RadiusNT

The Ultimate RADIUS Server
Version 2.5

Emerald Management Suite

IEA Software, Inc.

Software License Agreement

By purchasing or installing all or part of the Emerald Management Suite, 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 the Emerald Management Suite (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 decompile, 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. 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 Ageement, your license will be revoked.

Updates and Support All software updates are available via the IEA Software, Inc. web site. A maintenance contract is available for major version upgrades, which is not included or covered as part of the basic purchase agreement. Technical support is available via E-Mail, support mailing lists, or a purchased telephone support contract.

Trademarks IEA Software, Inc., Emerald, RadiusNT, 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. Suite 326, West 422 Riverside 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.

Should you have any questions concerning this license agreement, please contact IEA Software, Inc. at Suite 330, West 422 Riverside Spokane, Washington 99201 U.S.A. (509) 444-2455.

Trademarks

Emerald Management Suite and *RadiusNT* 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.

Credits

Programming by Dale E. Reed Jr., Peter Deacon, Jeff Holden
Documentation by Dale E. Reed Jr., Sheryl Stover, Jeff Presley
Tech Support by Kurt White, Sheryl Stover, Su Lan Presley, Dale E. Reed Jr.
Special Thanks to the rest of the IEA Software team.

Table Of Contents

Preface

RADIUS stands for Remote Authentication Dial-in User Services. RadiusNT is a RADIUS based security server used to handle authentication and accounting from RADIUS supported network access servers (NAS) or terminal servers. The RADIUS protocol, invented by Livingston Enterprises is now an RFC for Authentication, and an Informational RFC for Accounting.

This document is not intended to be technical about RADIUS. Technical RADIUS documentation is available from the RADIUS *client* (or NAS) you are using with RadiusNT (the RADIUS *Server*). Please browse your client information before attempting to install RadiusNT if you are not familiar with RADIUS.

The RadiusNT files are available from ftp.iea-software.iea.com. All updates will be available from there as well as the web site at www.iea-software.com.

About RADIUS

The RADIUS protocol was designed to solve the problem of centralized authentication and accounting from multiple, possibly heterogeneous, network access servers (NAS).

The RADIUS design allows for a server, RadiusNT, to accept authentication and accounting requests from a RADIUS client (NAS or Firewall). Typically there are two steps involved. In the first step the client sends a request to the server. In the second step, the server processes the request and sends a reply 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 for the request, including user service information, messages, and many other attributes of the calls or accounting information.

Most RADIUS clients can be configured to use an alternate RADIUS server in the event the primary RADIUS server does not respond. This allows for fail safe operations in larger networks or can be used to created a farm of RADIUS servers for a distributed implementation.

RadiusNT has very similar characteristics to most UNIX RADIUS servers, including basic Authentication and Accounting capabilities. RadiusNT also stands out among RADIUS servers, providing a multitude of powerful features and options. The most striking feature of RadiusNT is the extensive Relational DataBase Management System (RDBMS) interface available via Open DataBase Connectivity (ODBC). Because of the power of the database, RadiusNT can be enhanced by adding fields and tables and rules to the database at any time. Now instead of a RADIUS which simply authenticates based on Username/Password, RadiusNT can authenticate based on username/password/time online/port access and additional rules as configured by the Administrator.

With over three years of experience and real-world feedback, RadiusNT is the number one recommended RADIUS server on the Windows NT platform.

RadiusNT Editions

RadiusNT has two editions for stand-alone operations and works with three editions of the Emerald Management Suite. RadiusNT Enterprise includes advanced features that the lite or standard versions of RadiusNT or Emerald may not include. Some options may also be restricted by limitations of the database system RadiusNT is using in ODBC mode. Many advanced options are only available in ODBC mode as well.

Below is a breakdown of options available only in the Enterprise editions. Please see the chapter on Enterprise Features for further details on each one.

RadiusNT Enterprise Edition

- RADIUS Proxy and Roaming
- SNMP Support

Emerald Enterprise Edition

- Dual Mode Authentication
- RADIUS Proxy and Roaming
- SNMP Support

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 the expiration date or a balance/limit combination.

1. Installation

To install RadiusNT, run *setup.exe* from the distribution archive. This will walk you through installing RadiusNT into a directory. You should change the installation directory to *c:\radius* in most cases. We recommend using this directory for all first time installations of RadiusNT.

> ***The archive uses long file names, and so you should use an archive utility that supports long file names. Such an example is the WinZIP program (www.winzip.com). If you do not have such an archiver, then you will need to rename the following files:***
>
> | | |
> |---|---|
> | ***dictiona*** | ***dictionary*** |
> | ***clients.exe*** | ***clients.example*** |
> | ***users.exe*** | ***users.example*** |

Once the setup program has completed, you are now ready to configure RadiusNT for you environment.

Configuration

Configuration of RadiusNT should be performed primarily through the RadiusNT Administrator. When you complete the setup, an icon is created in the RadiusNT group for the Administrator. To start the RadiusNT Administrator, double click on the icon.

The other way to configure RadiusNT is via the command line options. This is not recommended however, unless you are trying to debug a problem. The settings of the RadiusNT Administrator are stored in the registry, while the command line options are only good for that specific instance of RadiusNT.

The following sections will detail information about the RadiusNT Administrator, command line options and registry settings.

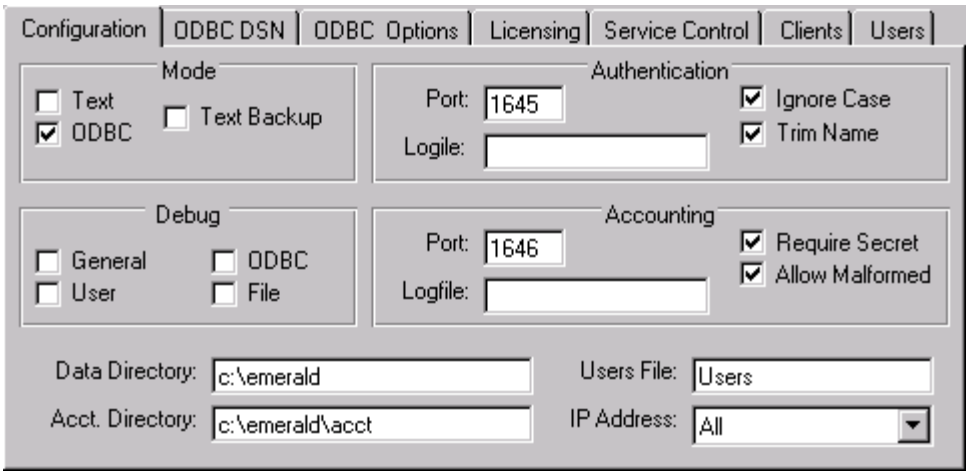
RadiusNT Administrator

The RadiusNT Administrator (radadmn.exe) has seven different areas: Configuration, Directories, and ODBC Security, Licensing, Service Control, Clients, and Users. You can freely move between each tab by selecting it from the top.

> ***You must save the information and options you have configured in the RadiusNT administrator by selecting the File…Save pull down menu option. If you simply exit, the settings will not be saved.***

Below is a short explanation of each option available in the RadiusNT Administrator. Some of these options are explained in more detail in later sections.

Configuration

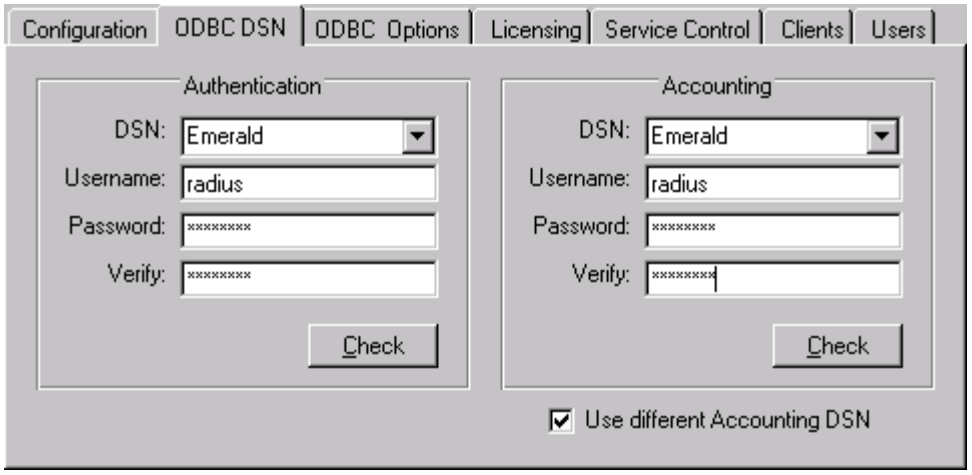


Option	Description
Mode	
Text	RadiusNT will read the users, clients, and dictionary file to retrieve all standard information. If ODBC mode is enabled as well as text mode, the only text file which will be read is the users file, and accounting will be stored in addition to the database, in the detail files. All other configuration (dictionary, clients, etc.) will be read from the ODBC database.
ODBC	RadiusNT will try and attach to a database via the ODBC Data Source Name (DSN) specified in the DSN list. If ODBC is enabled RadiusNT will retrieve all standard information (dictionary, clients, users, etc.) from the ODBC database and will not use the text files. Accounting will also be stored in the ODBC database, rather than the text files.
Debug	
General	General information about the operations of RadiusNT, 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	When authenticating a user name and password RadiusNT is normally case sensitive. If this option is enabled, RadiusNT will make case in-sensitive compares for authentication.
Trim Name	When enabled, this will cause RadiusNT to trim spaces before and 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).
Port	The port RadiusNT will listen for Authentication requests on. The default port is 1645 for RADIUS authentication.
Accounting	
Require Secret	Require Accounting packets to be signed This option is rarely needed, and should normally be left un-checked.
Allow Malformed	A RADIUS attribute with length two or less is usually considered to be a

	malformed packet. Enabling this option will allow RadiusNT to accept attributes with a length of two or more.
Proxy	If you have an Enterprise license for RadiusNT, this will enable proxy support for Accounting. See Chapter 9 for more information about proxy.
Port	The port RadiusNT will listen for Accounting requests on. The default port is 1646 for RADIUS accounting.

Data Directory	If text files mode is checked, this is the directory where RadiusNT will look for the configuration files (dictionary, users, clients, etc.). For RadiusNT to run as a service, this must be a fully qualified path. If you are using ODBC mode, this is where RadiusNT will write the log file.
Accounting Directory	If text files mode is checked, this is the base directory where RadiusNT will create the accounting directories (one per NAS) and detail file. This directory must exist or RadiusNT will not be able to save accounting information. For RadiusNT to run as a service, this must be a fully qualified path.
Users File	If text files mode is checked, this is the file name RadiusNT will try and read the users information out of. This file must be present in the **data directory**.

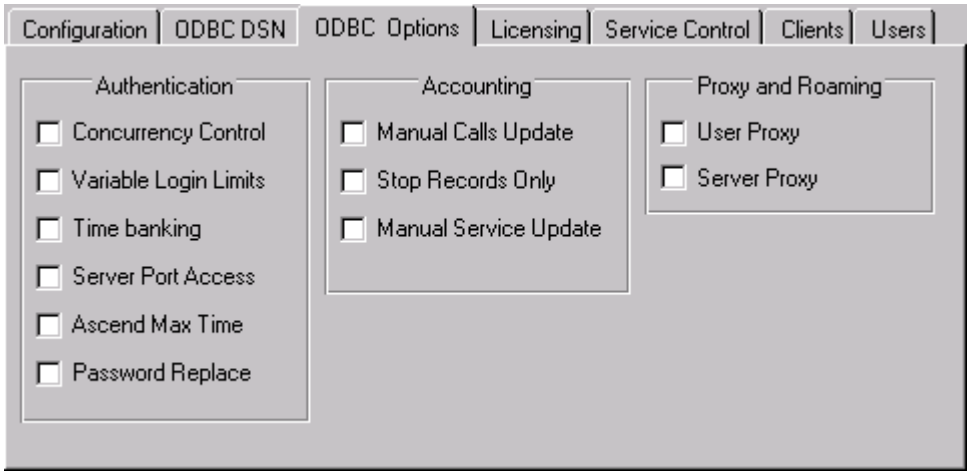
ODBC DSN



Option	Description
Authentication	
DSN	The ODBC DSN RadiusNT will use to connect to the ODBC database.
Username	The username RadiusNT will log into the ODBC database as.
Password	The password for the database user.
Verify	Verification of the password for the database user.
Check	Use the check button to verify the DSN settings are correct.
Accounting	
DSN	The ODBC DSN RadiusNT will use to connect to the ODBC database.
Username	The username RadiusNT will log into the ODBC database as.
Password	The password for the database user.
Verify	Verification of the password for the database user.
Check	Use the check button to verify the DSN settings are correct.

Use Different Accounting DSN	Check this option if you would like RadiusNT to use a different ODBC DSN or set of credentials for the Accounting thread, rather than those specified by the Authentication set.

ODBC Options



Option	Description
Authentication	
Concurrency Control	RadiusNT can restrict users from logging in more than one time if enabled. This requires a properly working callsonline view/query to work. If variable login limits is not enabled, then the limit is one time. If variable login limits is enabled, then the limit is taken from the login limit field.
Variable Login Limits	When concurrency is enabled, by default RadiusNT only lets the user on one time. With this enabled the LoginLimit of the user is respected and the user is allowed to concurrently login the number of times the LoginLimit field specifies.
Time banking	Enables time banking. If the time left field is not NULL, then RadiusNT will restrict the call to the length of time in the timeleft field. *A special case for MS Access is required, where this field should be set to -9999 if the user does not have a time restriction and you enable this option.
Sever Port Access	Enabling this option allows RadiusNT to restrict who can connect to a port based on access information. See Advanced options in Chapter 9 for more details.
Ascend Max Time	Instructs RadiusNT to use the Ascend-Maximum-Time RADIUS attribute rather than the Session-Timeout attribute for time banking.
Password Replace	When using external password authentication (“UNIX” and “WINNT” for the password), RadiusNT can replace the database password with the password the user entered as long as the password was authenticated using the PAP protocol.
Accounting	
Manual Calls Update	RadiusNT will manually update the calls online view. This is only needed for databases which do not have trigger support This is not needed with Emerald/SQL Server or an active database which can update the calls online view automatically.
Stop Records Only	RadiusNT usually stores both start and stop records in the database. With this option enabled, RadiusNT will not store start records in the database, but will

	perform a manual update to the serverports table to track calls online.
Manual Service Update	RadiusNT will manually update the user's information in order for time banking to work. This is not needed with Emerald or an active database that can update the subaccounts table automatically.

Proxy and Roaming	
User Proxy	If you have an Enterprise license for RadiusNT, this will enable user based proxy. See the Chapter 9 for more information about Proxy.
Server Proxy	If you have an Enterprise license for RadiusNT, this will enable server based proxy. See the Chapter 9 for more information about Proxy.

Licensing

Option	Description
Company	License Key Company Name
License	RadiusNT License Key

Service Control

Option	Description
Install Service	Install RadiusNT as a service. The radius.exe file must 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

Option	Description
Edit Window	Clients which can make requests to RadiusNT. See chapter x 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

Option	Description
Edit Window	User list for RadiusNT to authenticate from.. See chapter 2 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

2. Modes

User and Configuration Modes

RadiusNT can run in three different modes. Depending on which mode RadiusNT is configured for, it can give different results. Each mode also has different advantages as well.

> **If you are using the *Emerald Management Suite*, you will need to setup RadiusNT in ODBC mode. The ODBC DSN should point to the Emerald database you created with the Emerald Administrator.**

Text Mode

Running RadiusNT in text mode is the simplest way to authenticate users. When RadiusNT starts, it will read in the list of users, clients, and dictionary. If you change any of the files, you must stop and re-start RadiusNT in order for it to notice the changes. Follow these simple steps to run RadiusNT in text mode:

1. Create the accounting directory specified in the administrator.

2. Copy the clients.example to clients. You can rename it, although copying is preferred.
3. Edit the clients file. Replace portmaster1 with the IP address of your NAS (terminal server). DO NOT USE THE DNS NAME YET. Later you can change this to the DNS name if desired.
4. Change the testing123 to a secret. This can NOT have spaces in the secret. Choose something from 4-10 characters. CASE IS IMPORTANT. Remember this, as you will need to use it again in a later step when you configure your NAS.
5. Save the clients file.
6. Create the file: users. Copy the following four lines to this file. YOU MUST use an editor that will preserve the tab between test and Password. A good editor to use is PFE32, but not edit or notepad. 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
   ```

   Make SURE 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. CASE is also significant.

7. Save the users file. (Later you can look at the file users.example to get ideas of more complex user entries).
8. Start up a command prompt and change to the directory where RadiusNT is installed.
9. Execute the following command to start RadiusNT in full debug mode:

   ```
   radius -x15
   ```

RadiusNT will complain if something is not configured correctly. If everything goes well, you will see a final line "waiting for requests". At this point you can minimize the DOS windows and continue to the Terminal Server Configuration section.

ODBC Mode

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

RadiusNT's ODBC layout is based on the database layout of Emerald. With a little understanding of databases, you can easily setup RadiusNT to work with any database system. An example MS Access 7.0 database is included in the RadiusNT distribution with forms and example data already created.

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

1. From the Control Panel, select ODBC32. If you do not have ODBC installed, then you will need to install ODBC 2.5 or higher. ODBC is available with many applications, as well as directly from Microsoft's FTP site (ftp://ftp.microsoft.com/developr/ODBC/public/). You can also install ODBC from the SQL Server CD-ROM directory *\i386\odbc*.
2. When the ODBC Administrator comes up, select the system DSN button. If you do not have a System DSN button, you will need to upgrade to at least ODBC 2.5 or higher.
3. Click the Add button.
4. For an Emerald/SQL Server installation, select the "SQL Server" Driver. For other database types, select the appropriate ODBC driver for your database.
5. For the Data Source Name, enter "Radius".
6. For the description enter "RadiusNT"
7. Depending on what type of Driver you install, this step will vary. You may have to look at your database documentation to find out more information on configuring an ODBC DSN for your database system.

    - SQL Server
        For the server, enter the name of the SQL Server.
        Click on options and for the Database, enter the database on your SQL Server that RadiusNT will be accessing. For Emerald customers, this should be "Emerald". You should leave library and network address set to default.
    - MS Access
        In the database box, click the select button and choose your mdb file.
        If you need to login to the database, select advanced and fill in the information.

8. Select save and close the control panel.

To configure RadiusNT for ODBC operations, follow these steps:

1. In the RadiusNT Administrator check ODBC.
2. From the DSN pick list, select the ODBC DSN you created above. You must restart the administrator to read in the new ODBC DSN you created (if it doesn't appear in the list).
3. Click on the security tab and enter a username to log into the database as.
4. Enter the password in the password and verify text boxes.
5. Click on the Check button, if you want to see if the database connection succeeds.
6. Select File..Save to save the settings.

At this point you need to configure the database before starting RadiusNT. For Emerald, run the Emerald Administrator, select Config Radius, and go to the servers tab. Add an entry for each NAS. In order to finish the test you will also need to create an MBR/service with the Emerald client as well.

For all others, 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 calls online to work, you also need to populate the ServersPorts table.

Before going to the testing section, start RadiusNT by:

1. Start up a command prompt and change to the directory where RadiusNT is installed.
2. Execute the following command to start RadiusNT in full debug mode:

    radius -x15

RadiusNT will complain if something is not configured correctly. If everything goes well, you will see a final line "waiting for requests". At this point you can minimize the DOS windows and continue to the Terminal Server Configuration section.

In order for RadiusNT to work with Emerald, you must have already:

1. Used the Emerald administrator to create the Emerald database on your SQL Server.
2. Created an ODBC datasource called Emerald. 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.

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 starts. RadiusNT will attempt to locate the user in the ODBC database first. If the user is not found, then RadiusNT will search its copy of the users file in memory for the user.

For accounting, RadiusNT 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, just create an empty users file, and RadiusNT will work fine.

Thread Modes

RadiusNT can run in one of two thread modes. By default RadiusNT will spawn a thread to handle authentication requests and another thread to handle accounting requests. If RadiusNT is in ODBC mode, it will open up a connection for each thread as well. This dual thread design gives RadiusNT very high performance. You can configure RadiusNT to use a single thread to handle all authentication and accounting requests. If RadiusNT is in ODBC mode, it will only open one connection to the database.

RadiusNT does not spawn a new thread for each request that is received like many other RADIUS servers do. The overhead of spawning a thread for every request can be very resource consuming and allows a RADIUS client to overload the RADIUS server and machine it is running on. The single thread design of RadiusNT offers optimal performance without the threat of overloading the machine RadiusNT is running on or possibly the backend database server RadiusNT is connected to.

RadiusNT may also use additional threads for background management. These can include service and file management.

3. Terminal Server Configuration

RadiusNT can interact with many different RADIUS clients simultaneously, even if they are from different vendors. The following are several of the more popular NAS vendors and sample configuration information for their 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 type these commands in:

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 NT machine which you have RadiusNT running on and yyyyy is the secret which you entered for THIS NAS in the clients file or ODBC database. Remember the secret is case sensitive and MUST match exactly.

Ascend MAX and Pipeline

Configure the device in the menu system as below. The configuration menus may vary slightly based on what version of the OS software you are using.

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 NT machine which you have RadiusNT running on and yyyyy is the secret which you entered for THIS NAS in the clients file or ODBC database.

Other RADIUS compatible NASes

Basically you need to configure these settings:

Authentication and Accounting to RADIUS
Authentication and Accounting servers to the Radius NT server's IP Address
Authentication and Accounting secrets the same as in the users file or ODBC database.
Authentication and Accounting ports to 1645 and 1646, respectively.

You should also check the RadiusNT Technology Partners page for links to vendor configuration and RADIUS information specific to that vendor. You can find that page at the following URL:

http://www.iea-software.com/radiusnt/techpartners.html

4. Testing RadiusNT

You can test RadiusNT by dialing into your NAS and trying to login as a user you have configured in either the users file or the ODBC database. If everything is successful you should get a successful authentication response from RadiusNT and your NAS. At this point you can install RadiusNT to run as a service and startup automatically.

Radlogin

Sometimes it is desirable to test RadiusNT or accounts without going through the trouble of dialing into a RADIUS client. Included with RadiusNT is a program called radlogin that can make authentication and accounting requests to a RADIUS server.

To use radlogin, you must setup configure RadiusNT to accept requests from the machine which is running radlogin, just as if radlogin was a terminal server itself. If radlogin and RadiusNT 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 in text mode, edit your clients file to look be 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 tells RadiusNT that requests can come from the localhost using a secret of "localhost". If you are running RadiusNT in ODBC mode, you will need to add a similar entry to your servers table.

Note: You must restart RadiusNT 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, your server entry will look just like the line you added to your clients file above. See below for an example server file entry.

```
127.0.0.1 localhost
```

Only the first line of the server file is read. All other lines are ignored. Now that you have all the components configured, open up a command prompt and change to the directory you installed RadiusNT into (typically C:\radius).

The radlogin program can take two or three parameters. If you type radlogin by itself, it will show you the command line options:

```
Radlogin RADIUS test client for RadiusNT
Copyright 1996-1998 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, type radlogin followed by a username and password. You may need to put quotes around the username or password if they include a space. By default radlogin will return a verbose result of whether the request was acknowledged or not, and any attributes RadiusNT returned. Optionally you can include a number as the third parameter to send multiple, sequential tests (to check performance). At the end RadiusNT will summarize the requests and give an average response time.

Accounting Test

To send an accounting request to RadiusNT, 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 of whether the request was responded to and any attributes RadiusNT returned. Optionally you can include a number as the third parameter to send multiple, sequential tests (for check performance). At the end RadiusNT will summarize the requests and give an average response time.

Trouble Shooting

More detailed trouble shooting and Frequently Asked questions are available in Chapters 10 and 11. If your test is not successful, there are a couple of quick checks you can make:

1. If you do not see the authentication request on the RadiusNT screen, your NAS is not setup correctly and is not sending the RADIUS requests to RadiusNT. Check the NAS RADIUS configuration and make sure RadiusNT is listening on the same port the NAS is sending the request to.
2. If you see the request on the RadiusNT screen, but RadiusNT prints an error "security breach", then the request was received from an IP address which is not authorized to send RADIUS requests to RadiusNT. Check the clients file or the ODBC Database Servers tables to make sure the NAS making the request is listed with the proper information (and that you have restarted RadiusNT if you changed the client information).
3. If you get an Address mismatch error, then you have DNS problems. This means RadiusNT received a request from IP address x.x.x.x. When RadiusNT looked up the 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.
4. If RadiusNT 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 table: Servers.

5. RadiusNT as a service

RadiusNT runs natively as a service. If you try to run it from the DOS prompt without the -x command line option, RadiusNT will try to start as a service, fail, and return to the command prompt.

Installing the service

To install RadiusNT as a service follow the steps below:

1. Open the RadiusNT administrator and change to the Service Control tab.
2. Select the Install Service button.

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

1. Open a command prompt and change to the directory where RadiusNT resides (typically *c:\radius*).
2. Execute the command "Radius.exe -install". You can not leave off the .exe or the installation will not work. If everything goes well, you will see a note about the service being installed. If it doesn't work, troubleshooting steps begin with the –x15 command line option and continue through ensuring that services can interact with the desktop, and that the userid RadiusNT is running as for a service has the proper authentication to access the DSN datasource.

Removing the service

To remove the RadiusNT service follow the below steps:

3. Open the RadiusNT administrator and change to the Service Control tab.
4. Select the Remove Service button.

To manually remove the RadiusNT service follow the below steps:

3. Open a command prompt and change to the directory where RadiusNT resides (typically *c:\radius*).
4. Execute the command "Radius.exe -remove". If everything goes well, you will see a note about the service being removed.

Service considerations

You can use the Control Panel, Services applet to start and stop the RadiusNT service. If for any reason the service can not start, run RadiusNT from a DOS prompt with the -x15 option. In most cases it will tell you why RadiusNT can not start, so that you can fix the problem.

You can also use the Control Panel, Services applet to configure the service to startup automatically when the computer is booted. This is highly recommended and the default installation option.

6. External Authentication

UNIX passwd file

RadiusNT can authenticate from a UNIX passwd or spasswd file, very similar to how UNIX RADIUS servers do. In order to tell RadiusNT to authenticate the user from the passwd file, you need to make the user's password "UNIX". Case is significant. When RadiusNT finds a password of "UNIX" it will look for a file called "passwd" it its current directory. This file must match the format of a passwd file from a standard UNIX machine. The user's password is one-way encrypted and compared to their entry in the passwd file. If no entry is found, the user is not authenticated.

This works for both ODBC and text file user entries. A special option can be enabled in ODBC mode to allow RadiusNT to replace the "UNIX" password with the user's actual password they typed in during authentication (if the passwords match). This 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. See the section on RadiusNT Registry entries for more details.

A sample users file entry would be (Remember Case is VERY important):

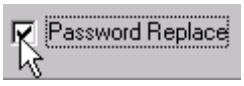
```
name    Password = "UNIX"
        User-Service = Framed-User

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

Windows NT SAM Support

RadiusNT can authenticate from Windows NT SAM as well. In order to tell RadiusNT to authenticate the user from the Windows NT SAM, you need to make the user's password "WINNT". Case is significant. When RadiusNT finds a password starting with "WINNT" it will look to see if there is a "\" following the password. If there is, and it is NOT the last character, then it will use whatever follows the \ as the NT Domain for the user. If the Password is just "WINNT" or "WINNT\" then the local user database is used to authenticate to user (assuming RadiusNT is running on a non-Domain Controller).

In order for RadiusNT to authenticate users from the NT SAM, RadiusNT must run as a user with sufficient rights. You can modify user rights in the Windows NT user manager. You can also specify who RadiusNT will login as when it runs as a service in the Control Panel, Service applet.

This works for both ODBC and text file user entries. A special option can be enabled in ODBC mode to allow RadiusNT to replace the "WINNT" password with the user's actual password they typed in 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. See the section on RadiusNT Registry entries for more details.



A sample users file entry would be:

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

If you are running RadiusNT in text mode, you can use the DEFAULT user entry to look in the NT SAM for the usernames and passwords. To do this, create an entry at the end of the users file like this:

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

The \DOMAIN is optional and should either be removed or changed to the default domain to authenticate against.

NT SAM Permission Requirements

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

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

If you try to authenticate against the NT SAM and RadiusNT gives the error message "RadiusNT does not have sufficient rights to authenticate against the NT SAM", then there is a permissions problem with the account RadiusNT is running as. If you will be 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. The system user on a stand-alone NT server or workstation does not have sufficient rights to authenticate against the domain.

7. Command Line and Registry Settings

RadiusNT can take a variety of command line options. Typically you will only use these if you are trying to debug a problem or test a configuration. All command line options can also be specified in the registry as permanent options.

Warning: Changing values in the registry for Windows NT can cause the system to become unstable or 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:

HKEY_LOCAL_MACHINE\Software\IEA\RadiusNT

To add parameters to RadiusNT via the registry, you need to add the values below to the RadiusNT key. Command line options will override registry defaults.

For example to set the default MODE for RadiusNT, you would add the value named:

HKEY_LOCAL_MACHINE\Software\IEA\RadiusNT\Mode

as 1 for ODBC, or 2 for BOTH. 0 is the default of text mode.

RadiusNT only reads the registry values at startup. If you change a value, you must re-start RadiusNT in order for the change to take affect.

Listing

Following is a list of all Command Line Options and Registry values, with descriptions, currently supported by RadiusNT.

Command Line	Registry	Description
-a [path]	AcctDirectory	Specify the accounting directory. Default is \radius\acct. Inside this directory will be a directory for each NAS that sends accounting requests to RadiusNT. An accounting file called "detail" will be in each NAS directory, which contains all the accounting information.
-A	ReqAcctAuth	Tells RadiusNT to require Accounting packets to have the secret appended to them. Otherwise any valid accounting packet from a NAS in the clients file or servers table is allowed.
-d [path]	DataDirectory	The directory where RadiusNT reads the users, clients, dictionary, and passwd file from.
-E	EncryptPasswords	RadiusNT will use the UNIX crypt one-way encryption to check the passwords in either the database or the users file. If you only want a few users to support this, use the "UNIX" passwd type from a UNIX passwd file. Only advanced users should use this option as it can prevent users from authenticating if used incorrectly.
-I[#]	IgnoreCase	Ignore case when comparing username and password. –I by itself specifies both username and password case insensitive compares. By specifying a number, RadiusNT can compare the username (1) or password (2) only.
-M[#] -o or –b	Mode	RadiusNT defaults to text mode, where it will read all configuration files from text files. -o or -b tells RadiusNT to connect to an ODBC database to read all configuration information and authenticate users from the database. -b allows RadiusNT to authenticate from both the users file and the database (the database is checked FIRST). It will also send accounting to both. The –M parameter allows you to set text mode (0), ODBC (1), or both (2).
-n [DataSource]	ODBCDataSource	If in ODBC mode (-o or -b), RadiusNT will use the specified ODBC DataSource Name rather than the default of "radius".
-p0 [port]	AuthPort	The ports to listen for Authentication requests on. Defaults to the port specified in the RadiusNT Administrator, or 1645.
-p1 [port]	AcctPort	The ports to listen for Accounting requests on. Defaults to the port specified in the RadiusNT Administrator, or 1646.
-P[#]	Proxy	If you have an Enterprise License, this allows Authentication and Accounting proxy. You can enable just authentication (1) or accounting (2). The default is both.
-R[#]	Options	Set many flags or options of RadiusNT, mostly dealing with concurrency control. Add up all options you wish to use: 1 Concurrency Lockout 2 Manual CallsOnline Update 4 Enable Time banking 8 Manual SubAccounts Update 16 MS Access Mode 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

		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	SingleThread	Use the same thread for Authentication and Accounting rather than spawn a new thread and database connection for each.
-S	ExtSupport	External Authentication support.
-T	ProxyTimeout	If you have an Enterprise License, this allows setting the timeout for Authentication and Accounting proxy. The default is 30 seconds.
-u [file]	UsersFile	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 above DataDirectory.
-v		Display RadiusNT version information.
-x[level]	Debug	The debug mode is generally only used from the command line to diagnose problems. Debug options are: 1 = Information 2 = User Debug 4 = ODBC Debug 8 = File Debug Simply add the options you want together. For instance if you want Information and ODBC debugging, you would use -x5.
-X		Packet level debugging.

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

Registry	Description
License	RadiusNT License
CompanyName	Company Name for RadiusNT License
DBM	ODBC RDBMS mode RadiusNT will be in. This determines the style of SQL statements and procedures used. Please see the ODBC Databases supported section for more details. 0 Automatic detection 1 Microsoft SQL Server 2 Microsoft Access 3 Sybase SQL Server 4 Oracle Database Server
ODBCTimeout	The number of seconds RadiusNT will wait for an ODBC query to return. Default is 15 seconds.
Username	The username RadiusNT will use to make the ODBC connection.
Password	The password RadiusNT will use to make the ODBC connection.
Logfile	The logfile used for RADIUS authentication requests (and accounting requests if an accounting logfile is not specified).
AcctODBCDataSource	RadiusNT will use this, rather than the default of "radius", for the Accounting ODBC connection. This is only applicable in ODBC multi-thread mode.
AcctUsername	The username RadiusNT will use to make the ODBC connection.

AcctPassword	The password RadiusNT will use to make the ODBC connection.
AcctLogfile	The filename where the Accounting Logs will go. Typically used in text only mode.
TrimName	When this is set to 1, RadiusNT will trim spaces around a name, and also truncate a name when a space is encountered. Normally RadiusNT tries to authenticate the user with exactly what the Username attribute contains.
IPCheck	When set to 0, if RadiusNT does not have a specific entry for the client making the request, it will allow the request and use the Global Secret specified below. This should be used only for testing or emergency reasons since it allows anyone to make requests to your RadiusNT server.
GlobalSecret	Global secret to use when IPCheck is set to 0 and the client is unknown.
ProxyTimeout	The number of seconds RadiusNT will store a proxy request in memory before it clears it. The default is 30 seconds.
ProxyID	Replace NAS-Identifier with this IP Address when sending a proxy request. This can hide the NAS-Identifier from the Proxy Server.

8. ODBC Database Schema

One of the most powerful features of RadiusNT is integrating it into a backend RDBMS. RadiusNT accomplishes this through ODBC. Many features are available in ODBC mode which are not available in text mode, simply because the backend RDBMS allows RadiusNT 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's authentication behavior.

Table Layout

There are many tables required by RadiusNT. Below is a list of those tables and a description of the fields. An * after 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 less than this field, the account will NOT be authenticated. This is used by Emerald only.
	*Balance	money	See the overlimit field above. This is used by Emerald only.
SubAccounts			Second Tier Account Information. 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 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 for the SubAccount. This should be set to NULL if the user has no time limit.
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 4 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 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 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.
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 for normal user-based proxy.

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, except that the field names do not include the dashes.
	NASIdentifier	varchar(16)	Identifier for the NAS. 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 the Call
	UserName	varchar(32)	Username of the caller
			The above fields are the BASE required fields. You can, and should, add more fields to allow storage of the fields you need to use. Some common fields to add would be AcctSessionTime and AcctDelayTime.
CallsOnline			The CallsOnline table/view tracks who is on-line at any given time on a specific port. This can be a standalone table, or a view/query based upon the Servers and ServerPorts table.
	UserName	varchar(32)	
	AcctStatusType	integer	
	CallDate	datetime	
	FramedAddress	varchar(16)	Default assigned IP Address for callers to this port who do not have a specific IP Address assigned to their account.
	NASIdentifier	varchar(16)	
	NASPort	integer	
AccountTypes			The AccountTypes table is not directly used by RadiusNT, but is used as a lookup table for the AccountType field in the SubAccounts table.
	AccountType	varchar(15)	Name of the Account Type
	Description	varchar(30)	Description of the Account Type
	DNISGroupID	integer	The DNISGroupID of the DNISGroup this account type is allowed to log into. No DNIS group is enforced

			is this field is NULL.
RadLogMsgs			The RadLogMsgs table provides text descriptions of the RadLogMsgID numbers in the RadLogs table.
	RadLogMsgID	integer	Log Message Identifier (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 is run in either ODBC or BOTH mode.
	RadLogMsgID	integer	Related Log Message Identifier from RadLogMsgs
	LogDate	datetime	The date of the message
	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 concurreny control and 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
	SNMPUsers	varchar(64)	SNMP OID string for SNMP Concurrencychecking
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
	StopTime	integer	The stop time allowed to login
DNISGroups			The DNISGroups table defines each DNIS group which 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 (1645)
	AcctPort	integer	Port number to send accounting requests to (1646)
	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 is not NULL, then RadiusNT 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 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
Licenses			The Liscenses table contains the license information for RadiusNT.
	LicenseID	varchar(25)	The License key
	Company	varchar(40)	The Company name in the License. This is case sensitive and much match exactly to what was provided with the license key itself.

Inside the Database

Understanding the RadiusNT database is the key to making RadiusNT do what you want. This section describes common operating procedures and assumes general understanding of databases.

Authentication Process

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

1. 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, send a reject.
3. If the requested password does not match the database password (with proper case check), send a reject.
4. If the saExpireDate Field is not NULL and the SubAccount saExpireDate plus Extension is before today, then send a reject. (This is only applicable to SQL Server or Sybase, as this is not supported by MS Access or Oracle.)
5. If the saExpireDate is NULL and the MasterAccounts maExpireDate plus extension and overdue is before today, then send a reject.
6. If Time banking is enabled and the SubAccount's TimeLeft field is not NULL and less than 1, send a reject.
7. If concurrency checking is enabled, and the user is listed in the callsonline view (with more entries than they are allowed), send 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, send 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 should 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 user check attributes, like Caller-ID.

The RadATConfigs table has attribute sets for each Account Type. This is where you would put the attributes for generic account types. You would not put user specific attributes in the RadATConfigs table.

If RadiusNT finds entries in the RadConfigs table that matches the user's AccountID, it does not look into the RadATConfigs table for Account Type matching entries. Therefore, if you do add an entry in the RadConfigs table, you must add the complete set of attributes, since RadiusNT will not bring other attributes in.

Accounting Process

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

When an accounting record is received by RadiusNT, it checks each attribute of the accounting request to see if there is a matching entry in the calls table list it read into memory. If there is, then that attribute is stored into the calls table. Since RadiusNT 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 to stop working.

You can add columns to the Calls table to have RadiusNT store additional information in the Calls table. You will need to look at a sample of the data that will be stored in the column, and create an appropriate column. Each RADIUS attribute has a type associated with it, which dictates how RadiusNT will create the INSERT statement.

For a type of string, IP address, or date/time RadiusNT will create a character type (varchar). For an integer type RadiusNT will create 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 is designed to use ODBC for database connectivity, not all ODBC drivers and SQL statements are the same. RadiusNT will check with the ODBC driver and automatically switch to support the RDBMS, if it has internal knowledge of the RDBMS (see the list below). Otherwise, RadiusNT will default to Microsoft SQL server mode. You can modify the DBM registry entry to force RadiusNT into a particular mode if you are using an unknown database. Please contact support if you would like to use RadiusNT with a database system that is not listed below. There is a charge for assistance with non-supported databases.

Microsoft SQL Server

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

Name	Description
RadCheckDomain	Check to see if a domain is listed for Proxy.
RadCheckOnline	Check to see how many times a user is on-line.
RadCheckPort	Check to see is a user has access to a specific port.
RadCheckTrigger	Check to see if an external trigger is available for this user.
RadCheckDNIS	Check to see if an account type is allowed to login into a specific number.
RadUserDefaults	Retrieve the list of all AccountType RADIUS defaults.
RadGetATConfigs	Retrieve the list of RADIUS default attributes for an AccountType.
RadGetConfigs	Retrieve the list of RADIUS default attributes for an AccountID.

Below is a list of the stored procedures that Emerald provides for RadiusNT 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 RadCheckDomain @Domain varchar(32) AS
Select Server, IPAddress, Secret, AuthPort, AcctPort, Priority, Timeout, Retries,
        StripDomain, TreatAsLocal, AccountType
```

```
From RadRoamDomains rrd, RadRoamServers rrs
Where rrd.RadRoamServerID = rrs.RadRoamServerID AND Domain = @Domain
Order By Priority

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 RadGetATConfigs @AccountType varchar(15) AS
Select ra.RadAttributeID, Name, Data, Value, Type, rc.RadVendorID, rc.RadVendorType, rc.RadCheck
From RadATConfigs rc, RadAttributes ra
Where ra.RadAttributeID=rc.RadAttributeID AND rc.AccountType=@AccountType

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
```

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. There is a significant performance issue when multiple users access the database, though. Since RadiusNT must have the database open at all times, this can become an issue as you grow. There are also no built-in replication or fail safe capabilities either.

RadiusNT 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 can offer.

A fully working Access 7.0 database is included with the RadiusNT distribution. You can use this as a starting point to test or build additional features or options that you would like to use.

Sybase SQL Server

RadiusNT supports operation with Sybase the same as Microsoft's SQL Server. Please see the above Microsoft SQL Server section for an overview. However, the scripts to create the database itself will differ, since there are slight differences between Microsoft's TSQL and Sybase's TSQL. Please see the RadiusNT distribution for an example set of scripts for creating a database under Sybase.

Oracle

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

Upgrading From An Earlier Version

The RadiusNT 2.5 database schema includes several database changes to either add new functionality or correct previous issues. This list is specially for those customers who are not using SQL Server or not using Emerald (those customers should use the rad25_up.sql script to update their database).

Below is a list of known database changes:

General

- The timeleft field in the SubAccounts table should now be NULL when time banking is not enabled for the user. Previously this was set to –9999 to specify no time banking.

SQL Server

- Added several stored procedures used during authentication and other areas to replace the queries RadiusNT manually built and executed. This allows for increased flexibility and adaptation when running against SQL Server. See the SQL database section for a list of the stored procedures.

9. Advanced ODBC Features

There are several advanced features of ODBC mode which are not available in text mode. The following sections explain more in depth about each of these features.

Concurrency Control

Preventing a single user from logging in multiple times simultaneously is called concurrency control. RadiusNT uses the RADIUS Accounting records to maintain a list of who is currently on-line. To achieve this, 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. You can run RadiusNT in -x15 debug mode to see examples of the NAS-Port numbers. RadiusNT will only update the records of the ServerPorts table, and will not create them.

The CallsOnline view contains columns from both the Servers and ServerPorts table. It is simply a convenient way to read and manipulate data based on both of those tables. This view is used mainly for checking and updating the callsonline list, as noted below.

When RadiusNT receives an authentication request and concurrency control is enabled, it will look at the number of entries in the CallsOnline view which match the username. If you do not have variable login limits enabled, then RadiusNT will default to only allowing the user to login one time. If you do have variable login limits enabled, then RadiusNT will only allow the user to login the number of times specified in the LoginLimit field. All other requests will be rejected.

A special note must be considered for ISDN or MPP users. Concurrency control may additionally restrict the number of channels a user can "bond" together into a single session. So if you want an ISDN user to be able to use 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. The Port-Limit attribute is not the same as concurrency control, since it does not limit non-MPP connections. You can use both of them together to effectively control the number of logins, though.

If you are using a passive database system, you can tell RadiusNT to manually update the CallsOnline view with the proper information. This should not be used in a true RDBMS system, since you can setup a trigger to do this much more efficiently.

Time Banking

Time banking allows you to specify a set number of minutes which is the maximum number of minutes the user will be able to log in. 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 the TimeLeft field of the SubAccounts table. If the field is NULL, then the account is not using time banking. RadiusNT will additionally return the Session-Timeout attribute equal to the number of minutes specified. If the RADIUS client (NAS) supports the Session-Timeout attribute, this will effectively only allow the user to be on the exact number of minutes specified.

If you are using a passive database system, you can tell RadiusNT to manually update the user's timeleft information. This should not be used in a true RDBMS system, since you can setup a trigger to do this much more efficiently. Time Banking is not enabled by default. You must enable Time Banking in the RadiusNT administrator and restart RadiusNT before it will work. In addition, you must have a NAS which supports it.

Server Access

Server Access allows you to limit the ports an Account Type can log into. When Server Access is enabled, RadiusNT will search for a matching 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 no match is found the user is not allowed to log into the port. The NASPort field may be NULL, which specifies that any Port is allowed for that NAS. This helps minimizes the numbers of records required in the ServerAccess table.

Server Access is not enabled by default. You must enable Server Access in the RadiusNT administrator and restart RadiusNT before it will work.

DNIS Access

DNIS Access allows you to limit the telephone numbers an Account Type can log into. When DNIS Access is enabled, RadiusNT will search for a matching 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 no match is found the user is not allowed to log via that number.

DNIS Access is not enabled by default. You must enable DNIS Access in the RadiusNT administrator and restart RadiusNT before it will work.

Logging

You can enable ODBC logging to allow RadiusNT to log information to the database. This information can be very useful in debugging or problem solving. You can also do reporting and gather statistics to find out any possible problems RadiusNT may be having.

The log table, described above, is very simple. The main field is the RadLogMsgID field, which tells 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, which is specific to the type of log message. For example, a type 0 generic message or type 1 generic error will have a description of what it is in the data field (and typically the username field is blank). However, for a type 4 message (bad password), the username field will be the username entered and the data field will be the password the user entered.

Below is a list and description of the RadLogMsgIDs:

RadLogMsgID	Log Message	Description
0	Generic Log Message	This is a generic log message, which does not have a pre-defined RadLogMsgID. This will be 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. This is typically a recoverable error.
10	User Not Found	The username 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 is expired.
13	Overdue Account	The user's account is overdue (Balance is larger than allowed)
14	Concurrency Limit	The user is already logged in the maximum allowed number of 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 who 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. This is typically because the secret used by the NAS does not match the secret RadiusNT has for the NAS.
60	Parse Error	The data RadiusNT was trying to parse was in error.
100	CHAP not allowed	The user authentication attempt used CHAP, but the user's Password is "UNIX" or "WINNT". For these two cases, the user must use PAP.

10. Enterprise Features

When RadiusNT is run with an Enterprise or Emerald license, additional features are available. These features are not enabled by default and require several configuration steps in order for proper operation. The following sections describe in detail, these features.

Proxy and Roaming

RadiusNT supports RADIUS proxy in ODBC mode. This allows you to forward or proxy a request to another RADIUS compatible server. RADIUS proxy is also known as forwarding or roaming. RADIUS proxy is not enabled by default. You can enable it for authentication, accounting, or both in the RadiusNT administrator.

User Based Proxy

Roaming is popular for allowing users of other ISPs or companies to dial locally into your facilities, rather than calling long distance to access the Internet. The user logs in with their full E-Mail address and this signals RadiusNT that the user is a roaming user, and not a local user. RadiusNT then extracts the domain from the user's E-Mail address. If it is a domain configured for proxy, the request will be forwarded to the specified RADIUS server. RadiusNT will then forward the response it receives back to the RADIUS client to finish the request.

The theory of roaming is pretty simple, although there are many technical aspects, which RadiusNT must take care of to insure reliable delivery to the final server and a response back to the RADIUS client. To configure RadiusNT for proxy, there are two basic steps:

1. Define the RADIUS servers which you will be proxying requests to. The server information is stored in the database table RadRoamServers.

2. Define the domains that you wish to forward and associate a RadRoamServer to send the requests to. The domain information is stored in the database table RadRoamDomains.

After RadiusNT 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 will build the response packet and finally send it back to the RADIUS client.

There are several options for configuring roaming in the above noted two tables. One of the more useful options is the default domain. You can define a domain as "DEFAULT", and RadiusNT will send all roaming requests to it, which 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 will strip the domain and look in your local database for the user. If you have several possible local domains your users may try to login as (for example, user@my.com, user@mail.my.com, and user@server.my.com) you can configure an entry for each with both of these flags set to true. 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.

Server Based Proxy

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

To achieve Server Based Proxy you need to first check the option in the RadiusNT administrator. When this option is checked, RadiusNT will look at the RadRoamServerID field in the corresponding record from the Servers table of the client making the request. If the RadRoamServerID is not NULL, then RadiusNT will look for the matching entry in the RadRoamServers table. If a matching entry is found, RadiusNT will then forward the request to that server.

In Server Based Proxy, RadiusNT does NOT modify or change the attributes in either direction (besides the addition and removal of its own Proxy-State attribute). The Strip Domain and Treat as Local options are not applicable either.

Modifying Return Attributes

In some situations, you may not want to forward the set of attributes returned from the server the proxy request is sent to, but rather return a different set of attributes all together. If the AccountType field in the RadRoamDomains table is not NULL, then RadiusNT will return the set of attributes associated to that AccountType, in the RadATConfigs table.

SNMP

RadiusNT can be both an SNMP server for external statistics tracking as well as an SNMP client. The following section explains how to setup SNMP support for each. You must have the SNMP service already installed via the network properties before RadiusNT can receive SNMP requests. However, you do not need the SNMP service installed for the SNMP concurrency checking.

RadiusNT supports most parts of the RADIUS Accounting and Authentication SNMP MIB proposal. This allows an SNMP agent to query statistics and information about RadiusNT in real time. If SNMP is configured correctly and allowed, then RadiusNT will spawn a separate thread to handle the SNMP requests. Therefore a total of four threads may be spawned in total with SNMP active.

You must have the SNMP service itself installed on each machine RadiusNT is installed on. You can install the SNMP service in the network properties of the control panel. If you did not have the SNMP service installed, you will most likely need to re-install Windows NT service pack 3, 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 you have the SNMP service installed, 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 of regedt32, and go to HKEY_LOCAL_MACHINE\Software\IEA\RadiusNT. Create a key named "SNMP", and then a value named "Pathname" under the SNMP key. The type of the value is REG_SZ and the data should be the full path to the radntmib.dll file (usually c:\radius\radntmib.dll).

3. Go to HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\SNMP. If you do not have this key, then the SNMP service was either not installed, or not installed correctly.
4. Continue to go to Parameters\ExtensionAgents key. This key will include several values, with names starting at "1" and increment by one for each new value. You need to add a value of type REG_SZ with the next number (for example, if 1 and 2 are present, you would use 3). The data should be the registry path to the key created in step 2 (usually "SOFTWARE\IEA\RadiusNT\SNMP") w/out the tree name (HKEY_LOCAL_MACHINE is assumed).

For the SNMP service to read the registry changes, you will need to restart the SNMP service.

The radntmib.dll is how the SNMP service communicates with RadiusNT. You can start either service (SNMP and RadiusNT) in any order and stop/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.

Querying SNMP values

The CMU SNMP tools are available as an example to query information from RadiusNT via SNMP. You can also use other SNMP tools to query RadiusNT (like the SNMP tools which come with the Windows NT Resource Kit). The OID for the base information for RadiusNT is 1.3.6.1.3.79. The easiest way to see each of the values available, is to use snmpwalk to walk the RADIUS tree. The below command illustrates an example of this:

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


radius.radiusAuthentication.radiusAuthServMIB.radiusAuthServMIBObjects.radi
usAuthServ.radiusAuthServIdent.0 = "RadiusNT 2.5.116"

radius.radiusAuthentication.radiusAuthServMIB.radiusAuthServMIBObjects.radi
usAuthServ.radiusAuthServUpTime.0 = 119192

radius.radiusAuthentication.radiusAuthServMIB.radiusAuthServMIBObjects.radi
usAuthServ.radiusAuthServResetTime.0 = 119192

radius.radiusAuthentication.radiusAuthServMIB.radiusAuthServMIBObjects.radiusAut
hServ.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 2.5.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 (successfully 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
.1.3.6.1.3.79.1.1.1.1.1.0	Identification	RadiusNT Identification string: "RadiusNT 2.5.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	Accounting Responses	Number of responses (successful requests).
.1.3.6.1.3.79.1.1.1.1.5.5	Malformed Requests	Number of malformed requests (not bad authenticators).
.1.3.6.1.3.79.1.1.1.1.5.6	Bad Authenticators	Number of bad authenticators (invalid secrets).
.1.3.6.1.3.79.1.1.1.1.5.7	Packets Dropped	Number of requests dropped w/out a reply sent.
.1.3.6.1.3.79.1.1.1.1.5.8	No Record	Number of packets of unknown types.
.1.3.6.1.3.79.1.1.1.1.5.9	Unknown Types	Number of packets of unknown types.

SNMP Concurrency Checking

One of the main problems with concurrency control is when RadiusNT does not correctly track the on-line users. This can cause a user to be inadvertently denied access when they should not be. To prevent this from happening, RadiusNT can verify that the user is on-line at the time of authentication by using SNMP. This feature only allows RadiusNT to do a real time verification check to see if the user is still on-line. It will not update the calls online list or correct any other problems pertaining to the calls online. It is designed to prevent incorrect concurrency denial rather than to always prevent logins because of concurrency limits.

For RadiusNT to query 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 in the Servers table, Community field. Although this is typically "pubic", you may have changed it for security reasons. The OID for each port is stored in the ServerPorts table, SNMPUser field. The contents of this field will change for each port. Currently, it must be a static entry for each port and may differ from NAS models and vendors.

For a Livingston Portmaster, 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 populate the ServerPorts table by using a derivative of the following SQL statement. For other NAS vendors you should consult the NAS documentation to see 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
```

The ServerID should match an entry from the Servers table for the NAS you want to update.

When running against SQL Server, RadiusNT calls the following stored procedure to retrieve information about each port the user is listed on.

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

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

You need to have this stored procedure in your database and the user RadiusNT is connecting as must have execute permission for it.

11. Trouble Shooting

Although we went to great strides to make the installation and use of RadiusNT as easy as possible, problems and errors will sometimes happen. Below are some common problems and solutions to installing and using RadiusNT.

If you are having problems with RadiusNT you should always run RadiusNT in debug mode. This is accomplished by stopping the service (you can not have two copies of RadiusNT running on the same machine) and from the directory you installed RadiusNT into type:

radius -x15

RadiusNT will start in foreground mode and display a lot of debug information. Most of the time this will be sufficient for you to resolve the problem. When sending E-mail to tech support, you should include a cut and paste of the debug output of the problem.

RadiusNT also logs information to a file named *logfile* in the data directory or to the RadLogs table in ODBC/both mode. You can use these as tools to help solve problems as well.

Installation and Setup Problems

- During installation, I receive an error telling me an RDC object can not be registered.

  Whether RadiusNT is used in ODBC or text mode, you must have ODBC installed. You can obtain the ODBC installation from http://www.microsoft.com/odbc or from /RadiusNT/ODBC on the IEA Software FTP site.

Startup Problems

- RadiusNT reports the radius entry could not be found in the services file.

  For RadiusNT 2.2 or lower, you need to make sure you add the two entries to your services file as outlined in the installation steps in Chapter 1.

- RadiusNT reports a file not found error and quits.

  Double check your path entries in the RadiusNT administrator to make at least the data directory point to the directory where you installed RadiusNT.

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

  User x has an attribute in the users file which does not match an attribute from the dictionary. Attributes are case sensitive and must match EXACTLY to the dictionary entries.

- RadiusNT reports a fewer number of users loaded than are in the users file

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

Operation Problems

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

  The machine which the request is coming in from is not authorized to send requests to RadiusNT. This is caused by not having the IP Address of the requester in the clients file (text mode) or database. You must re-start RadiusNT 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 Network Access Server (NAS) sending the request is not the same secret set for the NAS in the clients file (text mode) or the database. You must re-start RadiusNT for changes to the clients list to take affect. Secrets are case sensitive and should be between 6 and 15 characters long.

- Accounting packets in ODBC mode sometime display an error about entries must be unique.

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

12. Frequently Asked Questions

General

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

  RadiusNT is designed to work with any RADIUS compatible terminal server. Since the RADIUS protocol is vendor independent, this allows RadiusNT 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 WebSite.

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

  RadiusNT supports both PAP (clear text) and CHAP. However, if you will be using a user list which contains encrypted passwords (WindowsNT SAM, UNIX passwd file, or encrypted passwords in a database) only PAP authentication will work since RadiusNT must have the password in clear text in these cases.

- *I have downloaded RadiusNT and everything runs normal for awhile, then it stops authenticating. How can I find out what the cause of this is?*

  The evaluation copy of RadiusNT when running without a licensing key will only perform 100 requests in ODBC mode. We do offer extended evaluations if desired. If you need an extended evaluation, send e-mail to support@iea-software.com. When RadiusNT is run in ODBC mode the key is retrieved from the database. When RadiusNT is run in TEXT ONLY mode it looks for the key in the registry which is stored there by the RadiusNT administrator.

  If you are still having problems, run RadiusNT in –x15 debug mode and it will tell you why it stopped authentication or what the problem is.

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

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

- *Can RadiusNT authenticate against the Windows NT User Database?*

  RadiusNT can authenticate against the Windows NT User Database in both text and ODBC mode. However, only text mode can authenticate all users by default. If ODBC mode, each user must be added to the database as well. See Chapter six for more details on NT SAM support.

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

  Yes it does.

- *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.

- *Where can I find a copy of the Radius RFCs?*

  The RADIUS RFCs are 2138 and 2139. You should be able to find them on any site that carries standard RFCs, or you can ftp them from: ftp://ftp.livingston.com/pub/radius

- *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 happen when you do not start RadiusNT as a service. To remedy, go into the NT Administrator and install the service. Then from a command line, start the service by typing:

  net start RadiusNT

- *I installed RadiusNT as a service, but 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".*

  You need to define full paths for the accounting and data directories in the RadiusNT administrator. That will correct the problem.

- *Does RadiusNT support filters?*

  RadiusNT supports the standard RADIUS filter attribute as well as the Ascend Binary Filter attribute. You will need to inquire with your NAS vendor as to what kind of filters they support.

- *Does RadiusNT support a DNS attribute?*

  RadiusNT can support any basic attribute. It is the NAS/Proxy that must understand what it is and support it, or it will be of no use.

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

  Use the Port-Limit attribute (see if your NAS supports it) to restrict how many channels someone can bond together. You can also use concurrency control to limit the number of simultaneous connections a user can make.

- *Will RadiusNT assign from different groups of IP addresses?*

  Only if the NAS supports an attribute to specify the pool (like Ascend does).

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

  RadiusNT 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.

- *What should the Login Limit be set to, in order to prevent multiple logins?*

  If the variable login limits option in the RadiusNT Admin is unchecked, only one login is allowed for each user. Otherwise, RadiusNT looks at the LoginLimit field in the SubAccounts table and uses that value for the user's login limit.

- *How can I prevent Dr. Watson from bringing up a dialog box and preventing RadiusNT from being restarted from remote?*

Edit or add the following sections to the registry of the machine running RadiusNT.

HKEY_LOCAL_MACHINE\Software\Microsoft\DrWatson\VisualNotification: 0

There may be other values that you may want to change as well.

Text Mode

- *Do we need to restart the RadiusNT service when we change the user file?*

  There are two ways to handle the changes. You can either restart RadiusNT as the users are cached in memory, or you can also use the "*reload*" user entry with radlogin which will signal RadiusNT to reload the users file w/out restarting the service.

ODBC Mode

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

  1. You will need to add entries in the servers table to match the data for your NAS.
  2. Add entries to the ServerPorts table matching each port of the server (with matching ServerID) of the NAS you entered in step 1.

  Make sure the callsonline view/query is set correctly and that RadiusNT is receiving the accounting requests from the NAS, with NAS-Identifier matching Servers.IPAddress and NAS-Port matching the ServerPorts.Port fields.

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

  RadiusNT can use UNIX crypt passwords (like found in a Unix passwd file) in the database. This is an advanced feature and not for those who do not understand what crypt encryption is. RadiusNT does not include any tools to facilitate the creation or management of passwords in encrypted form.

  To enable this option, you must edit the Options registry entry. See the section on registry and command line options for more details. This is an all-or-nothing option: you can't have clear text passwords if you enable it.

- *Can RadiusNT be used to just log accounting to a database without entering user information? 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.*

  Many customers start with RadiusNT and just accounting. The setup is the same, but you will not have any users defined. Almost all terminal servers allow for a different accounting and authentication RADIUS server.

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

  Yes. Add 16 to the Options registry entry and it will force RadiusNT to act in MS Access mode.

- *Where can I learn more about ODBC?*

Check out this area on Microsoft's Web site! http://www.microsoft.com/accessdev/articles/clientkb.htm

- *Can I modify the SQL statement sent by RadiusNT for inserting records in the calls table?*

  The SQL statement is dynamically created based on the fields in the calls table and the attributes received in the accounting requests. The process is outlined in Chapter 9.

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

  You must add entries in the RadConfigs table, matching the user's SubAccountID. One of the attributes should be the Framed-Address attribute. You can not just simply add the Framed-Address in this table, as RadiusNT will only send the attributes in this table if any exists (ignoring any attributes in the RadATConfigs table).
  (Emerald customers see the next section)

Emerald Integration

- *What do I use for a license for RadiusNT when configuring it for use with Emerald?*

  You will not configure a license in the RadiusNT Admin. Once you have configured RadiusNT for ODBC mode and it is pointing to your Emerald database, RadiusNT will use your Emerald licenses. You should enter your Emerald license in the Emerald Administrator.

- *How can I setup a backup copy of RadiusNT which does not connect to my Emerald database?*

  To setup a stand-alone version of RadiusNT which is not attached to a database, use one of your Emerald license keys in the RadiusNT administrator. You can 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?*

  The process requires working knowledge of Microsoft SQL Server and Enterprise Manager. If you are not familiar with both of these, then please refer to someone who is.

  1. Right click over your current calls table and select indexes. This will show you the number of records and SIZE of your calls table. Use this as a general starting point (plus some) below.
  2. Create Two Database Devices, EmerCallsDev and EmerCallsLog. The first should be based on the size of the calls table from #1. Give it some room to grow, also. The EmerCallsLogs should be about 20% of the size of the EmerCallsDev (for example 200mb and 40mb, respectively).
  3. Create a database EmerCalls, with Data Device EmerCallsDev and Log Device EmerCallsLog. Use the Full size of each.
  4. Use SQL EM to transfer your calls table from your Emerald Database to your EmeraldCalls database. Transfer *JUST* the calls table, not the whole database.
  5. Under Manage Logins (SQL EM) go through and give each Emerald user permit permission to the EmerCalls Database (public group). Under the EmeraldCalls database, groups/users, public right-click and select permissions. Click grant all, set, and close.
  6. Right click over the new Calls Table (in EmerCalls database) and select triggers. Paste this 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. In your Emerald Database, drop your calls table and create a view of:

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

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

8. Check everything out and make sure it worked ok. :)

You probably WILL loose some call records unless you do this at a slow time. It won't hurt you (that much) but you may have some stuck users on-line for a while which you may have to manually clear.

Vendor Support

Ascend

- *I have an Ascend MAX 40xx and can not get RadiusNT to do 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, then it asks for Port and IP address. I have no idea what the ports are so assign IP addresses from a pool. Help!*

  First check to make sure you have the MAX configured for accounting and sending accounting requests to RadiusNT. The Port field should represent what the MAX returns in the NAS-Port field (run RadiusNT 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.

The IPAddress 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?*

  Information is available on the Ascend WebSite at: http://www.ascend.com/1994.html

Cisco

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

  This issue became Cisco bug-Id CSCdi87169 "RADIUS should never include multiple Framed-IP-Address fields". This has been fixed in the following releases: 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

  Cisco users should upgrade to one of the releases above to avoid problems in ODBC mode. Please note that the above are Cisco OS releases, not RadiusNT.

- *Do you know of a good resource for learning how to configure Cisco IOS software to support RADIUS?*

  Following are a couple of informative pages concerning Cisco and RADIUS.

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

Computone

- *Every time I reset my Computone, I have problems with RadiusNT returning errors when trying to store accounting records in the ODBC database. How can I prevent this?*

  The problem is the Computone products reset their Acct-Session-ID counter upon a reboot. You need to setup a time server and point the Computone product to it and a time value will be inserted as the first part of the Acct-Session-ID. One drawback to this is that the Acct-Session-ID field will be larger, which could cause RadiusNT 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 the newest version of RadiusNT support iPass roaming?*

  We have not finalized iPass support, but have been working on it. Look for it at a future date, yet to be determined.

  To learn more about iPass roaming, 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 tell you about an outage. Instructions are included with it on how to monitor a RADIUS server.

Livingston

- *Is it possible to prohibit analog account access on ISDN lines on the PortMaster 3? What would a sample text RADIUS look like?*

  You can use users file entry like the below. You can also add the NAS-Port-Type check to the RadConfigs or RadATConfigs table of your database with the check field enabled for ODBC mode.

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

  ALL check attributes must go on the first line.