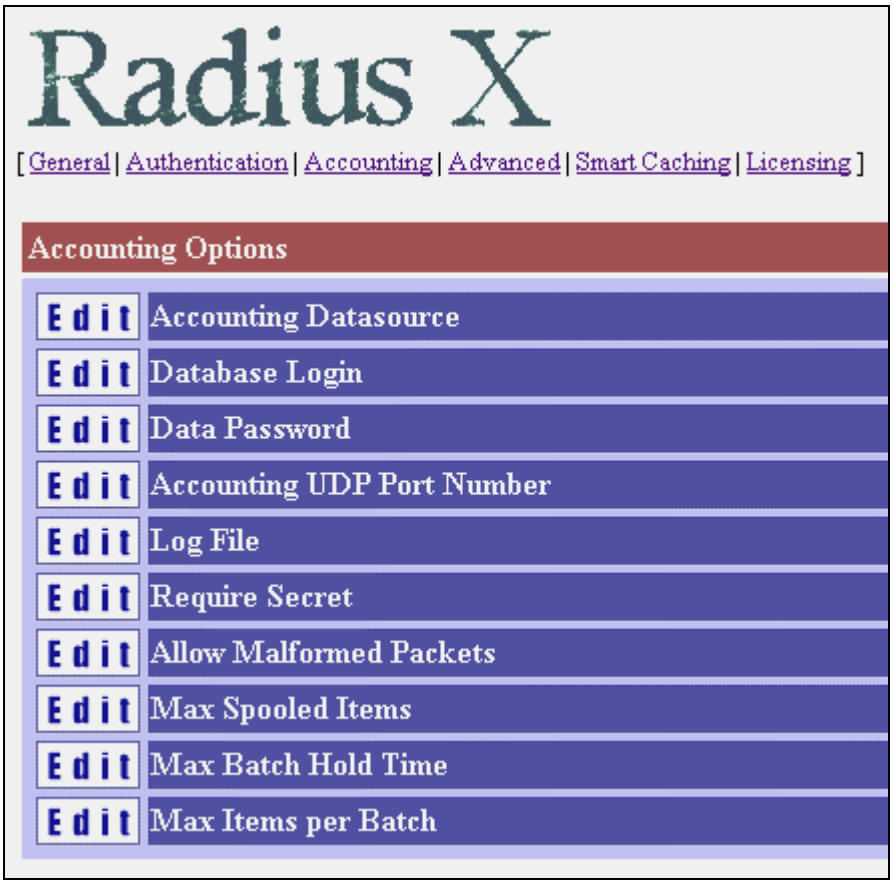
RadiusX Web-based Administrator Authentication Menu



Option	Description
Authentication Datasource	This specifies the ODBC DSN RadiusNT/X uses to connect to the ODBC database. Multiple DSNs can be specified (space separated) to fail-over to other database servers if the primary is not available. Other databases are tried in the order they're entered.
Database Login	Use this to specify the username RadiusNT/X uses to log into the ODBC database.
Database Password	This option specifies the password for the database user.
Authentication UDP Port Number	This option allows you to specify the port RadiusX will 'listen' for authentication requests on.

Log File	The logfile 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 make case in-sensitive compares for authentication. Note that CHAP authentication will **not** work if this option is selected.
Trim Name	When enabled, the Trim Name option will cause RadiusNT/X to trim spaces before and after a user's name. In addition, it will remove a DOMAIN\ prefix to a username. Please note that this is common on Windows NT Dial Up Networking (DUN) requests.
Trim Pre Delimiter	When enabled, this will cause RadiusX to trim spaces before a user's name, as well as remove a DOMAIN prefix to a username (which is common on Windows NT and Windows 95 Dial Up Networking (DUN) requests).
Trim Post Delimiter	When enabled, this will cause RadiusX to trim spaces after a user's name, as well as remove a DOMAIN prefix to a username (which is common on Windows NT and Windows 95 Dial Up Networking (DUN) requests).
Users File	If Text Files mode is checked, this is the file name RadiusX will try and read the user's information from. This file must be present in the data directory.

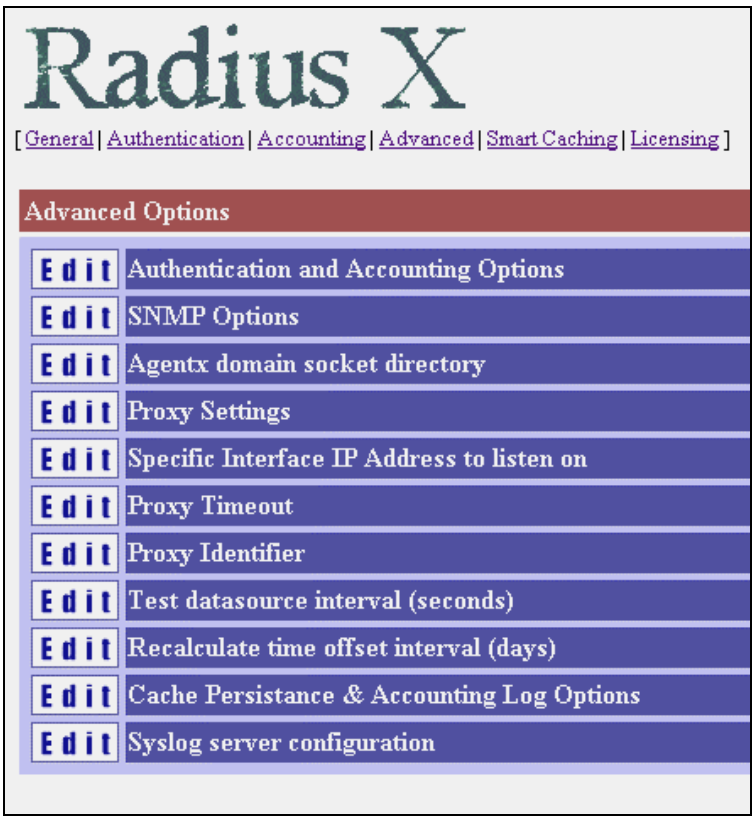
RadiusX Web-based Administrator Accounting Menu



Option	Description
Accounting Datasource	This specifies the ODBC DSN RadiusX uses to connect to the ODBC database. Multiple DSNs can be specified (space separated) to fail-over to other database servers if the primary is not available. Other databases are tried in the order they're entered.
Database Login	Use this to specify the username RadiusNT/X uses to log into the ODBC database.
Database Password	This option specifies the password for the database user.
Accounting UDP Port Number	The Port option allows you to specify the port RadiusX will 'listen' for accounting requests on.
Log File	Accounting logfile name. Typically used in text only mode.
Require Secret	The option requires accounting packets to be 'signed'. This option is rarely needed, and should normally be left unchecked.
Allow Malformed Packets	A RADIUS attribute with a length of two or less is considered to be a malformed packet. By enabling this option, you will allow RadiusX to accept attributes with a length of two or greater.
Max Spooled Items	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. New additions will be dropped if Max Spooled Items already exist in memory. RadiusX will not ACK the accounting packet giving another RADIUS server the opportunity to respond. (**Standard edition limited to 500**).
Max Batch Hold Time	RadiusX can queue accounting informaiton and then send a batch of multiple request 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. (**Professional version only**).
Max Items per Batch	The maximum number of items that can be sent in a single accounting batch. (See Max Batch Hold Time) (**Professional version only**).

RadiusX Web-based Administrator Advanced Menu

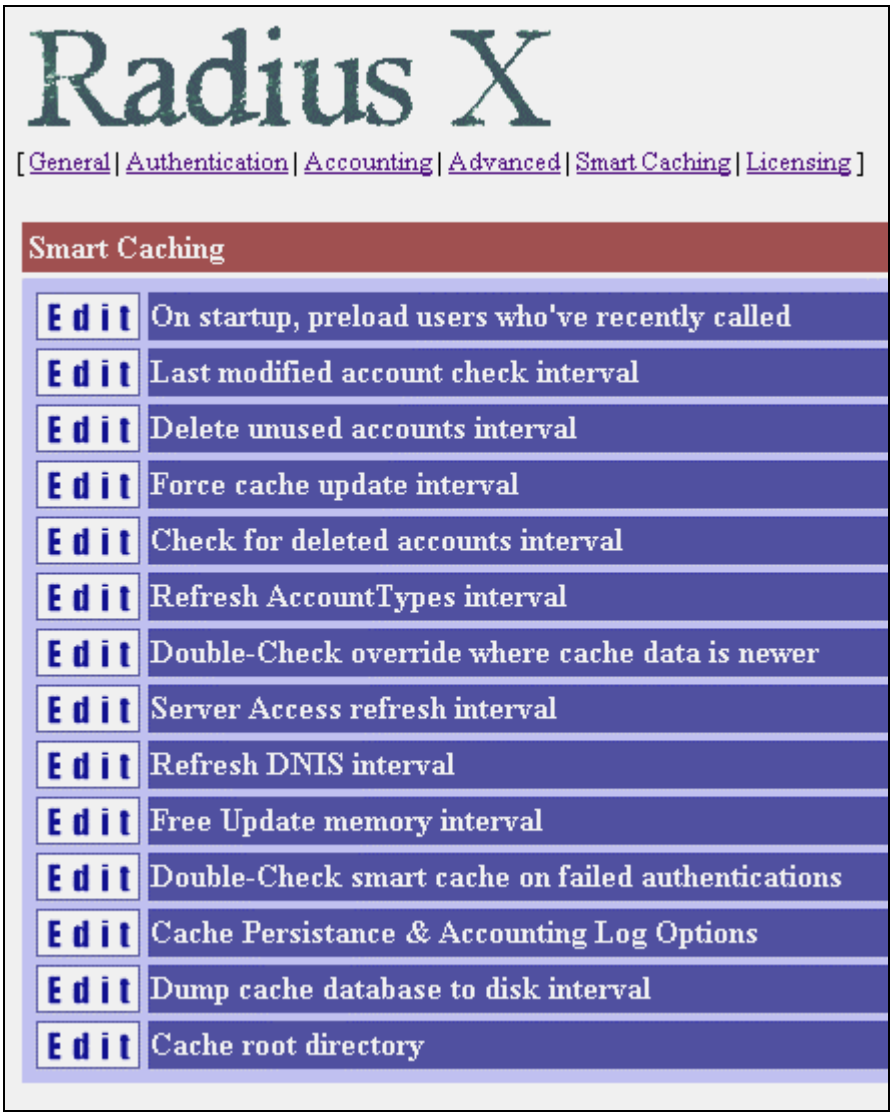


Option	Description
Authentication Concurrency Control	RadiusNT/X can restrict users from logging in more than one time if this

	option is enabled. If the Variable Login Limits option is not enabled, then the limit is set to one. On the other hand, if the Variable Login Limits option is enabled, then the limit is taken from the Login Limit field in the SubAccounts table.
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.
DNIS Checking	This enables the Dialed Number Identification Service (DNIS) checking option. Please see the Chapter 9 ODBC Advanced section for more details on DNIS checking and restrictions.
Reject List	This option enables Reject List checking. Please see the Chapter 9 ODBC Advanced section for more details on the Reject list option.
Accounting	
Manual Calls Update	RadiusNT/X will manually update the ServerPorts table. This is only needed for databases that do not have trigger support and the option is **not** needed with Emerald/SQL Server or an active database that can update the calls online 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 online.
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.
SNMP	
Statistics	This option enables SNMP statistics. See Chapter 9 for more information about SNMP. **(Professional version only)**
Concurrency Check	This option enables SNMP Concurrency verification See Chapter 9 for more information about SNMP. **(Professional version only)**
Agentx Domain Socket Directory	The pathname of the directory where the master agent's (snmpd) Unix domain socket endpoint is located. This can typically be left blank to accept the default (/var/agentx). If RADIUS or snmpd logs errors about initializing the Agentx library, make sure the directory exists and that both programs have enough permissions to access the directory.
Proxy and Roaming	
User Proxy	This option enables User Based Proxy. See Chapter 9 for more information about Proxy. **(Professional version only)**
Server Proxy	This option enables Server Based proxy. See the Chapter 9 for more information about Proxy.

	(Professional version only)
Specific Interface IP Address to Listen On	RadiusX can Bind to a specific IP Address, leave this option blank to bind to all.
Proxy Timeout	This option allows setting the timeout for Authentication and Accounting proxy. The default is 30 seconds.
Proxy Identifier	
Test Datasource Interval (seconds)	RadiusX opens a connection to every datasource available to it each X number of seconds. If the connection fails, the datasource is marked unavailable.
Recalculate Time Offset Interval (days)	Database time offset in days. This option queries the authentication and accounting databases and computes a time offset from the local clock for various authentication and accounting functions. This option controls how often to compute these offsets.
Cache Persistence & Accounting Log Options	Check the accounting box to enable the Accounting cache database to be regularly written to disk. This enables RadiusX to recover after being restarted where no valid authentication data sources exist. Check the authentication box to enable the Authentication cache database to be regularly written to disk. This enables RadiusX to recover after being restarted where no valid authentication data sources exist. (**Professional version only**).
Syslog Server Configuration	Error and informational messages can be directed to a syslog server by entering its IP Address.

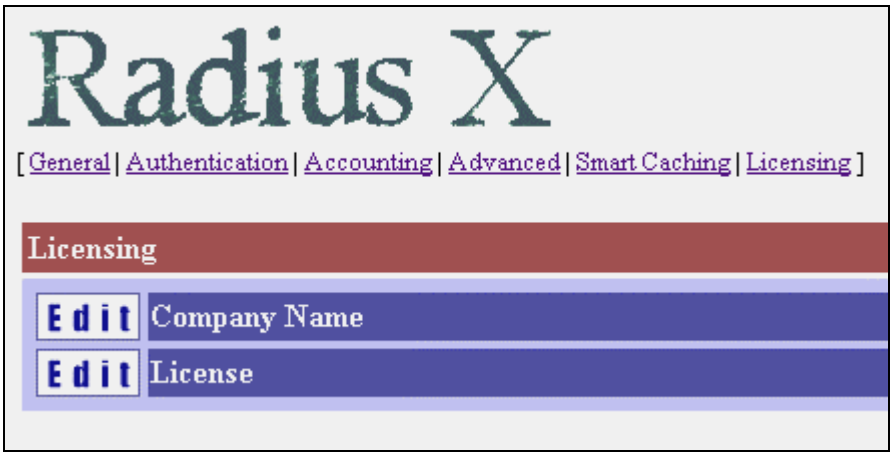
RadiusX Web-based Administrator Smart Caching Menu



Option	Description
On Startup, Preload Users Who Have Recently Called	Number of days since the last successful authentication an account should be preloaded into the cache.
Last Modified Account Check Interval	Interval to check for and update the cache database with new information on changed accounts (in seconds).
Delete Unused Accounts Interval	Number of days an account can remain in the cache without being requested before being removed.
Force Cache Update Interval	The number of days without a cache update to force account information to be updated.
Check for Deleted Accounts Interval	Interval (in minutes) to search for accounts that have been deleted in the database but still exist in the cache. If an account is marked inactive the most time a cached account can still successfully authenticate is based

	on the 'Modify' option. Otherwise if an account is simply removed the most time a cached account can successfully authenticate is based on this option.
Refresh AccountTypes Interval	Service type cache update interval (in minutes).
Double-Check Override Where Cache Data is Newer	Query the database when a cached account would otherwise reject an authentication request. (In the case of an expired account, bad password or no time left in the time bank). This usually isn't necessary as account changes are regularly synchronized with the database.
Server Access Refresh Interval	Server Access cache update interval (in minutes).
Refresh DNIS Interval	DNIS cache update interval (in minutes).
Free Update Memory Interval	Memory used to update account information is not immediately freed. Instead, it is placed in a queue to be removed later. This option controls how often the delete process is run. Any object less than 5 minutes old can not be removed. If you are performing timebanking and do not have much memory, set this low. Otherwise, in most cases the default value is optimal.
Double-check Smart Cache on Failed Authentications	This option queries the database when the cache copy would otherwise NACK an accounting request. (Ex: in the case of an expired account, bad password or no time left in the timebank). This option is usually not necessary as account changes are regularly synchronized with the database.
Cache Persistance & Accounting Log Options	Enable Accounting and Authentication cache database to be regularly written to disk. This enables RadiusX to recover after being restarted where no valid authentication data sources exist. **(Professional version only)**
Dump Cache Database to Disk Interval	If this option is selected, it 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. (**Professional version only**)
Cache Root Directory	This option specifies where to store cache data.

RadiusX Web-based Administrator Licensing Menu



Option	Description
Company Name	License Key Company Name
License	RadiusX License Key

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 setup 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 list of Users, Clients and Dictionary. If you change any of these files, you **must** stop and re-start RadiusNT/X in order for the changes to take affect. 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 referenced later.
3. Next, edit the *clients* file. Replace 127.0.0.1 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 a good editor such as Programmer's File Editor, pico, vi as Edit or Notepad do not preserve the Tab. The RadiusNT Administrator allows correct editing of this file as well.

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

Quick Tip!	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 the future you may want to refer to the *users.example* file to get some ideas of more complex user entries.
8. Next, go to a 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 configured correctly, a "waiting for requests" 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. 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 usage.

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

Please remember that if you change the file, you **must** stop and re-start RadiusNT/X in order for the changes to take affect.

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. We have included an example MS Access 7.0 database in the RadiusNT distribution with forms and sample data already created for your convenience.

To configure an ODBC DSN for RadiusNT, follow these steps:

1. Select Start, Settings and then Control Panel.

2. From the Control Panel, (Win2000 users select 'Admin Tools'), then select ODBC. Please note that if you do not have ODBC installed, you will need to install ODBC 2.5 or higher to proceed. ODBC is shipped with many applications, and is available from Microsoft's FTP site at ftp://ftp.microsoft.com/developr/ODBC/public/. You can also install ODBC from the SQL Server CD-ROM directory *\i386\odbc*.

3. After the ODBC Administrator opens, select the System DSN button. If your system does not display a System DSN button, you will need to upgrade to at least ODBC 2.5 or higher.

4. Click the Add button.

5. For a SQL Server installation, select the SQL Server Driver. For other database types, select the corresponding ODBC driver. For an Emerald installation, please see Appendix B.

6. For the Data Source Name option, type "**Radius**".

7. Enter "**RadiusNT**" for the Description.

8. Depending on what type of driver you have installed, the next step will vary. Please refer to your database documentation to learn more about configuring an ODBC DSN for your database system.

- SQL Server

1. For Server, enter the name of the SQL Server you are using.

2. Click Options, then Database. Enter the name of the database on your SQL Server that RadiusNT will be accessing.

3. Leave the Library and Network addresses set to default.

- MS Access

1. Click the Select button in the database box and choose your MS Access file. Please note that if you need to login to the database, you will need to select the Advanced option and fill in the required information.

9. Finally, select Save and close the Control Panel.

To configure an ODBC DSN for RadiusX (Solaris Only), follow these steps:

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

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

[ODBC Data Sources]
Radius_MSSQL65=RadiusX ODBC Driver

[Radius_MSSQL65]
Driver=/usr/local/radius/lib/E-msss14.so
Description=Radius_MSSQL65
Database=Radius
ServerIPAddress=127.0.0.1
ServerPortNumber=1433
LogonID=
Password=
UseProcForPrepare=0
QuotedId=No
```

AnsiNPW=No

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

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

Database=Radius
This is the name of the database containing your Radius database.

ServerIPAddress=127.0.0.1
This reflects the IP address of the SQL Server and must be numeric.

ServerPortNumber=1433
This notates the TCP port that the SQL Server is 'listening' on.

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

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

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

To configure RadiusNT for ODBC operations, follow these steps:

1. While in the RadiusNT Administrator, check ODBC.
2. From the DSN pick list, select the ODBC DSN that you created above. Please note that you **must reload DSNs** to read in the new ODBC DSN that you have created **if** it doesn't appear in the list. In order to do this, select **File**, then **Reload DSNs**.
3. Select the Security tab and enter a Username that you will use for logging into the database.
4. Next, enter a Password in the Password and Verify text boxes.
5. To verify the database connection, click the Check button.
6. Lastly, select File and then Save.

The next step is to configure the database **before** starting RadiusNT. 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. You do this by accessing a DOS Command Prompt and then changing to the directory where RadiusNT is installed. Execute the following command to start RadiusNT in full debug mode:

"radius -x15"

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

For an Emerald installation, please see Appendix B.

To configure RadiusX for ODBC operations, follow these steps:

The installation process configures most everything that is needed for RadiusX ODBC operations. Should you need to set the database mode or DSN option, please follow the steps below:

1. Change to the directory where the RadiusX Administrator resides, **/usr/local/radius**.

2. Start the Administrator by typing "**perl *radadmn.pl***".

3. At the Main Menu, select the **ODBC DSN** option. This is where you can set DSN options. When completed, select the **Main Menu** option to continue.

4. At the Main Menu, select the **Configuration** option .

5. Next, select the **Database Mode** option. This is where you can set Database Mode options. When completed, select the **Main Menu** option to continue.

6. Select **Exit** to complete the process. Your changes are automatically saved when you exit the RadiusX Administrator.

The next step is to configure the database **before** starting RadiusX. 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 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" (NT)
"./radiusd –x15" (UNIX)

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

For an Emerald installation, please see Appendix B.

Both Mode

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

For authentication, the *users* file is read when RadiusNT/X starts. RadiusNT 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, which does not exist. RadiusNT will not write any accounting information. You **must** have a *users* file if you have text file mode checked, though. 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. The following show sample configuration information for several of the more popular NAS vendor's equipment. You **must** consult the documentation for your NAS as the final authority on how to configure your NAS for RADIUS interaction.

Livingston Portmasters

Telnet to the Portmaster and enter these commands:

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

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

Ascend MAX and Pipeline

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

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

Auth=RADIUS
Auth Host #1=x.x.x.x
Auth Port=1645
Auth Timeout=5
Auth Key=yyyyy
Auth Pool=No
Auth Req=Yes

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

Acct=RADIUS
Acct Host #1=x.x.x.x
Acct Port=1646
Acct Timeout=5
Acct Key=yyyyy

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

Other RADIUS compatible NAS

Basic configuration settings are as follows:

- Set Authentication and Accounting to RADIUS
- Set Authentication and Accounting servers to the Radius NT/X server's IP address
- Set Authentication and Accounting secrets to the same as they are in the *clients* file or ODBC database
- Set Authentication and Accounting ports to **1645** and **1646**, respectively

Please check the Radius Technology Partners Web page on our Web site at 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 login as a user that you have configured in either the *users* file or the ODBC database. If the login is successful you will receive a successful authentication response from RadiusNT/X and your NAS. Once a successful test has been completed, you can then install RadiusNT to run as a service to startup automatically or RadiusX to start up automatically through a script.

Radlogin

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

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

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

1.2.3.4 mysecret
127.0.0.1 localhost

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

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

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

127.0.0.1 localhost

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

The Radlogin program allows two or three parameters. By simply typing "Radlogin" at the Command Prompt, command line options will be displayed as shown below.

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

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

Authentication Test

To send an authentication request to RadiusNT/X, type "radlogin" followed by a username and password. Please note that you may need to put quotes around the username or password if they include a space. By default, Radlogin will return a verbose result stating whether the request was acknowledged or not, along with any attributes that RadiusNT/X returned. Optionally, you can include a number as the third parameter to send multiple, sequential tests. This is a handy way to check performance. The Radlogin results will summarize the requests and give an average response time.

Accounting Test

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

Trouble Shooting

If your Radlogin test was not successful, please check the following hints. You can find additional trouble shooting tips and Frequently Asked Questions (FAQs) in Chapters 10 and 11.

1. If you do not see the authentication request on the RadiusNT/X screen, your NAS is not setup 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 that the NAS is sending the request to.

2. If you see the request on the RadiusNT/X screen, but RadiusNT/X prints an 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 yyyyy. However, the DNS for host yyyyy 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 then install it to run as a service and startup 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.

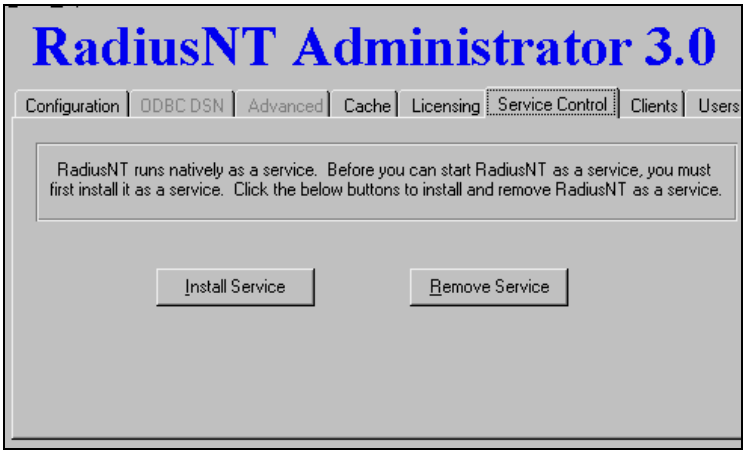
Quick Tip!	Running RadiusNT as a service is handy for times when you are not logged in and need to start or stop RadiusNT remotely.

Installing RadiusNT as a Service

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

1. Open the RadiusNT Administrator and change to the Service Control tab.
2. Click the Install Service button.

RadiusNT Administrator Service Control



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 finally that the userid RadiusNT is running as for a service has the proper permissions to access the ODBC datasource.

Removing the Service

To remove the RadiusNT service, follow these steps:

1. Open the RadiusNT administrator.

2. Select the Service Control tab.

3. Click the Remove Service button.

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 also start and stop the RadiusNT service using the Control Panel, Services applet.

Should you encounter any problems, proceed to 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. You can also configure the service to automatically start when the computer is booted using the Control Panel, Services applet. 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 how UNIX RADIUS servers function. In order 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 their entry in the '*passwd'* file. If no entry is found, the user is simply 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 user's actual password they entered during authentication (if the passwords match). This option is used for migration purposes to reverse out the encrypted passwords to clear text passwords stored in the database. To enable this option, select the Replace Password option in the RadiusNT Administrator. For more information, please read the RadiusNT 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. In order for RadiusNT to authenticate users from the NT SAM, RadiusNT **must** run as a user with sufficient rights. Please see the next section "NT SAM Permission Requirements" for specific instructions regarding these rights. You can modify user rights in the Windows NT User Manager. Using the Control Panel, Services applet, you can specify whom RadiusNT will login as when it runs as a service.

In order 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 databases. Please note that case is significant. 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 user’s actual password they entered during authentication (if the passwords match). This is used for migration purposes to reverse out the encrypted passwords to clear text passwords. To enable this option, select the Replace Password option in the RadiusNT Administrator. For more information, please read the RadiusNT Registry entries section.

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

```
name    Password                                =                    “WINNT”
        User-Service = Framed-User
```

If you are running RadiusNT in **text** mode, you can use the DEFAULT user entry to examine the NT SAM for the usernames and passwords. To accomplish, 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.

NT SAM Permission Requirements

In order for RadiusNT to authenticate against the NT SAM, the account RadiusNT is configured to use **must** have special user rights. You can change or add the rights of a user in the User Manager or User Manager for Domains option, which is typically available in the Administrative Tools Menu group of Windows NT. The required rights are as follows:

- Act as part of the Operating System
- Increase Quotas
- Replace a Process Level Token

Quick Tip!	If you receive the error message "RadiusNT does not have sufficient rights to authenticate against the NT SAM', there is a permissions problem with the account that RadiusNT is running as. If you are authenticating against a domain and RadiusNT is **not** running on a domain controller, you **must** change the service to login as a user with the above-mentioned rights for the domain. Please note that the system user on a stand-alone NT server or workstation does not have sufficient rights to authenticate against the domain. In some cases you may need to logout and log back in after changing the rights to implement the changes.

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 the values below 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 simply 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 *detail* 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 *clients* 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 or 2 Concurrency Checking
-d [path]	DataDirectory	This designates the directory where RadiusNT reads the *users*, *clients*, *dictionary* and *passwd* files.
-I[#]	IgnoreCase	Use this to ignore upper or lower 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 compares.
-M[#] **-o or –b**	Mode	By default RadiusNT uses text mode, where 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 *users* 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 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 1645.
-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 1646.
-P[#]	Proxy	If you have a Professional version 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	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. 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 Variable Login Limit 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 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).
-S	ExtSupport	Used to select External Authentication support.
-T	ProxyTimeout	If you have a Professional version 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 *users* 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	The debug mode is typically used directly from the command line to diagnose problems. Debug options are: 1 Information 2 User Debug 4 ODBC Debug 8 File Debug 16 SNMP Debug 32 Smart cache debug 64 Memory debug Simply add the options you want together. For instance, if you want Information and ODBC debugging, you would use -x5. The common full debug mode is –x15.
-X		This option specifies packet level debugging.

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

Registry	Description
License	Displays the RadiusNT license.
CompanyName	Displays the company name that is licensed for RadiusNT use.
DBM	This entry shows the ODBC RDBMS mode that RadiusNT will be 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: 0 Automatic detection 1 Microsoft SQL Server 2 Microsoft Access 3 Sybase SQL Server 4 Oracle Database Server
ODBCTimeout	The 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	The 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	Displays the username RadiusNT will use to make the ODBC

	connection to the alternate ODBC datasource for accounting.
AcctPassword	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 at intervals of for the specified number of seconds shown. If the connection fails the datasource is marked unavailable **(Professional version only).**
CacheUserModifyCheckSecs	Displays the interval (in seconds) to check for and update the cache database with new information on changed accounts.
CacheUserPrefetchLastDays	Upon startup, this will load users into the smart cache who've called within the specified number of days.
CacheDoubleCheck	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
CacheUserNoQueryOnFailSecs	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. For example: Consider an ISDN user with an expired account and the Cache Double Check Option enabled. Each channel of their ISDN router might try once a second to reconnect, causing unneeded database work.

CacheUserForceUpdateDays	Lists the refresh interval for any user who has been in the cache without being updated. This makes certain that any possible consistency problem cannot exist for more than the number of days specified.
AcctMaxHoldTime	Radius can buffer accounting information and send a batch of multiple requests to the database server as a single query. This reduces overall load on the database, but at the expense of added latency. This option will limit the number of seconds any single piece of accounting data can be queued in a batch. Note: Set this entry low (a few seconds) if you're doing time banking or require concurrent login checking. **(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 shows the Server-Access cache update interval (in minutes).
CacheRootDirectory	This entry shows the directory where RadiusNT stores cache data. **(Professional version only)**
CacheRoamServerUpdateMins	This shows the Roam Server cache update interval (in minutes). **(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. **(Standard edition limited to 500)**
CacheAccountTypesUpdateMins	This entry shows that the updating of the service types cache will be at the interval specified.
AgentxSocket	This displays the directory to 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 enough permissions to access the directory. **(UNIX Professional version only)**
CacheWriteMins	If cache persistence is enabled this option enables you to specify how often the contents of the cache database should be written to disk to allow starting radius to a useable state where no authentication database is available. **(Professional version only)**

DeferredMemFreeMins	This entry shows the amount of memory used to update account information that is not immediately freed. Instead it's 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. **(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 that if accounts have not been requested within the number of days specified, they will be removed from the cache.
NVFlag	This flag shows whether the ability to have the accounting and authentication cache database regularly written to disk is enabled. It enables RadiusX to recover after being restarted where no valid authentication data sources exist. **(Professional version only)** The flags are as follows: 1 Accounting 2 Authentication

Chapter 8 - ODBC DATABASE SCHEMA

One of the most powerful features of RadiusNT/X is the capability to integrate it with a backend RDBMS. RadiusNT/X accomplishes this through ODBC. You will find that many features are available in ODBC mode which are not available in text mode, simply because the backend 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. The following information details what is available.

Table Layout

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

Required Table	Field	Type	Description
MasterAccounts			First Tier Account Information
	CustomerID	Integer	IDENTITY / AutoNumber
	Active	Bit	If this field is 0, the account will **not** be authenticated.
	MaExpireDate	Datetime	Expiration date of the account. If this is NULL, the account will **not** expire.
	Extension	Integer	An extension (in days) to the Expiration date.
	OverDue	Tinyint	An extension (in days) to the Expiration date.
	*OverLimit	Money	If the Balance field is over 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.
SubAccounts			Second Tier Account Information Please note that there can be **many** records from this table, which relate to a **single** record in the MasterAccounts Table.
	AccountID	integer	IDENTITY / AutoNumber
	CustomerID	integer	Related MasterAccounts record
	Active	bit	If this field is 0, the account will **not** be authenticated.
	Login	varchar(32)	The Login ID for the user.
	Shell	varchar(32)	The Shell ID (login) for the user.

	AccountType	varchar(15)	The Account Type of the user.
	Password	varchar(16)	The password for the user.
	saExpireDate	datetime	The Expiration Date for this SubAccount. If this is NULL, the Expiration Date of the MasterAccount is used.
	Extension	integer	An extension (in days) to the Expiration Date (SA).
	*LoginLimit	tinyint	The Currency Login Limit for the SubAccount.
	*TimeLeft	integer	The Login Time Left (in minutes) for the SubAccount. This should be set to NULL if the user has no time limit.
	LastUsed	Datetime	Last date the user logged in, NULL if this is not being tracked. Used by the RadiusNT/X caching system to preload recently authenticated users into the cache database.
RadVendors			RADIUS Vendor Ids
	RadVendorID	integer	Vendor ID
	Name	varchar(32)	Vendor Name
RadAttributes			Stores the RADIUS dictionary information.
	RadAttributeID	integer	Unique RADIUS Attribute ID
	Name	varchar(25)	RADIUS Attribute Name
	Type	int	RADIUS Attribute Type 0 String 1 32-bit Integer 2 IP Address 3 Date Ascend Binary
	RadVendorID	int	If this attribute is a Vendor Specific Attribute (RadAttributeID = 26) then this denotes the Vendor ID. Otherwise the value should be NULL or 0.
	RadVendorType	int	If this attribute is a Vendor Specific Attribute (RadAttributeID = 26) then this denotes the Vendor Type. Otherwise the value should be NULL or 0.
RadValues			Lookup Values for some of the RADIUS Attributes
	RadAttributID	integer	Related RadAttributeID from RadAttributes table.
	RadVendorID	int	If this attribute is a Vendor Specific Attribute (RadAttributeID = 26) then this denotes the Vendor ID. Otherwise the value should be NULL or 0.

	RadVendorType	int	If this attribute is a Vendor Specific Attribute (RadAttributeID = 26) then this denotes the Vendor Type. Otherwise the value should be NULL or 0.
	Name	varchar(25)	Value Name
	Value	integer	Value Number
RadConfigs			RADIUS Reply Attributes for individual SubAccounts.
	RadConfigID	integer	IDENTITY / AutoNumber
	AccountID	integer	Related AccountID from SubAccounts table.
	RadAttributeID	integer	Related RadAttributeID from RadAttributes table.
	Data	varchar(99)	Used for String, IP Address or Date Types.
	Value	integer	Used for Integer Types.
	RadVendorID	int	If this attribute is a Vendor Specific Attribute (RadAttributeID = 26) then this denotes the Vendor ID. Otherwise the value should be NULL or 0.
	RadVendorType	int	If this attribute is a Vendor Specific Attribute (RadAttributeID = 26) then this denotes the Vendor Type. Otherwise the value should be NULL or 0.
	RadCheck	tinyint	A zero denotes this is a normal reply attribute. A non-zero denotes this a check attribute.
RadATConfigs			RADIUS Reply attributes for AccountTypes.
	RadATConfigID	integer	IDENTITY / AutoNumber
	AccountType	varchar(15)	Related to AccountType from the AccountTypes table.
	RadAttributeID	integer	Related RadAttributeID from RadAttributes table.
	Data	varchar(99)	Used for String, IP Address or Date Types.
	Value	integer	Used for Integer Types.
	RadVendorID	int	If this attribute is a Vendor Specific Attribute (RadAttributeID = 26) then this denotes the Vendor ID. Otherwise the value should be NULL or 0.
	RadVendorType	int	If this attribute is a Vendor Specific Attribute (RadAttributeID = 26) then this denotes the Vendor Type. Otherwise the value should be NULL or 0.
	RadCheck	tinyint	A zero denotes this is a normal reply attribute. A non-zero denotes this a check attribute.
Servers			RADIUS Clients Information

	ServerID	integer	IDENTITY / AutoNumber
	Server	varchar(25)	RADIUS Client Name
	IPAddress	varchar(16)	IP Address of RADIUS Client.
	Secret	varchar(16)	Shared Secret for RADIUS Client.
	RadRoamServerID	integer	Optional Roam Server to unconditionally forward all requests to. Set to NULL (the default) for normal user-based proxy.
	Community	varchar(16)	SNMP Community for the server.
	SNMPType	integer	Type of SNMP server.

Optional Table	Field	Type	Description
Calls			This table stores Accounting Call records. It is unique in that RadiusNT will dynamically read the table to find out what records to store. The field names and types **must** match an entry from the RadAttributes table, with the exception that the field names do not include the dashes. Please note that the Calls table is dynamic. Please see Appendix A for a full listing of the RADIUS standard attributes and their definitions.
	NASIdentifier	varchar(16)	Identifier for the NAS. Please note that this is typically the IP Address of the NAS.
	NASPort	integer	NAS Port the call came in on.
	AcctSessionID	varchar(16)	NAS generated unique ID for the call.
	AcctStatusType	tinyint	Accounting record type 1 Start 2 Stop
	CallDate	datetime	Date of Call.
	UserName	varchar(32)	Username of caller.
			The above fields are the BASE required fields. You can (and should) add more fields to allow for storage of the fields you need to use. An example of some common fields to add would be AcctSessionTime and AcctDelayTime. Please refer to Appendix A for a list of the RADIUS standard attributes and their definitions.

AccountTypes			The AccountTypes table is not directly used by RadiusNT/X, but is used as a lookup table for the AccountType fields in the SubAccounts and RadATConfigs tables.
	AccountType	varchar(15)	Name of the Account Type.
	Description	varchar(30)	Description of the Account Type.
	DNISGroupID	integer	The DNISGroupID of the DNISGroup that the account type is allowed to log into. No DNIS group is enforced if this field is NULL.
RadLogMsgs			The RadLogMsgs table provides text descriptions of the RadLogMsgID numbers in the RadLogs table.
	RadLogMsgID	integer	Log Message Identifier. Please see the section below on ODBC Logging for more details.
	Description	varchar(50)	Description of the Log Message Identifier.
	Severity	integer	Severity of the Log Message.
RadLogs			The RadLogs table contains log information if RadiusNT/X is run in either ODBC or both mode.
	RadLogMsgID	integer	Related Log Message Identifier from RadLogMsgs
	LogDate	datetime	The message date.
	UserName	varchar(32)	The associated username (if one exists).
	Data	varchar(50)	Additional data, dependent on the Log Message ID.
ServerPorts			The ServerPorts table contains information about each port available for a NAS. This is required for concurrency control and for monitoring who is on-line.
	ServerID	integer	Related ServerID From Servers.
	Port	integer	The port number.
	UserName	varchar(32)	Last Username on the port.
	AcctStatusType	tinyint	Status of the last user on the port.
	CallDate	datetime	Calldate of the last user on the port.
	FramedAddress	varchar(16)	IP Address of the last user on the port.

	SNMPUser	varchar(64)	SNMP Object Identifier (OID) string for SNMP Concurrency checking.
ServerAccess			The ServerAccess table contains information on which AccountTypes can access which ports.
	ServerID	integer	Related ServerID from Servers.
	Port	integer	Related Port from ServerPorts.
	AccountType	varchar(15)	Related AccountType from AccountTypes.
	MaxSessionLength	integer	The Maximum Session length allowed.
	StartTime	integer	The start time allowed to login, in minutes from midnight.
	StopTime	integer	The stop time allowed to login, in minutes from midnight.
DNISGroups			The DNISGroups table defines each DNIS group that an Account Type is allowed to use.
	DNISGroupID	integer	IDENTITY/AutoNumber
	DNIGGroup	varchar(25)	Name of the DNIS Group.
	Description	varchar(45)	Description of the DNIS Group.
DNISNumbers			The DNISNumbers table defines each DNIS number that is associated to a DNIS group.
	DNISGroupID	integer	Related DNISGroupID from the DNISGroups table.
	DNIGNumber	varchar(10)	The DNIS number as reported by the RADIUS client.
RadRoamServers			The RadRoamServers table contains information about Roam servers which RadiusNT can proxy requests to.
	RadRoamServerID	integer	IDENTITY / AutoNumber
	IPAddress	varchar(16)	IPAddress of Roam Server.
	Server	varchar(32)	Name of Roam Server.
	Secret	varchar(16)	Secret to use for requests going to Roam server.
	Timeout	integer	Number of seconds to wait for a reply (not currently used).
	Retries	integer	Number of retries (not currently used).
	TreatAsLocal	bit	Do not proxy domain and treat user as local.

	StripDomain	integer	Strip the domain from the username before sending.
	AuthPort	integer	Port number to send authentication requests to (defaults to 1645). Please note that if this field is 0 or NULL, authentication requests will not be forwarded to this server.
	AcctPort	integer	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.
	AllowRLogin	tinyint	A non-zero value allows a RLogin Framed-Service type.
RadRoamDomains			The RadRoamDomains table contains the domains RadiusNT can proxy requests for and which Roam Server the request should be forwarded to.
	RadRoamDomainID	integer	IDENTITY / AutoNumber
	RadRoamServerID	integer	Roam Server to forward requests to.
	Domain	varchar(32)	Roam Domain in the login (user@domain).
	Priority	integer	Roam Server's Priority for the domain.
	CostPerMinute	integer	Cost per minute (cents) for the roam (not currently used).
	AccountType	varchar(15)	If this option is **not** NULL, then RadiusNT/X will ignore the attributes returned in the proxy reply and return the set of attributes associated to this account type.
RadTriggers			The RadTriggers table contains program information for RadiusNT/X, which can be executed when the associated account logs in (accounting start record).
	RadTriggerID	integer	IDENTITY / AutoNumber
	AccountID	integer	Related AccountID from SubAccounts.
	Type	integer	Type of trigger (currently not used).
	Filename	varchar(64)	Executable program or file to run.
	Parameters	varchar(64)	Parameter for the program or file.
	Directory	varchar(128)	Working directory for the program or file.
RadRejects			The RadRejects table contains a list of attribute/value information for RadiusNT/X to

			immediately reject a request.
	RadRejectID	integer	IDENTITY / AutoNumber
	RadAttributeID	integer	Related RadAttributeID from RadAttributes table.
	RadVendorID	int	If this attribute is a Vendor Specific Attribute (RadAttributeID = 26), then this denotes the Vendor ID. Otherwise, the value should be NULL or 0.
	RadVendorType	int	If this attribute is a Vendor Specific Attribute (RadAttributeID = 26), then this denotes the Vendor Type. Otherwise, the value should be NULL or 0.
	Data	varchar(99)	Used for String, IP Address or Date Types.
	Value	integer	Used for Integer Types.
RadProxyAttributes			The RadProxyAttributes table holds attribute/value pairs for proxying radius requests by attributes and values.
	RadProxyAttributeID	integer	Identity / AutoNumber
	RadProxyAttributeGroupID	integer	Used by RadProxyAttributeGroups to associate a group of attributes to a proxy server.
	RadAttributeID	integer	Related RadAttributeID from RadAttributes table.
	SearchType	Integer	Type of rule used in searching for matching attribute/values. 1 string 2 substring 3 equal 4 less than 5 greater than
	String	Varchar(253)	Value to search on.
RadProxyAttributeGroups			The RadProxyAttributeGroups table is used to associate a group of RadProxyAttributes with a proxy server.
	RadProxyAttributeGroupID	Integer	Identity/ AutoNumber
	RadRoamServerID	Integer	Server to proxy matching requests.
	Priority	Integer	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.
	Description	Varchar(255)	Description of this attribute proxy group.
Licenses			The Licenses table contains license information for RadiusNT/X.

	LicenseID	varchar(25)	The License key.
	Company	varchar(40)	The Company name in the License. Please note that this is case sensitive and must match exactly with what was provided with the license key itself.

Inside the Database

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

Authentication Process

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

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

There are typically two ways to return a set of attributes for a user's authentication. If you want to return a set of attributes specific to a single user, then you need to add records to the RadConfigs table 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 Systems

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

Microsoft SQL Server

RadiusNT/X can be an Enterprise-wide solution when used with Microsoft SQL server. The inherent Client/Server design allows multiple clients to use the database simultaneously, without taking a performance hit. SQL Server is also suited to handle tables that can contain over one million records, and includes replication and fail safe operations.

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

Name	Description
RadCheckOnline	Check to see how many times a user is on-line.
RadCheckTrigger	Check to see if an external trigger is available for this user.
RadAtCache	Retrieve a list of service attributes.
RadServerAccessCache	Retrieve server access information.
RadDNISCache	Retrieve DNIS information.

RadGetProxyAttributes	Fetch proxy attributes.
RadGetRejects	Retrieve reject attributes.
RadRoamCache	Retrieve roaming information.
RadUserDefaults	Retrieve list of service RADIUS defaults.
RadGetConfigs	Retrieve list of RADIUS default attributes for an AccountID.

Below is a list of the stored procedures that Emerald provides for RadiusNT/X to use. The parameters and returned columns **must** be of the same type, but the stored procedures **can** be modified to the database design if you are not using Emerald.

```
CREATE PROCEDURE RadCheckOnline @UserName varchar(64) AS
Select Count(Username) From CallsOnline Where UserName=@UserName and AcctStatusType=1

CREATE PROCEDURE RadCheckOnlineSNMP @Username varchar(64) AS
Select s.IPAddress, s.ServerType, s.Community, sp.SNMPUser, sp.AcctSessionID
From Servers s, ServerPorts sp
Where s.ServerID = sp.ServerID
        AND Username=@Username
        AND AcctStatusType=1

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

CREATE PROCEDURE RadGetConfigs @AccountID int AS
Select ra.RadAttributeID, Name, Data, Value, Type, rc.RadVendorID, rc.RadVendorType, rc.RadCheck
From RadConfigs rc, RadAttributes ra
Where ra.RadAttributeID=rc.RadAttributeID
        AND ra.RadVendorID = rc.RadVendorID
        AND ra.RadVendorType = rc.RadVendorType
        AND rc.AccountID=@AccountID
GO

CREATE PROCEDURE RadUserSpecifics AS
SELECT rc.AccountID, ra.RadAttributeID, ra.Type, rc.Data, rc.Value, rc.RadVendorID,
        rc.RadVendorType, rc.RadCheck
From RadAttributes ra, RadConfigs rc
Where ra.RadAttributeID = rc.RadAttributeID
Order By AccountID, RadCheck, ra.RadAttributeID

CREATE PROCEDURE RadAtCache @accounttype VARCHAR(16) AS
SELECT rc.AccountType, ra.RadAttributeID, Name, Data, Value, Type, rc.RadVendorID,
rc.RadVendorType, rc.RadCheck
FROM RadATConfigs rc, RadAttributes ra
WHERE ra.RadAttributeID = rc.RadAttributeID
        AND (ra.RadVendorID = rc.RadVendorID OR rc.RadVendorID IS NULL)
        AND (ra.RadVendorType = ra.RadVendorType OR rc.RadVendorType IS NULL)
        AND (@accounttype IS NULL OR AccountType = @accounttype)
ORDER BY AccountType
GO
```

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

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

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

CREATE PROCEDURE RadGetCacheUsers @date DATETIME, @flag TINYINT AS
SELECT sa.AccountID, sa.Login, sa.Password, d.MailDomain, sa.AccountType, sa.LoginLimit,
sa.TimeLeft,
MasterExpire=CASE WHEN maExpireDate IS NULL THEN NULL ELSE
DATEDIFF(Day,'19700101',DATEADD(Day,ma.Extension+ma.OverDue,maExpireDate)) END,
SubExpire=CASE WHEN saExpireDate IS NULL THEN NULL ELSE
DATEDIFF(Day,'19700101',DATEADD(Day,sa.Extension,saExpireDate)) END,
OverLimit=CASE WHEN (ma.OverLimit > 0 AND ma.OverLimit > ma.Balance) THEN 1 ELSE 0 END
FROM SubAccounts sa, MasterAccounts ma, Domains d, Groups g
      WHERE sa.CustomerID = ma.CustomerID
      AND d.DomainID = g.DomainID
      AND ma.GroupID = g.GroupID
      AND sa.Active <> 0
      AND ma.Active <> 0
      AND sa.Login <> ''
      AND ((@flag = 1 AND sa.LastModifyDate > @date)
            OR (@flag = 2 AND (sa.LastUsed > @date OR sa.LastUsed IS NULL)))
UNION
SELECT sa.AccountID, sa.Email, sa.Password, d.MailDomain, sa.AccountType, sa.LoginLimit,
sa.TimeLeft,
MasterExpire=CASE WHEN maExpireDate IS NULL THEN NULL ELSE
DATEDIFF(Day,'19700101',DATEADD(Day,ma.Extension+ma.OverDue,maExpireDate)) END,
SubExpire=CASE WHEN saExpireDate IS NULL THEN NULL ELSE
DATEDIFF(Day,'19700101',DATEADD(Day,sa.Extension,saExpireDate)) END,
```

```
OverLimit=CASE WHEN (ma.OverLimit > 0 AND ma.OverLimit > ma.Balance) THEN 1 ELSE 0 END
FROM SubAccounts sa, MasterAccounts ma, Domains d, Groups g
      WHERE sa.CustomerID = ma.CustomerID
      AND d.DomainID = g.DomainID
      AND ma.GroupID = g.GroupID
      AND sa.Active <> 0
      AND ma.Active <> 0
      AND sa.Email <> ''
      AND ((@flag = 1 AND sa.LastModifyDate > @date)
            OR (@flag = 2 AND (sa.LastUsed > @date OR sa.LastUsed IS NULL)))
GO

CREATE PROCEDURE RadGetUser @user VARCHAR(64) , @password VARCHAR(32) AS
SELECT sa.AccountID, sa.Login, sa.Password, d.MailDomain, sa.AccountType, sa.LoginLimit,
sa.TimeLeft,
MasterExpire=CASE WHEN maExpireDate IS NULL THEN NULL ELSE
DATEDIFF(Day,'19700101',DATEADD(Day,ma.Extension+ma.OverDue,maExpireDate)) END,
SubExpire=CASE WHEN saExpireDate IS NULL THEN NULL ELSE
DATEDIFF(Day,'19700101',DATEADD(Day,sa.Extension,saExpireDate)) END,
OverLimit=CASE WHEN (ma.OverLimit > 0 AND ma.OverLimit > ma.Balance) THEN 1 ELSE 0 END
FROM SubAccounts sa, MasterAccounts ma, Domains d, Groups g
          WHERE sa.CustomerID = ma.CustomerID
          AND d.DomainID = g.DomainID
          AND ma.GroupID = g.GroupID
          AND sa.Active <> 0
          AND ma.Active <> 0
          AND sa.Login = @user
          AND (@password IS NULL OR sa.Password = @password)
UNION
SELECT sa.AccountID, sa.Email, sa.Password, d.MailDomain, sa.AccountType, sa.LoginLimit,
sa.TimeLeft,
MasterExpire=CASE WHEN maExpireDate IS NULL THEN NULL ELSE
DATEDIFF(Day,'19700101',DATEADD(Day,ma.Extension+ma.OverDue,maExpireDate)) END,
SubExpire=CASE WHEN saExpireDate IS NULL THEN NULL ELSE
DATEDIFF(Day,'19700101',DATEADD(Day,sa.Extension,saExpireDate)) END,
OverLimit=CASE WHEN (ma.OverLimit > 0 AND ma.OverLimit > ma.Balance) THEN 1 ELSE 0 END
FROM SubAccounts sa, MasterAccounts ma, Domains d, Groups g
      WHERE sa.CustomerID = ma.CustomerID
      AND d.DomainID = g.DomainID
      AND ma.GroupID = g.GroupID
      AND sa.Active <> 0
      AND ma.Active <> 0
      AND sa.Email = @user
      AND (@password IS NULL OR sa.Password = @password)
GO
```

Sybase SQL Server

RadiusNT/X supports operation with Sybase the same as Microsoft's SQL Server, thus please see the above Microsoft SQL Server section for an overview. The difference lies within the scripts used to create the database itself, since there are slight differences between Microsoft's TSQL and Sybase's TSQL. An example set of scripts for creating a database under Sybase is included with the RadiusNT/X distribution.

Microsoft Access

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

RadiusNT/X will internally create all SQL Statements for MS Access. This limits the flexibility of the database design to follow the Emerald layout, but does not limit the power or features of what RadiusNT/X can offer.

A fully working Access 7.0 database is included with the RadiusNT/X distribution. Please use this as a starting point to test or build additional features or options that you would like to use in your installation.

Oracle

RadiusNT/X supports operation with Oracle in a similar fashion to MS Access. Each SQL query is built into RadiusNT/X and executed on the fly. This differs from Microsoft SQL and Sybase in that it does not rely on stored procedures or additional database configuration (excluding the base tables).

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. In order 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. If you do **not** have variable login limits enabled, RadiusNT/X defaults to allow the user to login **one** time. If you do have variable login limits enabled, RadiusNT/X allows the user to login the number of times specified in the LoginLimit field in the SubAccounts table. All additional requests will be rejected.

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 login once, you **must** enable variable login limits; 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, like a trigger (ex: 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 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.

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 online 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 setup 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 RadiusNT/X Administrator and then restart RadiusNT/X. In addition, you **must** have a NAS that supports the Session-Timeout attribute.

Server Access

Server Access allows you to limit the ports 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 Access in the RadiusNT/x 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 RadiusNT/X Administrator and then restart RadiusNT/X. In addition, please check with your NAS vendor to be sure your NAS supports DNIS-related attributes before enabling DNIS restrictions.

Reject List

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

Logging

By enabling ODBC logging, RadiusNT/X will log information to the database. You will find this information to be very useful if needed for debugging or problem solving. In addition, you can generate reports and gather statistics to help solve possible 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. Lastly, 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. Furthermore, 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. Below you will find a table describing the RadLogMsgIDs.

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 in other words, the Balance is larger than allowed.
14	Concurrency Limit	The user is already logged in the maximum allowed number of login times.
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.
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 user names 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. Below is a list of the reserved user names.

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

Chapter 10 – PROFESSIONAL VERSION 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 their full e-mail address (ex: user@company.com). This signals to RadiusNT/X that the user is a roaming user, not a local user. RadiusNT/X extracts the domain (ex: 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 which RadiusNT/X **must** handle to insure reliable delivery to the final server and an accurate response back 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 which 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, RadRoamServer and RadRoamDomains. One of the more useful options is the default domain. If you define a domain as "DEFAULT", RadiusNT/X will send all roaming requests to it 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 actually allows you to specify that a domain should not be forwarded. This flag is very useful when used 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 that your users may try to login as (ex: 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 TreastAsLocal flag is set to true, the server that 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, but 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
User Proxy: Authentication
User Proxy: Accounting

3. 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 above step.

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 (ex: 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, you need to 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 successfully.

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 theRadProxyAttributes and RadProxyAttributeGroups tables for more information on configuring attribute proxy.

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 setup 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 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), in order 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", 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") w/out the tree name (HKEY_LOCAL_MACHINE is assumed).

7. In order 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

Please note that 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 (ex: the SNMP tools which come with the Windows NT Resource Kit). The Object Identifier (OID) for the base information for RadiusNT is 1.3.6.1.3.79. One of the easiest ways to see each of the values available is to use the *Snmpwalk* application to 'walk' the RADIUS tree. Snmpwalk will display the tree/subtree values that you specify. Below you will find the command that illustrates an example of this.

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

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

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

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

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

SNMP Authentication

SNMP Object Identifier	Object Name	Description
.1.3.6.1.3.79.1.1.1.1.1.0	Identification	RadiusNT Identification string: "RadiusNT 3.x.xxx"
.1.3.6.1.3.79.1.1.1.1.2.0	Up Time	The number of seconds RadiusNT has been running.
.1.3.6.1.3.79.1.1.1.1.3.0	Reset Time	The number of seconds since RadiusNT was reset.
.1.3.6.1.3.79.1.1.1.1.4.0	Config Reset	State of RadiusNT: 1-Unknown, 3-Init, 4-Running.
.1.3.6.1.3.79.1.1.1.1.5.1	Access Requests	Number of requests since startup.
.1.3.6.1.3.79.1.1.1.1.5.2	Invalid Requests	Number of requests from unknown clients.

.1.3.6.1.3.79.1.1.1.1.5.3	Duplicate Requests	Number of duplicate requests.
.1.3.6.1.3.79.1.1.1.1.5.4	Access Accepts	Number of good requests (successful logins).
.1.3.6.1.3.79.1.1.1.1.5.5	Access Rejects	Number of rejected requests (failed logins).
.1.3.6.1.3.79.1.1.1.1.5.6	Access Challenges	Number of CHAP Challenges.
.1.3.6.1.3.79.1.1.1.1.5.7	Malformed Requests	Number of malformed requests (not bad authenticators).
.1.3.6.1.3.79.1.1.1.1.5.8	Bad Authenticators	Number of bad authenticators (invalid secrets).
.1.3.6.1.3.79.1.1.1.1.5.9	Packets Dropped	Number of requests dropped w/out a reply sent.
.1.3.6.1.3.79.1.1.1.1.5.10	Unknown Types	Number of packets of unknown types.

SNMP Accounting

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

AgentX Support

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

If you run across errors regarding initializing the Agentx library, please make sure the directory exists and that both RadiusX and AgentX have enough 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 cause a user to be inadvertently 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 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 following stored procedure to retrieve information about each port the user is listed on. Please note that you need to have this stored procedure in your database and that the user RadiusNT/X is connecting as **must** have execute permission for it.

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

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

Server Types

RadiusNT/X uses the ServerType field in the Servers Table to track the types of servers. 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 denotations.

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 in 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 fail-over 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, 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.

Chapter 11 – TROUBLE SHOOTING

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 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 very valuable when diagnosing problems as well.

Installation and Setup Problems

- An error message stating an RDC object can not be registered during installation

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

Startup Problems

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

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

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

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

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

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

Operation Problems

- When a request is received, RadiusNT/X displays a “Security Breach” error.

  This error will appear if the machine that 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 affect.

- The decrypted password from the authentication request is garbage.

  This is caused when the secret which is configured on the NAS sending the request is not the same 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 affect. Also recall 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 entries being required to be unique.

  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 12 – 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 (ex: 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 normal for awhile, 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 describing why it stopped authenticating or what the problem is.

- *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 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, 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.itef.org. The RADIUS RFCs are 2138 and 2139. 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 (ex: Ascend).

- *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.

- *In order 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 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 methods ways to handle the changes. You can either restart RadiusNT/X as the users are cached in memory, you can use the *reload* user entry with radlogin This signals RadiusNT/X to reload the *users* file w/out restarting the service.
  Another option is to set the Reload User Minutes setting in the RadiusNT/X administrator to periodically reload the users file at regular intervals.

ODBC Mode

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

  A couple of 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.

  Radius will either automatically detect a crypted password string or the encryption type can be specified as part of the password (ex: {crypt}teH0wLIpW0gyQ). 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 NAS allow for a distinct accounting and authentication RADIUS server.

- *Is it possible to treat a non-SQL Server ODBC driver like the MS Access ODBC driver?*

  Yes. Simply add "16" to the Options registry entry to force RadiusNT/X to perform in MS Access mode.

- *Where can I learn more about ODBC?*

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

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

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

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

  In order to do this, you **must** add entries in the RadConfigs table, that match the user's SubAccountID. Please note that one of the attributes needs to be the Framed-Address attribute. In addition, you can **not** only add 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 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 tllcc where:

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

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

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

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

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

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

Cisco

- *I receive two Framed-Address attributes in my accounting packets and it is preventing RadiusNT/X from inserting the accounting packets into the database.*

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

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

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

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

  http://www.cisco.com/warp/public/732/General/rdius_wp.htm
  http://www.cisco.com/warp/public/732/111/555_pp.htm

Computone

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

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

iPass

- *Does RadiusNT/X support iPass roaming?*

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

ipSwitch

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

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

Livingston

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

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

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

Appendix A - RADIUS ATTRIBUTES

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 that 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 which 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 which is authenticating the user.
6	Service-Type	The type of service the user has requested, or the type of service to be provided. 1 Login 4 Callback Framed 7 NAS Prompt 2 Framed 5 Outbound 8 Authenticate Only 3 Callback Login 6 Administrative 9 Callback NAS Prompt

Below you find information from the RADIUS RFC 2138.

5.7. Framed-Protocol

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

Value

The Value field is four octets.

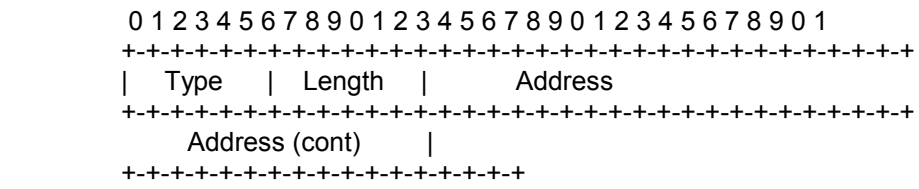
1 PPP
2 SLIP
3 AppleTalk Remote Access Protocol (ARAP)
4 Gandalf proprietary SingleLink/MultiLink protocol
5 Xylogics proprietary IPX/SLIP

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.

0 1 2 3



Type

8 for Framed-IP-Address.

Length

6

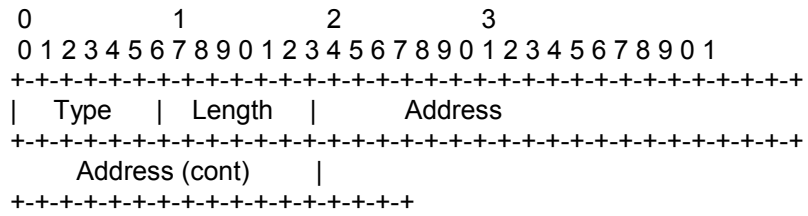
Address

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 0xFFFFFFFE 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

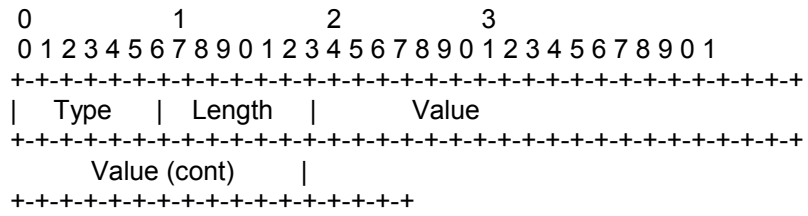
Address

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.

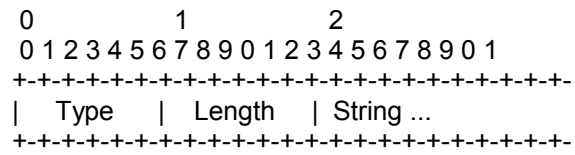
0 None
1 Send routing packets
2 Listen for routing packets
3 Send and Listen

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 NASes without regard to filter-list implementation details.

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



Type

11 for Filter-Id.

Length

>= 3

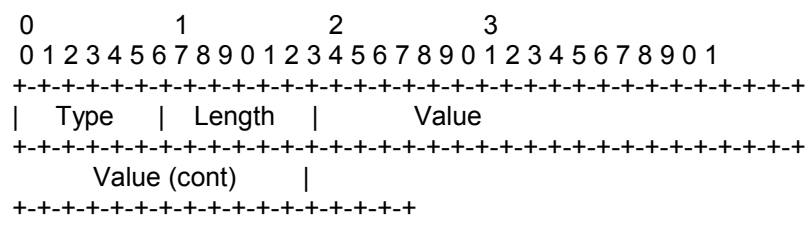
String

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

5.12. Framed-MTU

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

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



Type

12 for Framed-MTU.

Length

6

Value

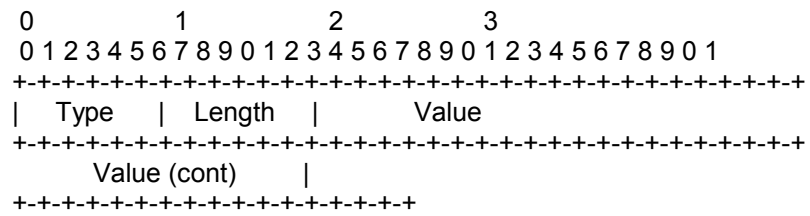
The Value field is four octets. Despite the size of the field, values range from 64 to 65535.

5.13. Framed-Compression

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

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

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



Type

13 for Framed-Compression.

Length

6

Value

The Value field is four octets.

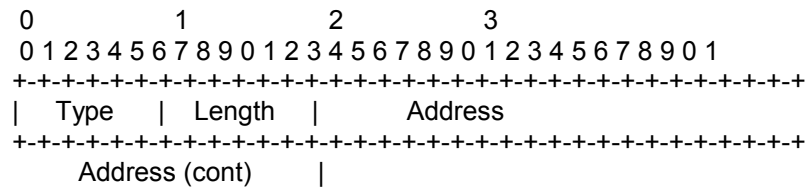
0 None
1 VJ TCP/IP header compression [5]
2 IPX header compression

5.14. Login-IP-Host

This Attribute indicates the system with which to connect the user, when the Login-Service Attribute is included. It MAY be used in Access-Accept packets. It MAY be used in an Access-

Request packet as a hint to the server that the NAS would prefer to use that host, but the server is not required to honor the hint.

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



```
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Type

14 for Login-IP-Host.

Length

6

Address

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

5.15. Login-Service

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

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

```
 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

15 for Login-Service.

Length

6

Value

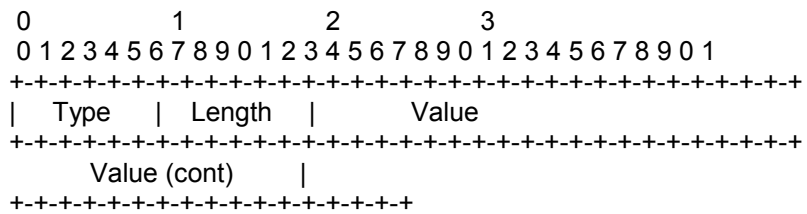
The Value field is four octets.

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.

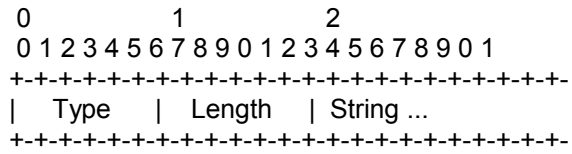
When used in an Access-Accept, it is the success message.

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

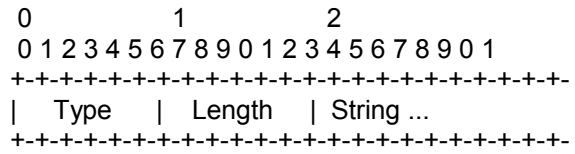
String

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 from the range 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.



Type

19 for Callback-Number.

Length

>= 3

String

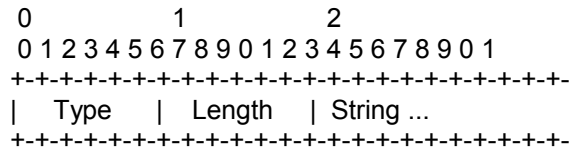
The String field is one or more octets. The actual format of the information is site or application specific, and a robust implementation SHOULD support the field as undistinguished octets.

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

5.20. Callback-Id

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

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



Type

20 for Callback-Id.

Length

>= 3

String

The String field is one or more octets. The actual format of the information is site or application specific, and a robust implementation SHOULD support the field as undistinguished octets.
The codification of the range of allowed usage of this field is outside the scope of this specification.

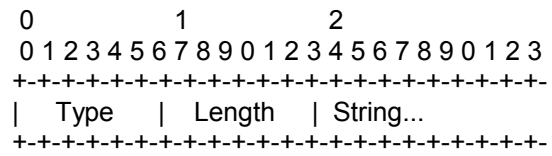
5.21. (unassigned)

ATTRIBUTE TYPE 21 HAS NOT BEEN ASSIGNED.

5.22. Framed-Route

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

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



Type

22 for Framed-Route.

Length

>= 3

String

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

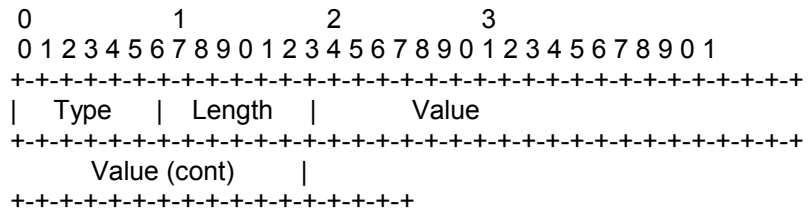
For IP routes, it SHOULD contain a destination prefix in dotted quad form optionally followed by a slash and a decimal length specifier stating how many high order bits of the prefix should be used. That is followed by a space, a gateway address in dotted quad form, a space, and one or more metrics separated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

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

5.23. Framed-IPX-Network

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

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



Type

23 for Framed-IPX-Network.

Length

6

Value

The Value field is four octets. The value 0xFFFFFFFE 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.

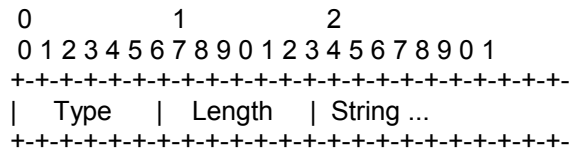
5.24. State

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.



Type

24 for State.

Length

>= 3

String

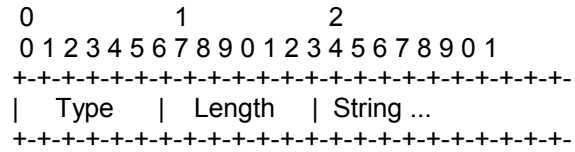
The String field is one or more octets. The actual format of the information is site or application specific, and a robust implementation SHOULD support the field as undistinguished octets.

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.



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.

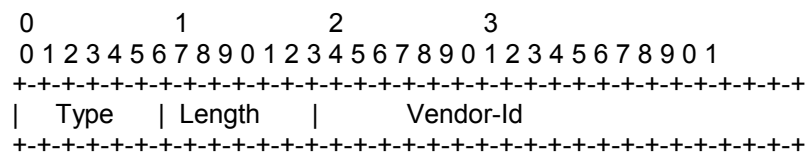
The codification of the range of allowed usage of this field is outside the scope of this specification.

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.



```
    Vendor-Id (cont)          |  String...
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

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:

```
 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       |           Vendor-Id
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
    Vendor-Id (cont)          | Vendor type   | Vendor length |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|   Attribute-Specific...
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-
```

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.

```
 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

27 for Session-Timeout.

Length

6

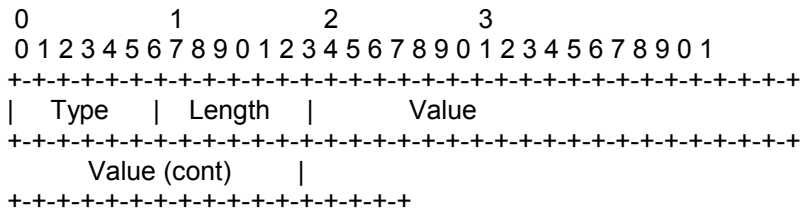
Value

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

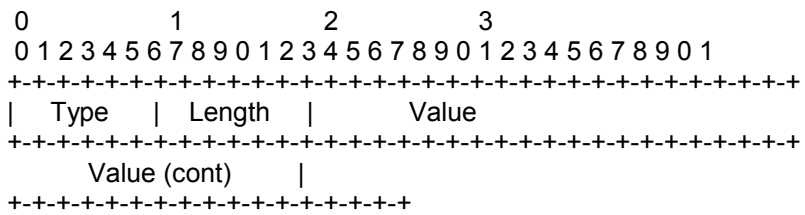
Value

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.

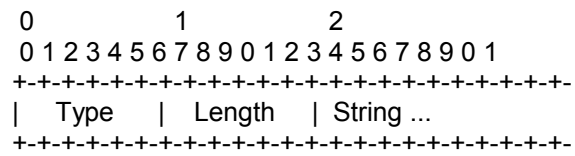
0 Default
1 RADIUS-Request

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.

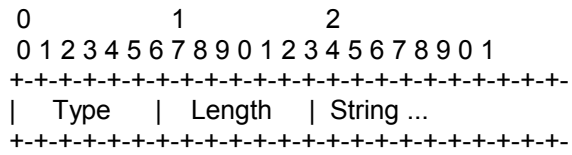
The actual format of the information is site or application specific. Printable ASCII is recommended, but a robust implementation SHOULD support the field as undistinguished octets.

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.



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.

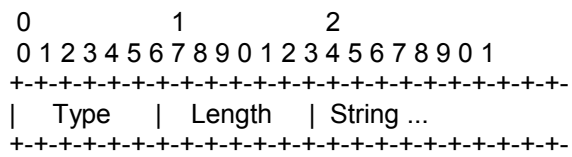
The actual format of the information is site or application specific. Printable ASCII is recommended, but a robust implementation SHOULD support the field as undistinguished octets.

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.



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.

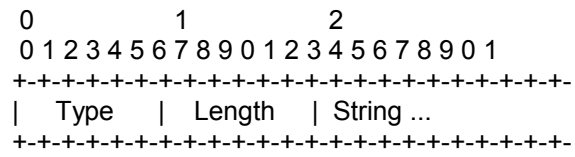
The codification of the range of allowed usage of this field is outside the scope of this specification.

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.



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.

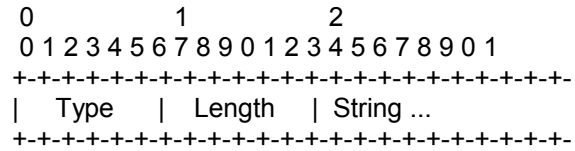
5.34. Login-LAT-Service

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.



Type

34 for Login-LAT-Service.

Length

>= 3

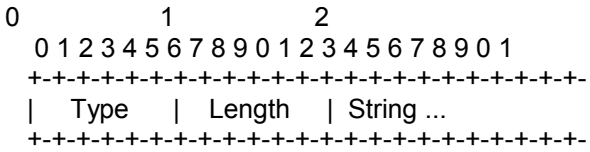
String

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 alphabetics, 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.



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 alphabetics, and the ISO Latin-1 character set extension. All LAT string comparisons are case insensitive.

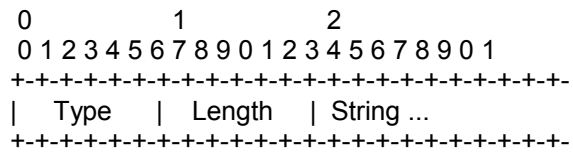
5.36. Login-LAT-Group

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

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

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

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



Type

36 for Login-LAT-Group.

Length

34

String

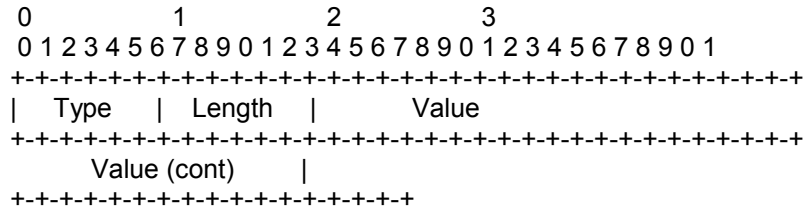
The String field is a 32 octet bit map, most significant octet first. A robust implementation SHOULD support the field as undistinguished octets.

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

5.37. Framed-AppleTalk-Link

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

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



Type

37 for Framed-AppleTalk-Link.

Length

6

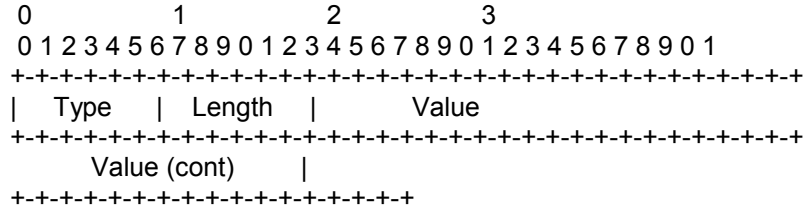
Value

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

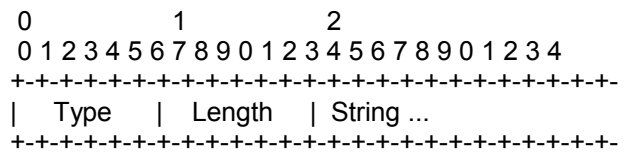
Value

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.



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.

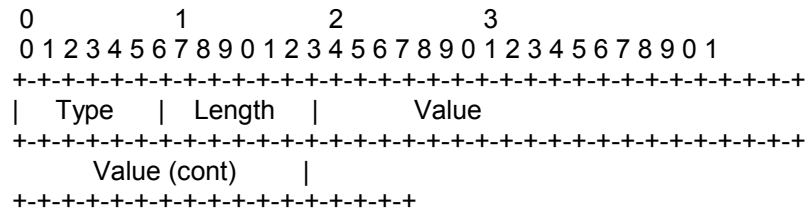
Below you find information from the RADIUS RFC 2139.

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.

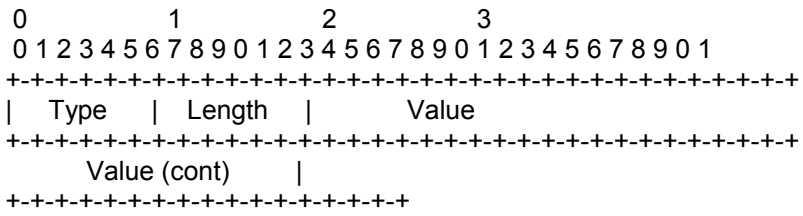
1 Start
2 Stop
7 Accounting-On
8 Accounting-Off

5.2. Acct-Delay-Time

This attribute indicates how many seconds the client has been trying to send this record 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.)

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

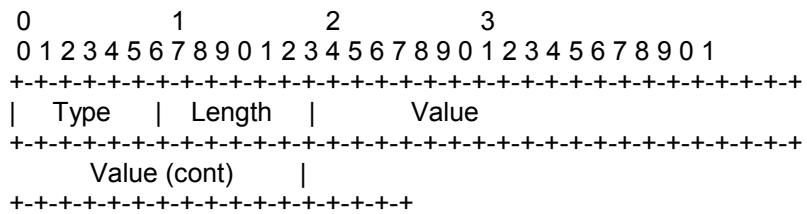
Value

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.



Type

42 for Acct-Input-Octets.

Length

6

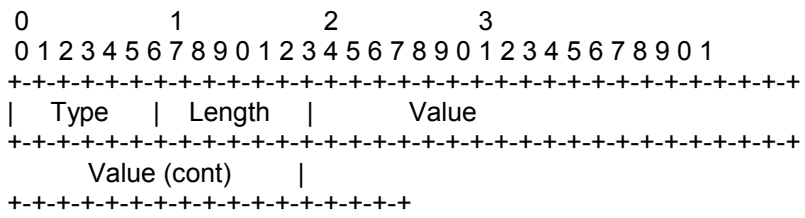
Value

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.



Type

43 for Acct-Output-Octets.

Length

6

Value

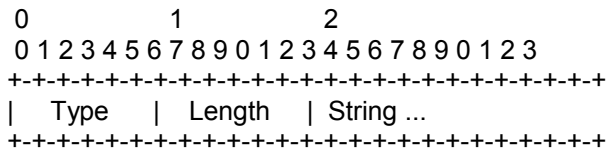
The Value field is four octets.

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.



Type

44 for Acct-Session-Id.

Length

>= 3

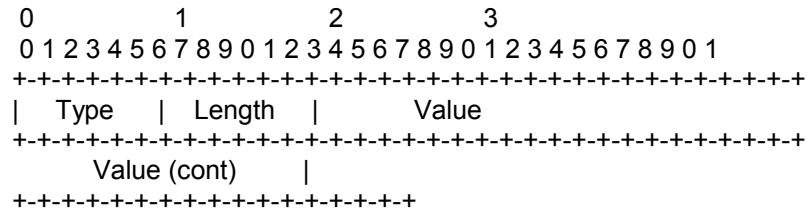
String

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.



Type

45 for Acct-Authentic.

Length

6

Value

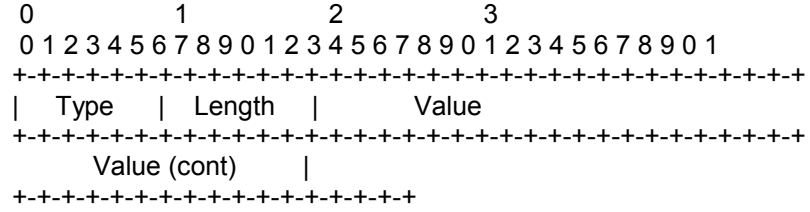
The Value field is four octets.

1 RADIUS
2 Local
3 Remote

5.7. Acct-Session-Time

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

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



Type

46 for Acct-Session-Time.

Length

6

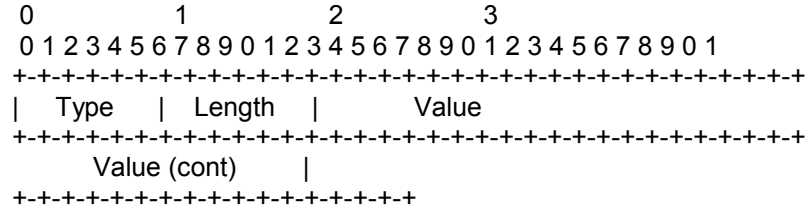
Value

The Value field is four octets.

5.8. Acct-Input-Packets

This attribute indicates how many packets have been received from the port over the course of this 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

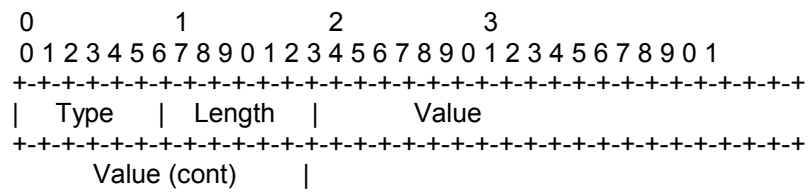
Value

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

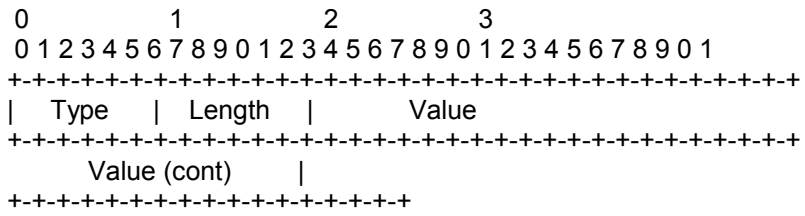
Value

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, 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 which required ending the session.

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

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

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

Port Suspended
NAS ended session to suspend a virtual session.

Service Unavailable
NAS was unable to provide requested service.

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

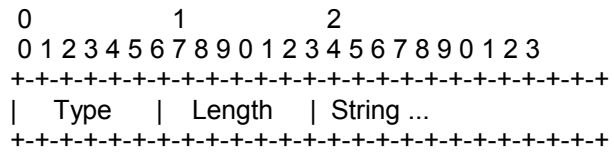
User Error
Input from user is in error, causing termination of session.

Host Request
Login Host terminated session normally.

5.11. Acct-Multi-Session-Id

This attribute is a unique Accounting ID to make it easy to link together multiple related sessions in a log file. Each session linked together 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.



Type

50 for Acct-Multi-Session-Id.

Length

>= 3

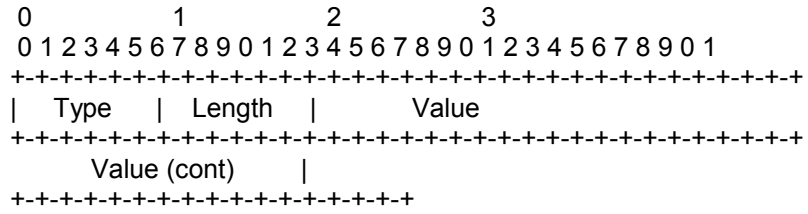
String

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.



Type

51 for Acct-Link-Count.

Length

6

Value

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

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

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

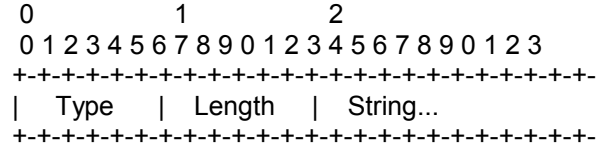
Multi-Session-Id	Session-Id	Status-Type	Link-Count
"10"	"10"	Start	1
"10"	"11"	Start	2
"10"	"11"	Stop	2
"10"	"12"	Start	3
"10"	"13"	Start	4
"10"	"12"	Stop	4
"10"	"13"	Stop	4
"10"	"10"	Stop	4

5.40. CHAP-Challenge

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

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

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



Type

60 for CHAP-Challenge.

Length

>= 7

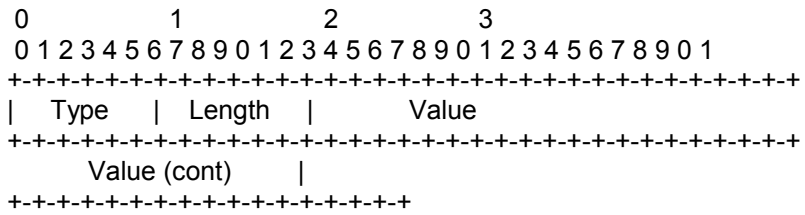
String

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

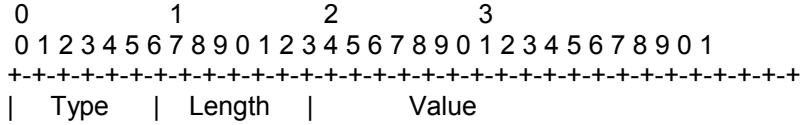
The Value field is four octets. "Virtual" refers to a connection to the NAS via some transport protocol, instead of through a physical port. For example, if a user telnetted into a NAS to authenticate himself as an Outbound-User, the Access-Request might include NAS-Port-Type = Virtual as a hint to the 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 that that 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.



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

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.

```
 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

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 alphabetics, 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.

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

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

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

0 This attribute **MUST** NOT be present in packet.

0+ Zero or more instances of this attribute MAY be present in packet.
0-1 Zero or one instance of this attribute MAY be present in packet.
1 Exactly one instance of this attribute **MUST** be present in packet.

5.13. Table of Attributes

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

RFC 2139 RADIUS Accounting

#	Attribute
0-1	User-Name
0	User-Password
0	CHAP-Password
0-1	NAS-IP-Address [5]
0-1	NAS-Port
0-1	Service-Type
0-1	Framed-Protocol
0-1	Framed-IP-Address
0-1	Framed-IP-Netmask
0-1	Framed-Routing
0+	Filter-Id
0-1	Framed-MTU
0+	Framed-Compression
0+	Login-IP-Host
0-1	Login-Service
0-1	Login-TCP-Port
0	Reply-Message
0-1	Callback-Number
0-1	Callback-Id
0+	Framed-Route
0-1	Framed-IPX-Network
0	State
0+	Class
0+	Vendor-Specific
0-1	Session-Timeout
0-1	Idle-Timeout
0-1	Termination-Action
0-1	Called-Station-Id
0-1	Calling-Station-Id
0-1	NAS-Identifier [4]
0+	Proxy-State
0-1	Login-LAT-Service
0-1	Login-LAT-Node
0-1	Login-LAT-Group
0-1	Framed-AppleTalk-Link
0-1	Framed-AppleTalk-Network
0-1	Framed-AppleTalk-Zone
1	Acct-Status-Type
0-1	Acct-Delay-Time

0-1	Acct-Input-Octets
0-1	Acct-Output-Octets
1	Acct-Session-Id
0-1	Acct-Authentic
0-1	Acct-Session-Time
0-1	Acct-Input-Packets
0-1	Acct-Output-Packets
0-1	Acct-Terminate-Cause
0+	Acct-Multi-Session-Id
0+	Acct-Link-Count
0	CHAP-Challenge
0-1	NAS-Port-Type
0-1	Port-Limit
0-1	Login-LAT-Port

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

The following table defines the above table entries.

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

Appendix B – EMERALD UPDATE

Emerald 2.5 and 2.75 are packaged with Radius Professional version 2.5. Customers whom have upgraded to Radius version 3 (e-mail Sales@iea-software.com) may still use Emerald 2.5 and 2.75. You will need to install Radius version 3 after Emerald has been installed. If you are an Emerald Internet Management Suite user, this section will describe additional steps that will need to be taken in order for the new version of RadiusNT/X to work with your installation.

Update Script for Emerald Users

For those using Emerald 2.5 that are upgrading to Radius version 3, you will need to run the 3.0 SQL Server upgrade script ***emer25_up.sql*** that was included with the distribution archive. To run the script, please do the following:

1. Run the SQL Server ISQLW application (SQL Server 6.5) or the Query Analyzer application (SQL Server 7.0).
2. **Connect** to the server you are using.
3. Click the **Load SQL Script** icon. 
4. Browse to locate the ***emer25_up.sql*** file, then click **Open**. The script is typically in the directory where you installed RadiusNT.
5. Click the **Execute Query** icon. 
6. Close ISQLW.
7. Restart RadiusNT and Emerald.

Configuring ODBC

Quick Tip!	If you are using the Emerald Management Suite, you will need to setup 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, follow these steps:

9. Select Start, Settings and then Control Panel.
10. From the Control Panel, select ODBC32. Please note that if you do not have ODBC installed, you will need to install ODBC 2.5 or higher to proceed. ODBC is shipped with many

applications, and is available from Microsoft's FTP site at ftp://ftp.microsoft.com/developr/ODBC/public/. You can also install ODBC from the SQL Server CD-ROM directory *\i386\odbc*.

11. After the ODBC Administrator opens, select the System DSN button. If your system does not display a System DSN button, you will need to upgrade to at least ODBC 2.5 or higher.

12. Click the Add button.

13. For an Emerald/SQL Server installation, select the SQL Server Driver. For other database types, select the corresponding ODBC driver.

14. For the Data Source Name option, type "**Radius**".

15. Enter "**RadiusNT**" for the Description.

16. Depending on what type of driver you have installed, the next step will vary. Please refer to your database documentation to learn more about configuring an ODBC DSN for your database system.

    - SQL Server
        4. For Server, enter the name of the SQL Server you are using.

        5. Click Options, then Database. Enter the name of the database on your SQL Server that RadiusNT will be accessing. Please note that for Emerald customers, this should be "Emerald".

        6. Leave the Library and Network addresses set to default.

    - MS Access
        2. Click the Select button in the database box and choose your MS Access file. Please note that if you need to login to the database, you will need to select the Advanced option and fill in the required information.

10. Finally, select Save and close the Control Panel.

To configure an ODBC DSN for RadiusX, follow these steps:

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

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

[ODBC Data Sources]
Radius_MSSQL65=RadiusX ODBC Driver

[Radius_MSSQL65]
Driver=/usr/local/radius/lib/E-msss14.so
Description=Radius_MSSQL65
Database=Radius
ServerIPAddress=127.0.0.1
```

ServerPortNumber=1433
LogonID=
Password=
UseProcForPrepare=0
QuotedId=No
AnsiNPW=No

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

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

Database=Radius
This is the name of the database containing your Radius/Emerald database.

ServerIPAddress=127.0.0.1
This reflects the IP address of the SQL Server and must be numeric.

ServerPortNumber=1433
This notates the TCP port that the SQL Server is 'listening' on.

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

6. Begin by changing to the directory where the ***odbc.ini*** file exists, **/usr/local/radius**.
7. Open the ***odbc.ini*** file with a plain text editor.
8. Make the needed changes.
9. When you have completed your changes, be sure to **Save** the file.
10. **Restart** RadiusX.

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

To configure RadiusNT for ODBC operations, follow these steps:

7. While in the RadiusNT Administrator, check ODBC.
8. From the DSN pick list, select the ODBC DSN that you created above. Please note that you **must reload DSNs** to read in the new ODBC DSN that you have created **if** it doesn't appear in the list. In order to do this, select **File**, then **Reload DSNs**.
9. Select the Security tab and enter a Username that you will use for logging into the database.
10. Next, enter a Password in the Password and Verify text boxes.
11. To verify the database connection, click the Check button.
12. Lastly, select File and then Save.

The next step is to configure the database **before** starting RadiusNT.

For those using Emerald, run the Emerald Administrator.

- Select Config Radius
- Select the Servers tab and then
- Add an entry for *each* NAS

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

"radius -x15"

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

Please remember that in order for RadiusNT to work correctly with Emerald, you **must** have already done the following steps:

1. Used the Emerald Administrator to create the Emerald database on your SQL Server.

2. Created an ODBC datasource called Emerald. Please note that it **must** be a 32-bit ODBC system data source and it **must** be pointed to the Emerald database you created.

3. Specified correct login information in the RadiusNT Administrator to allow RadiusNT to login to the SQL Server.

To configure RadiusX for ODBC operations, follow these steps:

The installation process configures most everything that is needed for RadiusX ODBC operations. Should you need to set the database mode or DSN option, please follow the steps below:

7. Change to the directory where the RadiusX Administrator resides, **/usr/local/radius**.

8. Start the Administrator by typing "**perl *radadmn.pl***".

9. At the Main Menu, select the **ODBC DSN** option. This is where you can set DSN options. When completed, select the **Main Menu** option to continue.

10. At the Main Menu, select the **Configuration** option .

11. Next, select the **Database Mode** option. This is where you can set Database Mode options. When completed, select the **Main Menu** option to continue.

12. Select **Exit** to complete the process. Your changes are automatically saved when you exit the RadiusX Administrator.

The next step is to configure the database **before** starting RadiusX.

For those using Emerald, run the Emerald Administrator.

- Select Config Radius
- Select the Servers tab and then
- Add an entry for *each* NAS

In order 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 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" (NT)
"./radiusd –x15" (UNIX)

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

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, which does not exist. RadiusNT will not write any accounting information. You **must** have a *users* file if you have text file mode checked, though. 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 that pertains only to your Emerald installation.

Accounting **Manual Calls Update**	RadiusNT/X will manually update the ServerPorts table. This is only needed for databases that do not have trigger support and 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.

Stored Procedures

Below is a list of the stored procedures that Emerald provides for RadiusNT/X to use. The parameters and returned columns **must** be of the same type, but the stored procedures can be modified to the database design if you are not using Emerald.

```
CREATE PROCEDURE RadCheckServer @rrsid int AS
Select Server, IPAddress, Secret, AuthPort, AcctPort, 0, Timeout, Retries, StripDomain,
TreatAsLocal, NULL
From RadRoamServers
Where RadRoamServerID = @rrsid

CREATE PROCEDURE RadCheckOnline @UserName varchar(64) AS
Select Count(Username) From CallsOnline Where UserName=@UserName and
AcctStatusType=1

CREATE PROCEDURE RadCheckPort @nasid varchar(16), @nasport integer, @at
varchar(15) AS
Select MaxSessionLength, StartTime, StopTime, CurrTime = (DatePart(Hour, GetDate()) *
60) + DatePart(Minute, GetDate())
From Servers s, ServerAccess sa
Where s.ServerID = sa.ServerID AND s.IPAddress = @nasid AND (sa.Port=@nasport or
sa.Port=NULL)
        AND sa.AccountType = @at

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

CREATE PROCEDURE RadGetConfigs @AccountID int AS
Select ra.RadAttributeID, Name, Data, Value, Type, rc.RadVendorID, rc.RadVendorType,
rc.RadCheck
From RadConfigs rc, RadAttributes ra
Where ra.RadAttributeID=rc.RadAttributeID AND rc.AccountID = @AccountID

CREATE PROCEDURE RadUserDefaults AS
```

```
SELECT rc.AccountType, ra.RadAttributeID, ra.Type, rc.Data, rc.Value, rc.RadVendorID,
        rc.RadVendorType, rc.RadCheck
From RadAttributes ra, RadATConfigs rc
Where ra.RadAttributeID = rc.RadAttributeID
Order By AccountType, RadCheck, ra.RadAttributeID

CREATE PROCEDURE RadUserSpecifics AS
SELECT rc.AccountID, ra.RadAttributeID, ra.Type, rc.Data, rc.Value, rc.RadVendorID,
        rc.RadVendorType, rc.RadCheck
From RadAttributes ra, RadConfigs rc
Where ra.RadAttributeID = rc.RadAttributeID
Order By AccountID, RadCheck, ra.RadAttributeID

CREATE PROCEDURE RadAtCache @accounttype VARCHAR(16) AS
SELECT rc.AccountType, ra.RadAttributeID, Name, Data, Value, Type, rc.RadVendorID,
rc.RadVendorType, rc.RadCheck
FROM RadATConfigs rc, RadAttributes ra
WHERE ra.RadAttributeID = rc.RadAttributeID
    AND (ra.RadVendorID = rc.RadVendorID OR rc.RadVendorID IS NULL)
    AND (ra.RadVendorType = ra.RadVendorType OR rc.RadVendorType IS NULL)
    AND (@accounttype IS NULL OR AccountType = @accounttype)
ORDER BY AccountType
GO

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

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

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

```
CREATE PROCEDURE RadGetCacheUsers @date DATETIME, @flag TINYINT AS
SELECT sa.AccountID, sa.Login, sa.Password, d.MailDomain, sa.AccountType,
sa.LoginLimit, sa.TimeLeft,
MasterExpire=DateAdd(Day, ma.Extension+ma.OverDue+1, maExpireDate),
SubExpire=DateAdd(Day, sa.Extension+1, saExpireDate),
OverLimit=CASE WHEN (ma.OverLimit > 0 AND ma.OverLimit > ma.Balance) THEN 1 ELSE
0 END
FROM SubAccounts sa, MasterAccounts ma, Domains d, Groups g
      WHERE sa.CustomerID = ma.CustomerID
      AND d.DomainID = g.DomainID
      AND ma.GroupID = g.GroupID
      AND sa.Active <> 0
      AND ma.Active <> 0
      AND sa.Login <> ''
      AND ((@flag = 1 AND sa.LastModifyDate > @date)
            OR (@flag = 2 AND (sa.LastUsed > @date OR sa.LastUsed IS NULL)))
UNION
SELECT sa.AccountID, sa.Email, sa.Password, d.MailDomain, sa.AccountType,
sa.LoginLimit, sa.TimeLeft,
MasterExpire=DateAdd(Day, ma.Extension+ma.OverDue+1, maExpireDate),
SubExpire=DateAdd(Day, sa.Extension+1, saExpireDate),
OverLimit=CASE WHEN (ma.OverLimit > 0 AND ma.OverLimit > ma.Balance) THEN 1 ELSE
0 END
FROM SubAccounts sa, MasterAccounts ma, Domains d, Groups g
      WHERE sa.CustomerID = ma.CustomerID
      AND d.DomainID = g.DomainID
      AND ma.GroupID = g.GroupID
      AND sa.Active <> 0
      AND ma.Active <> 0
      AND sa.Email <> ''
      AND ((@flag = 1 AND sa.LastModifyDate > @date)
           OR (@flag = 2 AND (sa.LastUsed > @date OR sa.LastUsed IS NULL)))
GO

CREATE PROCEDURE RadGetUser @user VARCHAR(64) , @password VARCHAR(32) AS
SELECT sa.AccountID, sa.Login, sa.Password, d.MailDomain, sa.AccountType,
sa.LoginLimit, sa.TimeLeft,
MasterExpire=DateAdd(Day, ma.Extension+ma.OverDue+1, maExpireDate),
SubExpire=DateAdd(Day, sa.Extension+1, saExpireDate) ,
OverLimit=CASE WHEN (ma.OverLimit > 0 AND ma.OverLimit > ma.Balance) THEN 1 ELSE
0 END
FROM SubAccounts sa, MasterAccounts ma, Domains d, Groups g
     WHERE sa.CustomerID = ma.CustomerID
     AND d.DomainID = g.DomainID
     AND ma.GroupID = g.GroupID
     AND sa.Active <> 0
     AND ma.Active <> 0
     AND sa.Login = @user
     AND (@password IS NULL OR sa.Password = @password)
UNION
SELECT sa.AccountID, sa.Email, sa.Password, d.MailDomain, sa.AccountType,
sa.LoginLimit, sa.TimeLeft,
MasterExpire=DateAdd(Day, ma.Extension+ma.OverDue+1, maExpireDate),
SubExpire=DateAdd(Day, sa.Extension+1, saExpireDate),
OverLimit=CASE WHEN (ma.OverLimit > 0 AND ma.OverLimit > ma.Balance) THEN 1 ELSE
0 END
```

```
FROM SubAccounts sa, MasterAccounts ma, Domains d, Groups g
      WHERE sa.CustomerID = ma.CustomerID
      AND d.DomainID = g.DomainID
      AND ma.GroupID = g.GroupID
      AND sa.Active <> 0
      AND ma.Active <> 0
      AND sa.Email = @user
      AND (@password IS NULL OR sa.Password = @password)
GO
CREATE PROCEDURE RadGetCacheUsers @date DATETIME, @flag TINYINT AS
SELECT sa.AccountID, sa.Login, sa.Password, d.MailDomain, sa.AccountType,
sa.LoginLimit, sa.TimeLeft,
MasterExpire=DateAdd(Day, ma.Extension+ma.OverDue+1, maExpireDate),
SubExpire=DateAdd(Day, sa.Extension+1, saExpireDate),
OverLimit=CASE WHEN (ma.OverLimit > 0 AND ma.OverLimit > ma.Balance) THEN 1 ELSE
0 END
FROM SubAccounts sa, MasterAccounts ma, Domains d, Groups g
      WHERE sa.CustomerID = ma.CustomerID
      AND d.DomainID = g.DomainID
      AND ma.GroupID = g.GroupID
      AND sa.Active <> 0
      AND ma.Active <> 0
      AND sa.Login <> ''
      AND ((@flag = 1 AND sa.LastModifyDate > @date)
            OR (@flag = 2 AND (sa.LastUsed > @date OR sa.LastUsed IS NULL)))
UNION
SELECT sa.AccountID, sa.Email, sa.Password, d.MailDomain, sa.AccountType,
sa.LoginLimit, sa.TimeLeft,
MasterExpire=DateAdd(Day, ma.Extension+ma.OverDue+1, maExpireDate),
SubExpire=DateAdd(Day, sa.Extension+1, saExpireDate),
OverLimit=CASE WHEN (ma.OverLimit > 0 AND ma.OverLimit > ma.Balance) THEN 1 ELSE
0 END
FROM SubAccounts sa, MasterAccounts ma, Domains d, Groups g
      WHERE sa.CustomerID = ma.CustomerID
      AND d.DomainID = g.DomainID
      AND ma.GroupID = g.GroupID
      AND sa.Active <> 0
      AND ma.Active <> 0
      AND sa.Email <> ''
      AND ((@flag = 1 AND sa.LastModifyDate > @date)
           OR (@flag = 2 AND (sa.LastUsed > @date OR sa.LastUsed IS NULL)))
GO

CREATE PROCEDURE RadGetUser @user VARCHAR(64) , @password VARCHAR(32) AS
SELECT sa.AccountID, sa.Login, sa.Password, d.MailDomain, sa.AccountType,
sa.LoginLimit, sa.TimeLeft,
MasterExpire=DateAdd(Day, ma.Extension+ma.OverDue+1, maExpireDate),
SubExpire=DateAdd(Day, sa.Extension+1, saExpireDate) ,
OverLimit=CASE WHEN (ma.OverLimit > 0 AND ma.OverLimit > ma.Balance) THEN 1 ELSE
0 END
FROM SubAccounts sa, MasterAccounts ma, Domains d, Groups g
     WHERE sa.CustomerID = ma.CustomerID
     AND d.DomainID = g.DomainID
     AND ma.GroupID = g.GroupID
     AND sa.Active <> 0
     AND ma.Active <> 0
```

```
    AND sa.Login = @user
    AND (@password IS NULL OR sa.Password = @password)
UNION
SELECT sa.AccountID, sa.Email, sa.Password, d.MailDomain, sa.AccountType,
sa.LoginLimit, sa.TimeLeft,
MasterExpire=DateAdd(Day, ma.Extension+ma.OverDue+1, maExpireDate),
SubExpire=DateAdd(Day, sa.Extension+1, saExpireDate),
OverLimit=CASE WHEN (ma.OverLimit > 0 AND ma.OverLimit > ma.Balance) THEN 1 ELSE
0 END
FROM SubAccounts sa, MasterAccounts ma, Domains d, Groups g
    WHERE sa.CustomerID = ma.CustomerID
    AND d.DomainID = g.DomainID
    AND ma.GroupID = g.GroupID
    AND sa.Active <> 0
    AND ma.Active <> 0
    AND sa.Email = @user
    AND (@password IS NULL OR sa.Password = @password)
GO
```

Microsoft Access

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

RadiusNT/X will internally create all SQL Statements for MS Access. This limits the flexibility of the database design to follow the Emerald layout, but does not limit the power or features of what RadiusNT/X can offer.

A fully working Access 7.0 database is included with the RadiusNT/X distribution. Please use this as a starting point to test or build additional features or options that you would like to use in your installation.

Emerald Integration FAQs

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

  When using RadiusNT/X in conjunction with Emerald, there is no need to configure a license in the RadiusNT/X Administrator. Once you have configured RadiusNT for ODBC mode and it is pointing to your Emerald database, RadiusNT/X uses your Emerald license. Please note that you do need to enter your Emerald license in the Emerald Administrator.

- *Can I setup a backup copy of RadiusNT/X that does not connect to my* Emerald *database?*

  Yes. In order to accomplish this, enter one of your Emerald license keys into the RadiusNTX Administrator. In addition, you may use the Emerald client to export a *users* file from your Emerald database for use in this situation.

- *How can I put my Calls table into another database when I am using* Emerald*?*

Please note that this process requires an **in-depth** working knowledge of Microsoft SQL Server **and** Enterprise Manager.

1. Begin by right clicking over the current Calls table and then select Indexes. This selection shows the number of records and the size of your Calls table. Please use this information below.

2. Create two Database Devices, EmerCallsDev and EmerCallsLog. The first will be based on the size of the Calls table discovered in step 1. Please add additional space for growing capacity. As a general rule, the EmerCallsLogs should be approximately 20% of the size of the EmerCallsDev (ex: example 200mb and 40mb, respectively).

3. Next, create a database named EmerCalls with Data Device EmerCallsDev and Log Device EmerCallsLog. Use the full size of each.

4. Use SQL EM to revoke INSERT permissions for RadiusNT/X on your current calls table. This will prevent Radius from writing to Calls during the transfer.

5. You will use SQL EM to transfer your Calls table from your Emerald database to your EmeraldCalls database. Please note that you will transfer **just** the Calls table, **not** the whole database.

6. In Manage Logins (SQL EM), give each Emerald user 'permit' permission for the EmerCalls database (public group). Under the EmeraldCalls database, select 'groups/users' and 'public', then right click to select permissions. Select 'grant all', 'set' and finally 'close'.

7. Next, right click over the **new** Calls Table (in the EmerCalls database) and select Triggers. Cut and then paste the following information in as the trigger:

```
CREATE TRIGGER calls_insert ON dbo.Calls
FOR INSERT
AS
    UPDATE Emerald..ServerPorts
        Set sp.UserName = i.UserName,
            sp.AcctStatusType = i.AcctStatusType,
                    sp.CallDate = DateAdd(Second, 0-i.AcctDelayTime, i.CallDate),
                    sp.FramedAddress = i.FramedAddress,
                    sp.ConnectInfo = i.ConnectInfo
        FROM Emerald..Servers s, Emerald..ServerPorts sp, inserted i
        WHERE s.IPAddress = i.NASIdentifier AND
                    s.ServerID = sp.ServerID AND
            sp.Port = i.NASPort AND
                    DateAdd(Second, 0-i.AcctDelayTime, i.CallDate) >= sp.CallDate

    UPDATE Emerald..SubAccounts
        Set sa.TimeLeft = sa.TimeLeft - (i.AcctSessionTime/60 + 1)
        FROM Emerald..SubAccounts sa, inserted i
        WHERE sa.login = i.UserName
                    and sa.TimeLeft <> NULL
                    and i.AcctStatusType = 2
GO
```

7. Finally, in your Emerald Database, drop the Calls table and create a view as follows.

```
CREATE VIEW Calls AS
Select * From EmerCalls..Calls
```

```
GO

GRANT  SELECT ,  INSERT ,  DELETE ,  UPDATE  ON dbo.Calls  TO Emerald
GO
```

Please note that some call records will probably be lost unless you do this during a 'slow' period. Also, there may be users that show as being on-line for a while that you may have to manually clear.

Glossary

Term	Definition
A	
AAA	Authentication, Authorization and Accounting. A methodology for securing remote access to networks. AAA requires user identification and can restrict access to only specific network resources. It also maintains usage records for billing and network audits.
Accounting	A method of tracking a remote users calls. The accounting data can include such information as a user's login, 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 services that the operating system makes available to the programs. It usually includes a set of routines, protocols and tools. Compared to a Graphical User Interface (GUI), the 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. Rather 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.
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	FAQs are documents that list and answer the most common

Questions (FAQs)	questions on a particular subject.
File Transfer Protocol (FTP)	A very common method of moving files between two systems based on the File Transfer Protocol.
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 researches 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 (ex: 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: The act of entering into a computer system.
M	
Maximum Transmission Unit (MTU)	The largest frame or packet that can be sent through a port on a NAS without fragmentation.
N	
Name Server	A server that resolves host names into network addresses.
Network Access Server(s) (NAS)	A server in a network dedicated to authenticating users that log on.
Network	Two or more computers connected together so that they can share resources. If you connect 2 or more networks together, 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.
R	
Relational DataBase Management System (RDBMS)	A database organization method that links files together 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 another device or server that establishes 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 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 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 that connects to the network.