Ascend Access Control
User's Guide

Ascend Communications

Part Number 7820-0491-002 August 14, 1997

ASCEND END USER AGREEMENT

License

The term “Software” includes all Ascend and third party (“Supplier”) software provided to you with this Ascend product, and includes any accompanying documentation (the “Documentation”). The term “Software” also includes any updates of the Software provided to you by Ascend at its option. Subject to the terms of this Agreement, Ascend grants to you, and you accept, a personal, non-exclusive, and nontransferable (except as set forth below) license to use the object code version of the Software on a single computer. The Software is “in use” on a computer when it is loaded into the temporary memory (i.e. RAM) or installed into the permanent memory (e.g. hard drive, CD-ROM or other storage device) of that computer, except that a copy installed on a network server for the sole purpose of distribution to other computers is not “in use.” If you permanently install the Software on the hard disk or other storage device of a computer (other than a network server) and you use that computer more than 80% of the time it is in use, then you may also use the Software on a portable or home computer. You may make a reasonable number of copies of the Software and Documentation for backup or archival purposes only, so long as Ascend's and its licensors’ copyright notices are reproduced on such copies.

Limitations on Use

You may not copy, rent, lease, sell, sublicense, assign, loan, time-share or otherwise transfer or distribute copies of the Software or Documentation to others, except as set forth in this agreement. You may physically transfer the Software from one computer to another provided that you do not retain any copies of the Software, including any copies stored on a computer. You may permanently transfer this license to another user, but only if you transfer or destroy all copies of the Software and Documentation, and the recipient agrees in writing to be bound by all of the terms of this agreement.

You agree that you will not decompile, disassemble, or otherwise reverse engineer the Software, and you will use your best efforts to prevent your employees and contractors from doing so, except to the extent that such

restriction is expressly prohibited by applicable law. You may not modify, adapt, create a derivative work, merge, or translate the Software or the Documentation without the prior written consent of Ascend.

Specific Suppliers may be identified in the Documentation. You agree to any additional terms and conditions specific to particular Suppliers or Products, as described in the Documentation, which are incorporated herein by reference.

Intellectual Property Rights

You acknowledge that Ascend or its Suppliers retain exclusive ownership of all copyrights, trademarks, patents and/or other intellectual property rights in the Software and the Documentation. You are not granted any rights in the Software or Documentation other than the license rights expressly set forth above.

Term and Termination

The term of this license is for the duration of any copyright in the Software. This license automatically terminates if you fail to comply with any of the terms and conditions of this agreement. You agree that, upon such termination, you will either destroy (or permanently erase) all copies of the Software and Documentation, or return the original Software and Documentation to Ascend. You may terminate this license at any time by destroying the Software and Documentation and any permitted copies.

Limited Warranty and Limited Remedy

Ascend warrants to the original end user purchaser only that the Software as delivered at the time of purchase will substantially conform to the Documentation, and that the original diskettes and Documentation are free from defects in material and workmanship under normal use, for a period of ninety (90) days from the original end user's purchase thereof (the “Limited Warranty Period”), provided the Software is used with compatible computer hardware and operating systems. This limited warranty is void if failure of the Software has resulted from accident, abuse, or misapplication. Ascend's entire liability, and your sole and exclusive remedy shall be, at Ascend's option, either to (a) correct

or help you work around or avoid a reproducible Error, (c) replace defective diskettes or Documentation or (b) authorize a refund, so long as the Software and Documentation are returned with a copy of your receipt within ninety (90) days of your date of purchase together with a brief written statement describing the alleged Error. An “Error” is a defect in the Software that causes it not to perform substantially in accordance with the limited warranty set forth above. Any replacement Software or Documentation will be warranted for the remainder of the original warranty period only.

No Liability of Suppliers

You acknowledge that your rights under this Agreement, in the nature of warranty or otherwise, are solely against Ascend. NO SUPPLIER MAKES ANY WARRANTY, ASSUMES ANY LIABILITY, OR UNDERTAKES TO FURNISH TO YOU ANY SUPPORT OR INFORMATION CONCERNING PRODUCTS OR ANY PORTION OF PRODUCTS. You hereby release all Suppliers from any claims, damages or losses arising from the use of Products, regardless of the form of action.

Disclaimer of Warranties

EXCEPT AS SPECIFICALLY PROVIDED ABOVE, THE SOFTWARE AND THE DOCUMENTATION IS PROVIDED “AS IS,” WITHOUT WARRANTY OF ANY KIND. ALL OTHER WARRANTIES ARE DISCLAIMED, WHETHER EXPRESS, IMPLIED OR STATUTORY, INCLUDING BUT NOT LIMITED TO WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, NON-INFRINGEMENT OR THAT THE SOFTWARE'S FUNCTIONS WILL MEET YOUR REQUIREMENTS OR THAT ITS OPERATION WILL BE UNINTERRUPTED OR ERROR FREE. EXCEPT AS SET FORTH IN THIS AGREEMENT, THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE SOFTWARE AND THE DOCUMENTATION IS WITH YOU. IF THEY PROVE DEFECTIVE AFTER THEIR PURCHASE, YOU, AND NOT ASCEND OR ITS SUPPLIERS, ASSUME THE ENTIRE COST OF SERVICE OR REPAIR. If a disclaimer of implied warranties is not permitted by law, the duration of any such implied warranty is limited to ninety (90) days from the date of purchase by the original

end user purchaser. Some jurisdictions do not allow the exclusion of implied warranties or limitations on how long an implied warranty may last, so such limitations or exclusions may not apply to you. This limited warranty gives you specific legal rights, and you may also have other rights which vary from jurisdiction to jurisdiction.

Liability Exclusions and Limitations

IN NO EVENT SHALL ASCEND OR ANY SUPPLIER BE LIABLE FOR ANY INDIRECT, SPECIAL, INCIDENTAL, EXEMPLARY OR CONSEQUENTIAL DAMAGES OF ANY KIND (INCLUDING LOST PROFITS, LOSS OF USE OR INTERRUPTION OF BUSINESS), OR FOR LEGAL FEES, ARISING OUT OF THE USE OF THE SOFTWARE OR THE DOCUMENTATION, REGARDLESS OF THE FORM OF ACTION, WHETHER IN CONTRACT, TORT (INCLUDING NEGLIGENCE), STRICT PRODUCT LIABILITY OR OTHERWISE, EVEN IF ASCEND HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. IN NO EVENT WILL ASCEND'S AGGREGATE LIABILITY FOR ANY CLAIM EXCEED THE LICENSE FEE PAID BY YOU. This limitation shall apply notwithstanding any failure or inability to provide the limited remedies set forth above. Some jurisdictions do not allow the exclusion or limitation of incidental or consequential damages, so the above limitation(s) or exclusion(s) may not apply to you.

Proprietary Rights-Contracts with Certain U.S. Government Agencies

If the Software is acquired under the terms of a Department of Defense or civilian agency contract, the Software is “commercial item” as that term is defined at 48 C.F.R. 2.101 (Oct. 1995), consisting of “commercial computer software” and “commercial computer software documentation” as such terms are used in 48 C.F.R. 12.212 of the Federal Acquisition Regulations and its successors and 48 C.F.R. 227.7202-1 through 227.7202-4 (June 1995) of the DoD FAR Supplement and its successors. All U.S. Government end users acquire the Software and the Documentation with only those rights set forth in this agreement.

Export Restrictions

You acknowledge that the laws and regulations of the United States restrict the export and re-export of certain commodities and technical data of United States origin, including the Software and the Documentation, in any medium. You agree that you will not knowingly, without prior authorization if required, export or re-export the Software or the Documentation in any medium without the appropriate United States and foreign government licenses.

Severability

You acknowledge and agree that each provision of this agreement that provides for a disclaimer of warranties or an exclusion or limitation of damages represents an express allocation of risk, and is part of the consideration of this agreement. Invalidity of any provision of this Agreement shall not affect the validity of the remaining provisions of this Agreement.

General

This Agreement is the entire agreement between you and Ascend relative to the Software and Documentation, and supersedes all prior written statements, proposals or agreements relative to its subject matter. It may be modified only by a writing executed by an authorized representative of Ascend. No Ascend dealer or sales representative is authorized to make any modifications, extensions or additions to this agreement. This Agreement is governed by the laws of the State of California as applied to transactions taking place wholly within California between California residents, without application of its conflicts of law principles. The United Nations Convention on Contracts for the International Sale of Goods is specifically excluded from application to this Agreement.

Questions

If you have any questions, write or call Ascend Communications, Inc., One Ascend Plaza, 1701 Harbor Bay Parkway, Alameda, CA 94502.

Ascend Customer Service

When you contact Ascend Customer Service, make sure you have this information:

- The product name and model
- The software and hardware options
- The software version
- The type of computer you are using
- A description of the problem

How to contact Ascend Customer Service

Ways to contact Ascend Customer Service	Telephone number or address
Telephone in the United States	800-ASCEND-4 800-272-3634
Telephone outside the United States	510-769-8027
E-mail	support@ascend.com
Facsimile (FAX)	510-814-2300

You can also contact the Ascend main office by dialing 510-769-6001, or you can write to Ascend at the following address:

Ascend Communications
1275 Harbor Bay Parkway
Alameda, CA 94502

Need information on new features and products?

We are committed to constantly improving our products. You can find out about new features and product improvement as follows:

- For the latest information on the Ascend product line, visit our site on the World Wide Web:

  `http://www.ascend.com/`

- For software upgrades, release notes, and addenda to this manual, visit our FTP site:
  `ftp.ascend.com`

Contents

About This Guide

How Use This Guide

This guide describes Ascend Access Control, a software package that provides authentication, authorization, and accounting services for users who request network connections. Ascend Access Control includes a RADIUS server.

This guide contains instructions for configuring files that contain data Ascend Access Control must parse to perform authentication and authorization. Ascend Access Control is distributed with example configuration files you can copy. Edit the copied file's entries to reflect your personal installation.

What this guide contains

Chapter 1, "Introducing Ascend Access Control."

- Explanation of Ascend Access Control functions
- Ascend access Control and Ascend RADIUS compatibility

Chapter 2, "Quick Setup."

- Planning to Set up Ascend Access Control
- Installing Ascend Access Control
- Default Ascend Access Control Settings

Chapter 3, "Installing Ascend Access Control and its graphical user interfaces."

- Ascend Access Control demos
- Temporary license key

- Introduction to graphical user interface (GUIs)
- HTML Help files

Chapter 4, “Configuring Ascend Access Control Files.”

- Formats of `users`, `authfile` and `clients` entries
- Using Ascend Access Control Manager
- Using User Account Wizard
- GUI editing privileges

Chapter 5, “Understanding Ascend Access Control.”

- RADIUS authentication, authorization and accounting
- RADIUS messages and packets
- Field values in `authfile` and `clients` file entries
- Alternative authentication methods Ascend Access Control supports

Chapter 6, “Creating Example Client, User and Realm Entries.”

- Building a user profile and a client entry
- Adding a realm and a new client
- Adding support for token card authentication
- Converting RADIUS user profiles
- Verifying an Ascend Access Control server is operational
- Verifying user passwords on an Ascend Access Control server
- Debugging Ascend Access Control

Chapter 7, “Open Database Connectivity (ODBC).”

- Introduction to ODBC
- User profiles in Database Management System tables
- Ascend Access Control links to ODBC data sources
- DBMS drivers
- Configuring Ascend Access Control for ODBC support
- Example - INTERSOLV driver installation

Appendix A, “Ascend Access Control files and commands.”

- Field entries in Ascend Access Control files
- RADIUS daemon options

Appendix B, “Attributes Reference.”

- RADIUS and Ascend vendor-specific attributes

Appendix E, “MAX Accounting codes.”

- MAX accounting disconnect codes

MAX accounting progress codes

What You Should Know

This guide is intended for the person who will configure and maintain an Ascend Access Control server. You must have a basic understanding of security, authentication methods, and networking concepts.

You can use Ascend Access Control’s two graphical interface’s, Access Control Manager and User Account Wizard, or a text editor to create or edit Ascend Access Control data files.

Documentation Conventions

Table 1 shows the documentation conventions used in this guide.
Table 1.Ascend Access Control User Guide conventions.

Convention	Meaning
Monospace text	Represents text that appears on your computer’s screen, or that could appear on your computer’s screen.
`Boldface monospace text`	Represents characters that you enter exactly as shown (unless the characters are also in *`italics`*–see *Italics*, below). If you could enter the characters, but are not specifically instructed to, they do not appear in boldface.

Convention	Meaning
Italics	Represent variable information. Do not enter the words themselves in the command. Enter the information they represent. In ordinary text, italics are used for titles of publications, for some terms that would otherwise be in quotation marks, and to show emphasis.
[ ]	Square brackets indicate an optional argument you might add to a command. To include such an argument, type only the information inside the brackets. Do not type the brackets unless they appear in bold type.
|	Separates command choices that are mutually exclusive.
>	Points to the next level in the path to a parameter. The parameter that follows the angle bracket is one of the options that appears when you select the parameter that precedes the angle bracket.
Key1-Key2	Represents a combination keystroke. To enter a combination keystroke, press the first key and hold it down while you press one or more other keys. Release all the keys at the same time. (For example, Ctrl-H means hold down the Control key and press the H key.)
Press Enter	Means press the Enter, or Return, key or its equivalent on your computer.
Note:	Introduces important additional information.
 Caution:	Warns that a failure to follow the recommended procedure could result in loss of data or damage to equipment.
 **Warning:**	Warns that a failure to take appropriate safety precautions could result in physical injury.

User Interface Terminology

The Ascend Access Control GUI's are composed of standard Windows components, such as textboxes, drop down lists, buttons and radio buttons. Table 2 lists actions included in the GUI instructions and their meanings:

Table 2.Actions used in the manuals GUI instructions.

Actions	Meaning
Click	Move your cursor to an object on the screen, such as a button labeled Add Client, and press the mouse button that you use to select, highlight or drag.
Enter	Use your keyboard to type an entry.
Select	Click on an object, such as a textbox, to activate it, or click on an entry in a list to highlight it.

Related Publications

If your network includes Ascend routers that support Ascend Access Control, the supplemental security sections in your user guides contain useful information about RADIUS and other topics in the Ascend Access Control User's Guide.

Introducing Ascend Access Control

1

Ascend Access Control is a program that authenticates users. This chapter lists Ascend Access Control's features and provides an introduction to the Ascend Access Control authentication, authorization and accounting functions.

What is Ascend Access Control

Ascend Access Control is one of the Ascend family of security products developed to protect your network. Ascend Access Control provides authentication, authorization, and accounting services. It is based on the RADIUS protocol.

Ascend Access Control provides a central location to store information, or attributes, that defines individual users and the local and remote systems and services you allow them to access. The attributes and their values are maintained in user profiles. You can store user profiles on the Ascend Access Control servers, on other servers for which Ascend Access Control can be a proxy, or in Database Management System (DBMS) tables. Ascend Access Control's user profile information enables you to:

- Authenticate users
- Configure incoming WAN connections
- Configure dialout connections
- Establish routes
- Install filters
- Record connection-accounting data

Ascend products supported by Ascend Access Control

Ascend Access Control is extensible. Its `dictionary` file contains all standard RADIUS attributes and many others developed by Ascend for these units:

- MAX TNT
- MAX 4000
- MAX 2000
- MAX 1800
- MAX 200Plus
- Pipeline 400
- Pipeline 220

Ascend Access Control features

Ascend Access Control is a packaged executable. You do not need to compile source code before installing the program. It supports these features:

- Licensed support for security tokens
  - Security Dynamics ACE
  - AssureNet Pathways (formerly Digital Pathways) Defender
  - Bellcore S/Key (see Note)
- Token card caching
- Password aging
- Proxy-RADIUS authentication and accounting
- Graphical user interfaces (see Note)
- Multiple realms for authenticating users by domain
- Vendor-specific user profile attributes
- User Authentication via other methods
  - TACACS and TACACS+
  - MIT and AFS Kerberos (see Note)
- ODBC-compliant Database Management Systems tables (see Note)
- RADIUS IP Address Daemon
- Ascend packet filter profiles

Note: Some features are not available on all operating systems. Please note these restrictions:

- S/Key is not available on Solaris 2.5 x.86 (Intel)
- You can install Ascend Access Control's Java-based GUI applications on Windows 95 and Windows NT operating systems. Java's current release does not support true cross-platform installation of the applications.
- Kerberos is not available on SunOS 4.1.4 - SPARC
- ODBC is not available on SunOS 4.1.4 - SPARC. Ascend Access Control includes INTERSOLV's DataDirect ODBC 2.1 Driver Manager. You must obtain INTERSOLV's driver and the DBMS client for your operating system.

What Ascend Access Control does

Ascend Access Control performs three functions. It authenticates and authorizes remote users and, optionally, stores accounting information about the events that occur during users' connections to the network.

Authentication

Ascend Access Control's primary function is to confirm that someone requesting a connection to or from the network has permission to make the connection and to use network services. Ascend Access Control authenticates users by comparing information the users send to Network Access Servers (NAS) with information called check-items stored the user profiles in Ascend Access Control' `users` files.

Ascend Access Control also authenticates the NAS machines that send it Access-Request packets on behalf of the users that want to access the network. Ascend Access Control and the NAS share a secret key that allows the Ascend Access Control server to identify the NAS. The shared secret is stored as the value of a field in Ascend Access Control `clients` file entries.

Authorization

Ascend Access Control `users` files can contain reply-items as well as check-items, such as names, passwords and secret keys. Reply-items define the services users can access and the connections they can make. Ascend Access Control may include reply-items from user profiles in Access-Response packets it sends to clients that request user-authentication. The reply-items may authorize the NAS to allow the user to connect to a specific network machine, such as a Telnet server.

Authorization information that Ascend Access Control sends to a NAS might also tell the NAS how users are allowed to make internal and external connections. For example, Ascend Access Control's authorization might instruct the NAS to allow an incoming connection to a local Telnet server via an unframed protocol, but force another, outbound, user to connect with a remote location via the framed Point-to-Point Protocol.

Accounting

Ascend Access Control's third function is to serve as a repository of information about the activities that occur over network connections. When it has authenticated a user and authorized the connection and services, Ascend Access Control might receive an accounting of the connection from the NAS. The accounting can include such things as the start and stop times of the connection and the number of packets and octets that passed over the connection. Information such as this is valuable if you want to evaluate your security policies and network usage.

How Ascend Access Control works

Although simplified, the following steps summarize how Ascend Access Control works:

1. A client, such as a router, contacts the Ascend Access Control server and sends Ascend Access Control a message requesting authentication of a user who has requested network access. The outside source that contacts Ascend Access Control is referred to as a client.
2. Ascend Access Control searches its `clients` file for an entry that matches client-identification information in the client's message. If Ascend Access Control finds a match, it extracts user-identification information from the message. Typically, the user-identification in the message is a user name and a password or type of authentication.
3. Ascend Access Control searches a `users` file for a profile that contains data that matches the user-identification information from the client's request message. If successful, Ascend Access Control sends the client a user-authentication message.
4. The message verifies the user's identity, specifies the extent of the user's access to the network, and defines how the user's link to the network is to be configured.

Authentication and authorization information

You need to supply Ascend Access Control with information it can use to authenticate and authorize, including:

- Who its clients and their users are
- What its clients and their users will provide as identifying information
- Where to find matching information to identify clients and their users
- How its clients should configure their users' access and links

You store the information in Ascend Access Control files named `clients` and `users`. You might also store some of the information you gather in an Ascend Access Control file named `authfile` if you want to group users in entities called realms.

Gathering needed information

Gathering the needed information and adding it to the appropriate files is less complicated than it might appear. Suppose you receive a call from a city building inspector who requests that you meet and allow him to see some of your company's site plans for a new project. You ask the inspector some questions, while mentally considering some of the issues and consequences of granting his request. Here are your questions and considerations:

- Who are you?
- How will I know you?
- Where are you located?
- What's your telephone number?
- Should I call him back to verify that number?
- Where do you want to go?
- How do you want to get there?
- What do you want to see there?
- How can I limit what he sees?
- How long will you be involved in the project?
- Should I keep track of him while he's there?

The caller answers your questions. His name is Jeff Carr and his telephone number is 212-555-1212. Tomorrow he will drive to your office from the city building at 929 High Street. He will show the guard his employee ID so the guard can bring him to your office. After reviewing the plans in your office, he would

like to visit the construction site next door. He will probably return every few weeks for six months to keep abreast of the project's progress.

After hanging up you decide that, for now, you need only show him the model of the project. You think it will be a good idea to have a guard accompany him on his visit to the construction site and report back to you afterwards. You will provide Mr. Carr a pass to the site that is good for 30 days. Later you will call the number he gave you and ask to speak to him to confirm the time of your appointment.

At this point, you have gathered many of the kinds of information Ascend Access Control uses to authenticate and authorize a user. Table 1-1 illustrates how the building inspector's answers and your own security plan have given you information that resembles the values of attributes you enter in an Ascend Access Control user profile.

Table 1-1. Identifying Ascend Access Control attribute values

Question	**Ascend Access Control Attribute**
Who are you?	User-Name
How will I know you?	Password
Where are you located?	Framed-IP-Address
What's your telephone number?	Calling-Station-ID
Should I call you back to verify your identity?	Ascend-Callback
Where do you want to go?	NAS-IP-Address
How do you want to get there?	Framed-Protocol
What do you want to see there?	Service-Type
How can I limit what you see?	Ascend-Data-Filter
How long will you be involved in the project?	Ascend-PW-Expiration

Table 1-1. Identifying Ascend Access Control attribute values

Question	Ascend Access Control Attribute
Should I keep track of you while you're there?	Accounting service

Ascend Access Control includes `dictionary`, a file that lists all the types of information you can collect about users and their connections. Ascend Access Control uses the term attribute to describe a type of information. Each attribute has a value, or a list of possible values. You could think of the name "Jeff Carr" as the value of the User-Name attribute displayed in parentheses in the table's right column.

Ascend Access Control uses some attributes, such as User-Name, to perform authentication. It uses others, like Framed-Protocol, to perform authorization. Ascend Access Control attributes and their values are described in the Reference section of the Appendix.

Compatibility with Ascend RADIUS

Before developing Ascend Access Control Ascend distributed Ascend RADIUS server source code. Ascend RADIUS and Ascend Access Control are compatible, although some of the differences in the programs are noted in the sections that follow. The items listed in "Attribute differences," are explained in Chapter 6, "Creating Example Client, User and Realm Entries." The items listed in "Operational differences," are discussed in Appendix A, "Ascend Access Control files and commands."

Note: Ascend Access Control does not support the `builddbm` utility for indexing the user profiles in the `users` file. If you have used the `builddbm` utility for Ascend RADIUS implementations, the "Note about the RADIUS builddbm utility" on page 7-3 explains why Ascend Access Control does not support indexing of `users` files.

Attribute differences

- Changing passwords
  - A new names is assigned to an attribute that defines how a user can change passwords during authentication
  - The Ascend Access Control RADIUS daemon requires a new command line option, `-P`
- Specifying a Token Card
  - Ascend Access Control is not run with a daemon option to reserve values to identify token cards
  - Authentication-Type attribute values are automatically reserved to identify token cards
  - Ascend Access Control does not reserve Password attribute values
- AppleTalk Remote Authentication (ARA)
  - Ascend Access Control uses a new Authentication-Type attribute value to add ARA authentication to a user profile
  - Ascend Access Control uses a new value to indicate ARA is a user's `Framed-Protocol`
- Identifying Network Access Servers (NAS) Vendors
  - Ascend Access Control provides a means of identifying the vendor who manufactures a NAS
  - Based on the vendor identification, Ascend Access Control only sends appropriate vendor-specific attributes to the NAS
- New attribute names
  - Ascend Access Control supports attribute names as they appear in the IETF RADIUS RFC, not the RADIUS draft

Operational differences

- Reading changes in data files
  - Ascend Access Control does not re-read the files when a change is made in the `clients` or `users` files
- Ascend Access Control supports new daemon command line options
  - `-C` allows token-caching

  - `-f` changes the default finite state machine file which monitors the status of authentication requests
  - `-g` changes the default location where the log `radiusd` activities is sent
  - `-h` activates help
  - `-k` provides key information
  - `-oa` stores accounting information in an ODBC DBMS
  - `-P` allows password changes
  - `-p` changes the authentication port (this supports the standard, but is different than the Ascend free RADIUS
  - `-pp` changes the default relay authentication port
  - `-q` changes the default accounting port
  - `-qq` changes the default relay accounting port
  - `-r` changes the first default separator in a realm-aligned user's user name
  - `-rr` changes the second default separator in a realm-aligned user's user name
  - `-t` sets the timeout limit for the authentication request
  - `-z` removes old `logfile` at startup
- Debugging
  - Ascend Access Control automatically sends debugging information to a file called `radius.debug` instead of to `stderr`

User's Guide Summary

This list summarizes the information in chapters 2 through 7 of the Ascend Access Control User Guide and the appendixes of the Ascend Access Control References. Chapters 2 through 4 constitute a quick start guide for experienced RADIUS users.

Ascend Access Control User Guide

Chapter 2, "Quick Setup," is the first of three chapters written for users who already understand RADIUS authentication and authorization and want to start using the Ascend Access Control graphical interfaces. It describes how to plan for and set up Ascend Access Control and lists the RADIUS daemon options that control the location of the Ascend Access Control data directory, the server's authentication and accounting ports, and the depth of information collected when debugging is turned on.

Chapter 3, "Installing Ascend Access Control and its graphical user interfaces,"describes how you install demonstration copies of Ascend Access Control and obtain a temporary 30 day license key. The chapter is also an introduction to Access Control Manager and User Account Wizard, the Ascend Access Control graphical user interfaces, and the programs' on line help.

Chapter 4, "Configuring Ascend Access Control Files," is a tutorial for using the Access Control Manager and User Account Wizard interfaces to create entries in users, clients and authfile data files. users files contain user profiles.

Chapter 5, "Understanding Ascend Access Control," explains how Ascend Access Control communicates with Network Access Servers (NAS), which initiate authentication requests. The explanation describes RADIUS attributes and values, RADIUS accounting and the Ascend Access Control data files.

Chapter 6, "Creating Example Client, User and Realm Entries," is another tutorial explaining the format of the users, clients, and authfile files. The focus of this chapter is manual editing of the data files to create clients, users and realms. The chapter also explains Ascend Access Control utilities.

Chapter 7, "Open Database Connectivity (ODBC),"explains how you can set up a link between Ascend Access Control and ODBS-compliant Database

Management Systems (DBMS).You can use DBMS tables in lieu of the server's users file to store user profiles.

Ascend Access Control References

Appendix A, "Ascend Access Control files and commands," contains information presented in the format of UNIX man pages.

Appendix B, "Attributes Reference," is a list of Ascend Access Control attributes. In addition to RADIUS attributes, the list includes and vendor-specific attributes developed by Ascend Communications.

Appendix E, "MAX Accounting codes," is a collection of tables that explain the accounting codes supported and used by the Ascend MAX family of routers.

Quick Setup

2

This chapter begins a quick start guide that includes Chapters 3 and 4. Together, they provide information experienced RADIUS users need to install and to use Ascend Access Control and its graphical user interfaces. If you don't know how RADIUS authenticates and authorizes users, read Chapter 5, "Understanding Ascend Access Control," and Chapter 6, "Creating Example Client, User and Realm Entries."

Planning to set up Ascend Access Control

Following are preparations you should take to set up Ascend Access Control.

1. Review the Ascend Access Control attributes.

   Appendix B, "Attributes Reference," contains descriptions and values of Ascend-specific and RADIUS authentication, authorization and accounting attributes. Ascend Access Control's `dictionary` file is also a list of the attributes.

2. Gather information about the Network Access Servers (NAS) and other authentication servers that will be your Ascend Access Control server's clients.

3. Gather information about individual users that you will enter in the `users` file's profiles.

   Steps 2 and 3 are the most time consuming. You might be able to collect user information from an existing user database. If your NAS clients are Ascend units, you might find useful information in the units' Answer and Connection profiles.

4. Decide if the users Ascend Access Control authenticates should be separated into realms.

   Realms are discussed in "Understanding authfile" on page 4-22.

5. Decide where to install Ascend Access Control on the workstation.

   You can create a directory for the program, or accept the installation script's default location. The default is `/etc/raddb` on UNIX machines and `C:\Ascend\Access_Control` on Windows NT machines. The directory and other default settings, such as the RADIUS authentication and accounting ports, work for most installations, but you can change them using the `radiusd` command line options listed in Table 2-1.

6. Read the Ascend Access Control `README` file.

   Information that differs from the steps outlined here, and elsewhere in the Ascend Access Control User Guide, might be included in a `README` file.

Default Ascend Access Control settings

`radiusd` is the RADIUS daemon. A discussion of `radiusd` is in Appendix A, "Ascend Access Control files and commands." Table 2-1 lists the daemon command line options and their default settings. You can change the default settings.

Table 2-1. RADIUS daemon command line options

Option	Description	Default
`-a`	Accounting directory Location of accounting detail file	`/etc/radacct`
`-C`	Allow token caching	Not enabled
`-cwd`	Current working directory Only affects file system operation for files with no relative file names	`/etc/raddb`
`-d`	Data directory Location of `dictionary`, `clients`, `authfile`, and `users` files	`/etc/raddb`
`-f`	Finite State Machine (FSM) file Table describing machine state	`radius.fsm`
`-g`	Logging Style for logging warning, error and informational messages	Enabled. Output to `logfile`.
`-h`	Help messages Sends help messages to standard output	Not enabled
`-p`	Authentication port Port receiving authentication requests	1645
`-q`	Accounting port Port receiving accounting information	1646
`-pp`	Alternate authentication relay port Port for relaying request to proxy server	1645 (same as authentication port)

Option	Description	Default
`-qq`	Alternate accounting relay port Port for relaying information to proxy server	1646 (same as accounting port)
`-s`	Ascend Access Control processing mode How Ascend Access Control handles each request	Multi-thread process
`-t`	Timeout Time server will wait during inactivity before timing out	Fifteen (15) minutes
`-v`	Display Ascend Access Control version number to standard output	Not enabled
`-x`	Debugging Level of debugging output	Not enabled When enabled, `radius.debug` is default file to receive information
`-z`	Empty logfile and debug file Not applicable if debugging is not enabled or if syslog is used for logging.	Not enabled

Installing Ascend Access Control and its graphical user interfaces

3

Chapters 3 and 4 explain Ascend Access Control's graphical user interfaces (GUIs). Experienced RADIUS users can read chapters 3 and 4 and begin to configure Ascend Access Control data-files.

- Chapter 3 reviews installation of the software, obtaining a license key, and configuring files with the Access Control Manager and User Account Wizard graphical user interfaces. You must obtain a license key from Ascend to use permanent and demonstration copies of Ascend Access Control.
- Chapter 4 explains how to use the Access Control Manager and the User Account Wizard to configure the data files Ascend Access Control consults for authentication, authorization and accounting.

Who should read this chapter

This chapter and the next were written for experienced RADIUS users who want to install and use Ascend Access Control's graphical user interfaces, Access Control Manager and User Account Wizard. This chapter also contains instructions for downloading a demonstration copy of Ascend Access Control and obtaining a thirty day license key for those who want to review the program's authentication and authorization functions.

You should be familiar with RADIUS if you plan to install and configure Ascend Access Control before reading Chapter 5, "Understanding Ascend Access Control," and Chapter 6, "Creating Example Client, User and Realm Entries,". Some Ascend Access Control features discussed in chapters 3 and 4, such as realms, go beyond standard RADIUS. The concept of user realms and the configuration of Ascend Access Control's `authfile` file should not be difficult for experienced RADIUS administrators.

Technical Support

Contact the Ascend Technical Support Center at 1-800-ASCEND4 if you need help. The center is open Monday through Friday 6:00AM to 6:00PM PST.

Installing AAC demonstration software

Ascend Access Control is a binary distribution. You can download the demonstration program from the Ascend FTP server, but you must purchase a permanent version of Ascend Access Control to use the program for more than thirty (30) days. Read the text file named `README` before installing either version of Ascend Access Control. The file may include new or updated material that is not in this guide.

The Ascend Access Control installation instructions in this section are brief and describe how to install the demonstration version of Ascend Access Control. Chapter 6, "Creating Example Client, User and Realm Entries," contains instructions for installing a permanent version of Ascend Access Control.

Following are steps that install Ascend Access Control server demonstration software. The first series of steps describe how to install the software on a UNIX machine if you do not use an utility such as `pkgadd` or `swinstall`. If you have questions about how to use an installation utility, obtain the utility's man page. Steps describing an Ascend Access Control for Windows NT installation follow the UNIX instructions.

For UNIX installations:

1. Make sure you have root privileges on the Ascend Access Control server.
2. Use a web browser that supports frames to access Ascend's web site at http://www.ascend.com.
3. Follow the links from Ascend Products to Security Product Family to Ascend Access Control.
4. Click to Download Ascend Access Control demonstration software.
   Copy the Ascend Access Control compressed tar file to the server. Do not copy the file in the `/etc/raddb` directory because the Install script places the program's files in that directory.
5. Uncompress and untar the compressed tar file.
6. Run the uncompressed `Install` script to install Ascend Access Control.
7. Create three files named `authfile`, `clients` and `users` in the program's directory. These are Ascend Access Control's data files.

Note: Ascend Access Control includes examples of `authfile`, `clients` and `users` files. The example files carry the extension `.ex,` such as `clients.ex.` You might copy examples from these files to the new `clients`, `authfile` and `users` files.

For Windows NT installations:

Steps 1 through 4 are the same as a UNIX installation.

5. Ascend Access Control for Windows NT is self-installing. Double click on the `.exe` file that you downloaded to start the `Install Shield` program.
   Ascend Access Control for Windows NT creates data files for you.

Obtaining a temporary Ascend Access Control license key

You can use Ascend Access Control on a trial basis for thirty (30) days when you download it from the Ascend FTP site. However, the program and its graphical user interfaces will not work until you obtain a temporary Ascend Access Control license key. To obtain your key:

1. Use a web browser that supports frames to access Ascend's web site at

   http://www.ascend.com.
2. Click the links that refer to downloading demonstration software.
3. Click to accept the terms of the software license agreement.
4. Enter the requested information, including your email address, in the labeled textboxes in the screen's right frame.
5. Click Submit

   Your license key appears at the bottom of the WWW client's screen.
6. If your server is a UNIX machine, create a file called `licenses` in the directory where Ascend Access Control is installed.

   If your server is a Windows NT machine the `licenses` file is created when you install the Ascend Access Control for Windows NT demonstration software.
7. After a short time, check your email for a message containing instructions for entering the key in the `licenses` file.

   The message also contains a copy of the Ascend Access Control key that appeared in the WWW page.

The graphical user interfaces

You can use two graphical user interfaces (GUIs), the Access Control Manager and the User Account Wizard, to edit entries in the Ascend Access Control program's data files. The interfaces are Java applications and they are not installed on the server when you install the Ascend Access Control program. You must install them if you want to use them. Because both interfaces can create or edit data file entries, they must be on machines which can read and write to the server's `authfile`, `clients`, `users` and `templates` data files.

The Access Control Manager can perform many system administration and data entry functions, including adding users, clients and realms in the Ascend Access Control `users`, `clients` and `authfile` files. Access Control Manager also enables you to create templates for user profiles, which you can save in a file called `templates`. The `templates` file is created when you install Access Control Manager. It is not created when you install the Ascend Access Control program. The User Account Wizard is a simpler interface that only enables someone to create and edit Ascend Access Control's user profiles.

Configuring the GUIs

When you install Access Control Manager, a file called `config.acm` is copied to the Ascend Access Control data directory. The `config.acm` file is a simple text file that contains lines that define the Access Control Manager's default configuration. You can change the default configuration entries in the `config.acm` file with a text editor or by clicking on the *Setup AACM* button on the Access Control Manager's first screen and changing the selections on the GUI's *Setup* screen. The `config.acm` file defines how the Access Control Manager performs various tasks, including:

- Locating the Ascend Access Control data files
- Sorting the attributes in the dictionary file
- Identifying the names of the Ascend Access Control data files
- Creating automatic backups of edited data files
- Displaying selected attributes contained in user profiles

The User Account Wizard's configuration can be the same as, or different than, the Access Control Manager's configuration. If you install both GUIs on the Ascend Access Control server you should install one `config.acm` file on the server that defines the location of the Ascend Access Control data directory. Both GUIs should get their configuration from that `config.acm` file because you will want both GUI's to be able to edit the same Ascend Access Control data files.

If you install the User Account Wizard on another machine you must create a `config.acm` file on that machine. The User Account Wizard's configuration file can be different than the configuration file for the Access Control Manager on the server. For example, you can give the User Account Wizard Simple editing

privileges and give the Access Control Manager Advanced editing privileges. The differences between Simple and Advanced editing levels are described in the section "The GUIs Simple and Advanced editing levels," in this chapter.

Creating the User Account Wizard configuration file

When you install the User Account Wizard on a separate machine, you must use make a copy of a `config.acm` file and place it on the User Account Wizard's machine. Installing the User Account Wizard's installation process does not create a `config.acm` file. You can create the file via the Access Control Manager's *Setup AACM* function or copy the Access Control Manager's `config.acm` file, edit its entries with a text editor, and save the file on the User Account Wizard's machine.

Note: If you use the Access Control Manager to create a different `config.acm` file for the User Account Wizard you will change the Access Control Manager's `config.acm` file in the process. Save a copy of the Access Control Manager's `config.acm` in a different directory or under a different name so you can restore the file later. If you plan to install the User Account Wizard application on more than one machine, create and save one `config.acm` file that you can copy to each machine. For discussion of stand-alone User Account Wizard installations, see "Installing a stand-alone User Account Wizard application" on page 3-11.

The GUIs Simple and Advanced editing levels

The data entry functions you can perform with the Access Control Manager and the User Account Wizard depend on which of two editing levels you set in a file called `config.acm.` This file is created when you install the GUIs. The editing levels are Simple and Advanced. You must use Access Control Manager to set the editing level in `config.acm`. You cannot use User Account Wizard to set the editing levels.

Following are the actions you can perform with Access Control Manager when you have set the editing level to Simple:

- Create or edit user profile templates.
- Create or edit Network Access Server (NAS) entries in the `clients` file.
- Create or edit user profiles in a `users` file.

Advanced editing mode enables you to edit entries in the data files that affect user realms.When Access Control Manager is in the Advanced editing mode you can perform the following actions and the Simple editing mode actions:

- Create or edit realm entries in the `authfile.`
- Create or edit user profiles in multiple `users` files.

You can also use Advanced and Simple modes in the User Account Wizard. However, you can only use the User Account Wizard to create or edit user profiles in the `users` file. You cannot use the User Account Wizard to create or edit entries in the `templates`, `clients` or `authfile` files.

Backing up Ascend Access Control data files

You can set `config.acm` so that any files you open are backed up any before you use either GUI to create or edit data file entries. Click the appropriate box under the heading `Create backup Files for:` on the Access Control Manager Setup screen. For example, you might turn on the automatic backup function for `users` and `prefix.users` files by checking the User File box.

If you check the User File box before entering the first user profile in an empty `users` or `prefix.users` file, Access Control Manager immediately creates an empty backup file called `users.bak` or `prefix.users.bak` when you save the first user profile.

Locking data files while editing

Opening a data file to add or edit an entry locks the file so that no one else can edit and save changes in that file while you are working with it. The lock is removed when you close the editing screen after saving your changes or canceling them.

Understanding the Access Control Manager

Access Control Manager is Ascend Access Control's master GUI. You can install it on a machine other than the Ascend Access Control server if the GUI can access Ascend Access Control's data files. The interface has six editing screens which provide all the tools to set up the both GUIs, create and edit entries in all of

the Ascend Access Control data files and edit and create user profile templates. The GUIs screens include:

- Setup AACM
- Edit Realms
- Edit Clients
- Edit Users (primary - accessible from the Home screen)
- Edit Users (secondary - accessible from the Primary Edit Users screen)
- Edit User Templates (primary and secondary screens)

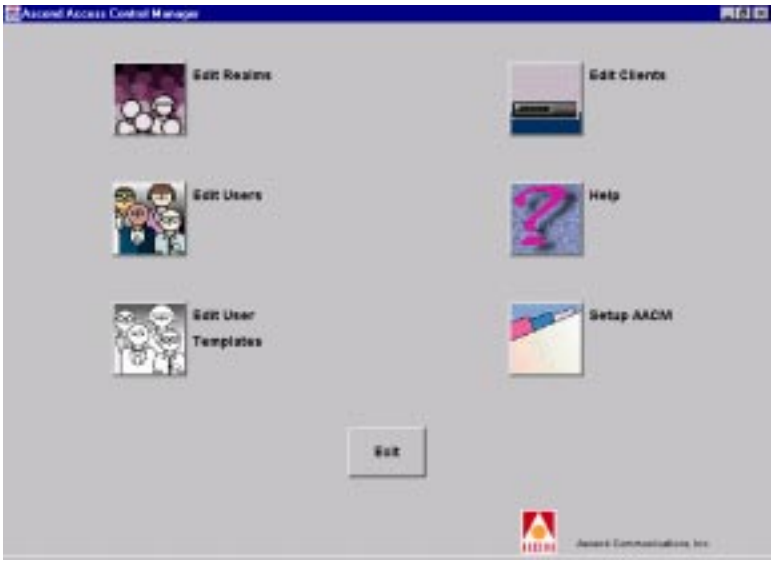


Figure 3-1. Access Control Manager's main screen.

Access Control Manager GUI configuration functions

You can use Access Control Manager's administrative Setup AACM functions to set the `config.acm` file's configuration for:

- The GUI's editing level.
- The location of the Ascend Access Control data directory.
- The GUI's automatic back up function for Ascend Access Control data files.

Locating and starting the Access Control Manager

You can only install the Access Control Manager on a machine running Windows 95 or Windows NT. Follow the README file's instructions to install Ascend Access Control from files you download from the Ascend Web site or the Ascend Access Control CD-ROM. Run `setup.exe`, a file that is copied to the machine's hard drive, to start the Install Shield program that installs Access Control Manager. By default, Install Shield creates a directory called `C:\Ascend` and places Access Control Manager's files there. When the Install Shield finishes, you can select the Access Control Manager icon in the Ascend program group to start Access Control Manager.

Understanding the User Account Wizard

The User Account Wizard is Ascend Access Control's graphic interface for working strictly with Ascend Access Control's `users` files. Like Access Control Manager, you can install the User Account Wizard on the Ascend Access Control server or another machine that can access the server's Ascend Access Control files. The interface has three editing functions:

- Add a User
- Modify a User

- Delete a User

Figure 3-2. User Account Wizard's main screen.

The User Account Wizard can not create or edit a `config.acm` file. The User Account Wizard's purpose is to provide easy, but limited, data entry services confined to user profiles. A typical User Account Wizard installation might be one which is used by a person in a customer service office who adds user profiles for new customers or changes existing customers' password entries.

Locating and starting the User Account Wizard

You can only install the User Account Wizard on a machine running Windows 95 or Windows NT. The installation process is the same as the one described in "Locating and starting the Access Control Manager" on page 3-9. The Install Shield program installs the User Account Wizard in a directory called C:\Ascend and places the User Account Wizard's files there. You can start the installed program by selecting the program icon created by Install Shield.

Installing a stand-alone User Account Wizard application

After installing the Access Control Manager, you can install the User Account Wizard as a stand-alone application on different machine. Proceed as follows:

1. Double-click the Access Control Manager's Setup AACM icon.
2. Enter the path to the Ascend Access Control data directory containing the `users`, `clients`, `templates` and `authfile` files.
3. Select the appropriate editing mode for the User Account Wizard.

   Typically, a stand-alone User Account Wizard should be configured to allow Simple editing privileges, preventing the wizard's users from viewing or editing user profiles in multiple `users` files.
4. Select the file backup and sorting options, if appropriate.

   Close the Access Control Manager application when you have selected all the Setup options you want in the wizard's configuration file.

   The `config.acm` file in the Access Control Manager's directory now contains the User Account Wizard configuration.
5. Install the User Account Wizard on the machine where it will be used to create or edit user profiles.
6. Copy the Access Control Manager's `config.acm` file to the User Account Wizard's directory on the machine running the wizard.
7. Store the new copy of `config.acm` file for use in subsequent User account Wizard installations.

Using the User Account Wizard

The icons on the home screen of the User Account Wizard represent the user profile editing screens. Choose an editing screen by clicking on the appropriate icon.

The User Account Wizard resembles other applications described as wizards or coaches. It progresses step-by-step through the creation, deletion, or modification of a user profile, moving forward when you select a button labeled Next. You may also return to a previous screen or cancel the process at any time. At the end of the procedure, select a button labeled Finish, then respond to the prompts to end the session.

Accessing On Line help for the GUIs

Two forms of on-line help are available for Access Control Manager and User Account Wizard. You can access plain-text help by clicking on any editing screen's help button and you can access HTML documents through a World Wide Web browser.

Plain text help

You can access plain text help files from the Access Control Manager's home screen and from each of its editing screens. Clicking on the help button does not change the cursor's functionality, so you can click on a screen object for context-sensitive help. However, clicking on help does display the plain text files that explain basic information about the screens' functions.

Each plain text file begins with a description of the file's contents, explaining what you may edit and configure from the editing screen you are working with. The rest of the document explains how you perform those functions.

Each plain text help document appears in a java window that can be resized. Use the scroll bar to the right of the text to move the text up or down.

When you finish, close the help window by clicking the OK button at the bottom of the screen.

HTML help

Ascend Access Control also provides another set of help files that contain hypertext markup text links (HTML). To use them:

1. Open your WWW browser.
2. From the File menu, choose Open.
3. Display the Ascend Access Control data directory.
4. Open the file Alphabet.htm
   The main HTML help screen appears (Figure 3-3).

5 Click on a letter to jump to index entries that start with that letter.

6 Double-click on an entry to display the corresponding help topic.

Figure 3-3. Alphabet.htm, the main HTML help screen. The table of alphabet characters provides hypertext links to individual help screens.

The Ascend logo in the upper left hand corner of each help file is a link back to the main help screen. Hypertext links are blue and underlined. Previously selected hypertext links are light blue. The icons at the bottom represent the Access Control Manager's functions for editing realms, users, templates, clients and graphical user interface configuration, respectively.

Ascend Access Control HTML help files have been tested for viewing compatibility with Netscape Navigator, version 3.0b6Gold, and NCSA Mosaic, version 2.1.1.

Configuring Ascend Access Control Files

4

This chapter contains descriptions of Ascend Access Control's `users`, `templates`, `authfile` and `clients` files and explains how to use the Access Control Manager and User Account Wizard to configure these files.

The configuration process

The information you gather as you prepare to configure Ascend Access Control should indicate whether you will benefit by grouping users in realms. Follow all of the steps in "Configuration steps," below, if you have determined that realms are beneficial for authenticating and authorizing your user community. If you determine that user realms are unnecessary, skip step 2 "Add realms in `authfile`".

Although the order of the configuration steps is arbitrary, users cannot be defined by their realms if you have not created a list of realms they can belong to. Also Ascend Access Control checks the `users` file before checking the `authfile`, even if users are grouped in realms.

Many system administrators do not enter individual user profiles in the `users` file. They only create a DEFAULT user in the `users` file and a DEFAULT realm in the `authfile.` The first line they create for the DEFAULT user profile contains the attributes Password and Authentication-Type. They enter `UNIX` as the Password value and `Realm` as the Authentication-Type value. In the DEFAULT realm entry in the `authfile` they enter `File` as the value for the Realm/DNS/File field and a name in the Prefix field. These actions:

- Prevent people with access to the `users` file from reading user passwords because the passwords are stored in the server's `/etc/passwd` file.
- Similarly protect user authentication and authorization attributes because they are not stored in the `users` file, but in a file named *.`users,` where * is the name entered in the DEFAULT realm's Prefix field.

Configuration steps

Following are the steps to configure Ascend Access Control:

1 Add a DEFAULT user in the `users` file.

2 Add realms in `authfile`, including a DEFAULT realm.

3 Add clients in `clients` file.

4 Add users in `users` file.

Understanding users files

A `users` file is a list of user profiles containing attribute/value pairs. The people the profiles define are users Ascend Access Control can authenticate for an NAS or a server listed in the `clients` file.

You may create one `users` file or many `users` files for the Ascend Access Control server. If you organize users into realms, as explained in "Understanding authfile" on page 4-22 you can create separate `users` files for each realm. For example, you might create a file named `ournet.users` to contain the profiles of users associated with a realm called *Ournet*. A prefix such as *ournet* is derived from the value of the Realm/DNS/File field in an `authfile` realm entry. The realm's Type field value must be *File* to enter a name in the Realm/DNS/File field. See "authfile(5)" on page A-2 for more information about the fields in `authfile`.

Users file attributes

You can only enter in a `users` file the attributes that appear in the `dictionary` file. User profile attribute/value pairs are classified as either check-items or reply-items.

Check-items are attribute/value pairs Ascend Access Control compares to the attributes/values it receives from a client to authenticate a user.

Reply items are attribute/value pairs Ascend Access Control sends the client to authorize a link and services if authentication is successful.

If authentication fails, Ascend Access Control typically sends an attribute/value containing a message about the authentication failure.

Users file format

The `users` file is installed in the `/etc/raddb` directory. However, you may reconfigure Ascend Access Control to use a different directory. (For more information on changing Ascend Access Control defaults, see "Default Ascend Access Control settings" on page 2-3.)

A `users` file may contain general comments about the file and separate comments about individual user's profiles. Each user profile contains one line of check-items for authentication and, possibly, one or more lines of reply-items for authorization. Although the Access Control Manager does not provide a view of the `users` file, this is the format of the entries:

```
#Comment

username check-item [, check-item]...

   reply-item,

   reply-item
```

Example users file entry

A `users` file entry viewed with a text editor looks like this:

```
#This user began it all.
gwash@whitehse Password=paterusa
   Service-Type=Framed,
   Framed-Protocol=PPP,
   Framed-IP-Address=105.23.0.1,
   Framed-IP-Netmask=255.255.255.0
```

Editing a users file with Access Control Manager

You can use either Access Control Manager or the User Account Wizard to create or edit user profiles in any `users` file or `prefix.users` file. The material that immediately follows describes how to create and edit user profiles with the Access Control Manager application. To see how the User Account Wizard deals with user profiles, read "Editing users files with User Account Wizard" on page 4-18.

User profile templates

When you create a user profile with either application, you can begin by selecting a template that contains most or all of the attributes and values you want in that user profile. The example `users` file entry described in the section "Users file format" on page 4-3, could be developed from a template for users who dial in using the PPP protocol. Such a template would include all the attributes and some of the values that appear in the example. Using that template to create user profiles, you would only add values that describe an individual user, such as those for Password and Framed-IP-Address.

Templates can only be created with the Access Control Manager although you can use templates to create user profiles in the User Account Wizard. The process of creating templates, which is very similar to that of creating a user profile is described in "Creating user profile templates" on page 4-15.

Access Control Manager Edit User screens

The Access Control Manager has two Edit User screens. In the procedures that follow they are referred to as the *primary* and *secondary* Edit Users screens. To use the edit screens:

1 From the Access Control Manager home screen, click the Edit Users icon.

The Access Control Manager loads the Ascend Access Control `dictionary` file.

2 Select a realm of users to edit.

The Access Control Manager loads the selected `users` file and the primary Edit Users screen appears (Figure 4-1).

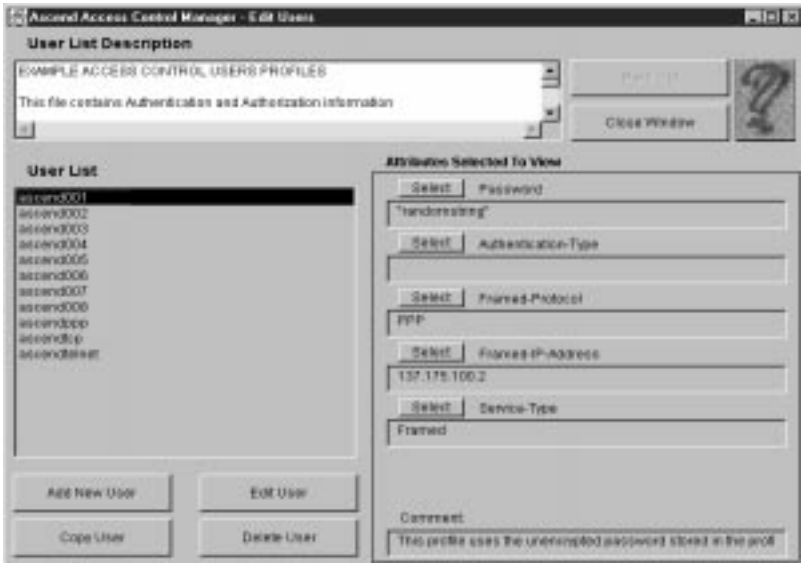


Figure 4-1. Access Control Manager primary Edit User screen.

Primary Edit Users screen

The primary Edit Users screen contains the following elements:

- User List
  A scrolling textbox listing user profiles
- Attributes Selected to View
  Values of selected user profile attributes
- Four editing buttons
  Add New User, Copy User, Edit User and Delete User
- Two comment textboxes
  User List Description and Comment
- Save List, Close Window and Help buttons

Secondary Edit Users screen

The secondary Edit Users screen appears when you select a user profile from the primary screen's User List and click the Edit User button. It contains the following elements:

- Username textbox.
- User Authentication Attributes section.
  Columns for editing authentication attribute/value pairs.
- Connection Configuration Attributes section.
  Columns for editing authorization attribute/value pairs.
- Four attribute editing buttons.
  Insert Attribute, Delete Attribute, Delete All Attributes, and Copy Template.
- Commit and Close Window buttons.
-

Editing users file comments

The textbox labeled User List Description on the primary Edit User screen contains comments about the `users` file. They can be general comments that describe the user profiles in this particular `users` file, when it was last updated, or the realm associated with this `users` file. To enter new comments:

1 Click in the textbox where you wish to type your comments
The textbox scrolls and you may overwrite, insert new lines between, or append new lines at the end of the existing comments.

2 Type your comments.

Editing User profiles

Editing profile attribute snapshots

A snapshot is a quickly captured image that can identify a larger event or setting. The Edit User screen snapshot is a short list of attributes you select to help you identify the user whose name is highlighted in the User List.

Values for some of a profile's attributes are displayed in textboxes at the right of the primary Edit User screen. As you scroll through the User List, the values displayed in the textboxes are those of the currently selected user. You can change the displayed attributes.

Note that you cannot edit the values in the textboxes from the primary Edit User screen. You have to use the secondary Edit User screen for that. At the primary screen:

1 Click on the Select button above a textbox where you want to view a different attribute.

The secondary Edit User screen appears. It includes a drop-down list of all the attributes in the Ascend Access Control `dictionary`.

2 Click on the attribute whose value you want displayed in the textbox.

Values for this attribute are displayed in the textbox until you next edit the Attributes Selected to View. The currently selected attributes will be in place the next time you access the Edit User screen.

Editing the User List

The four buttons below the scrolling User List box provide functions for adding users and editing, copying and deleting user attributes.

Before choosing to edit, copy or delete a user, select a user from the list by clicking on a name in the User List box. Copied profiles appear below the profile that was selected. Before Ascend Access Control deletes a user from the list a warning dialog box demands confirmation of the action. New users are added at the top of the list if no current user has been selected, otherwise the new user is inserted in the list below the user whose name is highlighted.

Editing user attributes

You edit a user profile's attribute/value pairs from the secondary Edit User screen. At the primary screen:

1 Select a user from the User List to edit, or create a new user with the Add New User or Copy User buttons.

2 Click the Edit User button or double click on the selected user to display the secondary Edit User screen (Figure 4-2).

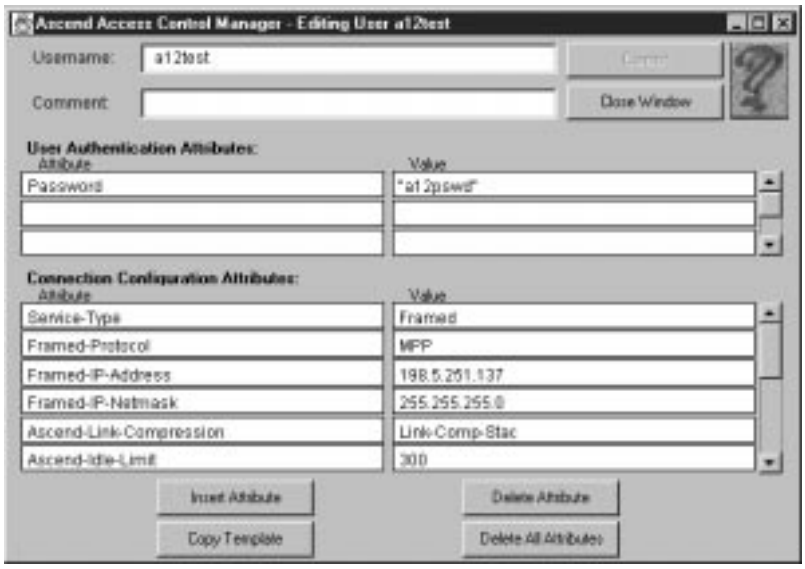


Figure 4-2. Access Control Manager secondary Edit User screen.

You can edit any of the secondary Edit User screen's textbox entries. Attribute/value pair textboxes are grouped into three areas of the screen, as follows:

- Username

  Displays the value of the profile's user-name attribute.

- User Authentication Attributes

  Displays check-item attributes and their values. These are the attribute/value pairs Ascend Access Control uses to authenticate a user. Ascend Access Control compares these attribute/value pairs to those for the check-items it receives from clients in Access-Request packets.

Caution: Do not indicate that the user authenticates with a token card by entering `ACE`, `Defender`, or `S/Key` as the value for the Password attribute. You were required to do this if you authenticated users with Ascend's free RADIUS program. Instead, enter those strings as values of Ascend Access Control's Authentication-Type attribute. Please note that although a Password attribute and an Authentication attribute can be part of the same user profile, you cannot enter `ACE`, `Defender`, or `S/Key` as Password values.

- Connection Configuration Attributes
  Displays the reply-item attribute/value pairs that Ascend Access Control sends to the NAS after successful user authentication. These attribute/values are the instructions the NAS uses to configure the user's connection.

Username attribute

When you need to edit the user's name or are creating a new user profile based on an existing profile, click in the textbox and type a new user name.

Authentication and Configuration Attributes

Following are steps to edit authentication and configuration attributes:

1. Click in the textbox you wish to edit.
   A button with an arrow appears at the right of the textbox, indicating that a drop down list is available.
2. Click on the arrow button.
   The list that appears contains all the attributes in the `dictionary` file.
3. Select one of the visible choices.
   Use the mouse cursor or the keyboard direction/paging keys to find a new attribute.
4. Click on the new attribute you want to add to the user profile.

Entering a connection configuration attribute more than once in a user profile

It is possible, and in some cases necessary, to enter the same connection-configuration attribute more than once in a user profile. If this occurs by accident, the Network Access Server that receives the attributes should still establish a connection for an authenticated user. The NAS will set up the connection using the last value it reads for the duplicated attribute.

For example, suppose you inadvertently include the attribute Service-Type twice in the same user profile. You enter `Framed` as the value of the first entry and `Login` as the value of the second entry. The NAS receives Ascend Access Control's Access-Response packet containing these attribute/value pairs and reads Service-Type=Framed then Service-Type=Login. The NAS will set up a

login connection rather than a framed connection because Login is the last value it receives for the attribute Service-Type.

An example of an attribute that should appear more than once in a user profile or user template is the Ascend-Menu-Item attribute. You can use this attribute to create a text message on an authenticated user's screen. The message generally provides a menu from which the user may select one of several options.

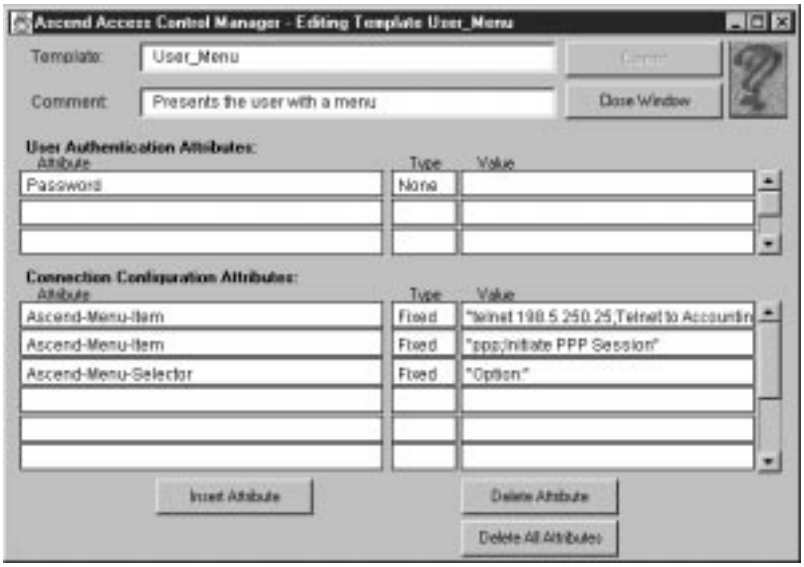


Figure 4-3. Access Control Manager Edit User Template screen displaying Ascend-Menu-Item attributes.

The Access Control Manager's Edit User Template screen (Figure 4-3) shows a typical use of multiple Ascend-Menu-Item attributes in a single template. A user profile based on this template will display the following message for the user:

```
1. Telnet to Accounting
2. Initiate PPP Session
      Option:
```

Editing attribute values

The procedure for editing values is the same as that for editing attributes. Values for an attribute appear in a drop down list if the values are limited and defined in the Ascend Access Control `dictionary`. If the values are not defined in the `dictionary` you can enter a value by typing it in the textbox. To edit a value:

1. Select an attribute.
2. Select the textbox containing the attribute's values.

   The attribute's values are in the textbox to the right of the attribute.
3. Follow the procedure described in "Editing user attributes" on page 4-8 or type in a value.

Editing an attribute/value row

You can add or delete rows of attribute/value pairs in the secondary Edit User screen's Authentication and Configuration Attributes sections. An inserted row appears below the currently selected attribute. After selecting an attribute, click the Insert Attribute or Delete Attribute button.

Editing user profile file comments

You can add comments about individual user profiles as follows:

1. Click in the last textbox on the right of the screen.

   The textbox displays one line of comments at a time, although you can type as many lines as is necessary. The lines wrap when you reach the edge of the textbox.
2. Enter new comments, or overwrite existing comments

Saving or canceling edits of user profiles

When you edit user attribute/value pairs on the secondary Edit User screen, the changes are not permanently saved to the `users` file. They are written temporarily into memory when you click on the screen's Commit button. The entire `users` file is saved permanently, along with the changes in the temporary memory, when you click the Save List button on the primary Edit User screen.

You can click the Close Window button on either of the Edit User screens to discard the changes you have made to user profiles. Clicking the button on either screen causes a dialog box to appear that asks if you want to save changes to the user list. Your options are Yes, No, and Cancel. When you close the window from the primary Edit User screen you cancel all the edits you have made to any user profiles during your editing session. When you close the window from the secondary Edit User screen's you cancel the changes to the current user profile and return to the primary Edit User screen.

Understanding user profile templates

User profile templates are stored in a file called `templates`, which is created when Ascend Access Control is installed. By default the `templates` file is placed in the `/etc/raddb` directory, along with `clients`, `users`, and `authfile` files.

You may choose to place these files in a different directory during installation. If you do place them elsewhere, you must identify the location of that directory by entering it in the Access Control Manager Setup screen's data directory textbox.

The information you place in the textbox is stored in the `config.acm` file. Remember that the User Account Wizard must also know where the files are, even if that application is on a different machine. Take the necessary steps to include the data-directory location in the User Account Wizard's `config.acm` file (as discussed in "Creating the User Account Wizard configuration file" on page 3-6).

User profile template format

This is an example of an entry for a dial in user template in the `templates` file. It's format is very similar to the format of a user profile in a `users` file or `prefix.users` file. The only noticeable difference is the additional lines that appear at the end of the template entry. The numbers in the final two lines indicate the editing type of the attribute's values. The number *3* in the next to last line of the example is the editing type for the value of the Password attribute. The initial number *1* in the last line is the editing type for the value of the Service-Type attribute.

```
Dial-in-User Password = “xxx”
 Service-Type = Framed,
 Framed-Protocol = MPP,
 Framed-IP-Address = 0.0.0.0,
 Framed-IP-Netmask = 255.255.255.0,
 Ascend-Link-Compression = Link-Comp-Stac,
 Ascend-Idle-Limit = 300,
 Framed-Compression = Van-Jacobson-TCP-IP
3
1 1 3 2 1 1 1
```

Note: Please bear with the proliferation of *types* in Ascend Access Control. In addition to editing types in templates, you will also find references in the User Guide to a Realm field called Type, and some attributes that include the word *type* in their names, such as Authentication-Type and Service-Type.

Assigning attribute-value editing types

The primary difference between creating a user profile and a user template is the assignment of an editing type to the values of the template’s attributes.

A value’s editing type determines whether or not you can change that value when using the template to create a user profile. The editing types for attribute values follow, along with the numbers that represent the editing types in the `templates` file:

- None (3)
  None means that the attribute value in the template must be altered when the user profile is created. In the example, the Password attribute should have an editing type of None so that a Password other than “xxx” must be entered in the user profile.
- Default (2)
  Default means that the creator of the user profile may retain the template’s attribute value in the user profile. The value of the Framed-IP-Netmask in the example has a Default editing value because 255.255.255.0 might be suitable for most user profiles created with the template. When the value is not suitable, the user can change it.

- Fixed (1)
  Fixed means that the templates attribute value must be retained in the user profile you create from the template. When you create a user profile from a template with the User Account Wizard, the application does not even display the attributes whose values have an editing type of Fixed.

Creating user profile templates

The Access Control Manager has two Edit User Templates screens. The templates screens are almost identical to the Edit Users screens, described in "Access Control Manager Edit User screens" on page 4-5. To load the `dictionary` file and bring up the primary Edit User Templates screen, click the Edit User Templates icon on the Access Control Manager's home screen.

Note: You cannot edit a template's attributes from the primary Edit User Templates screen.

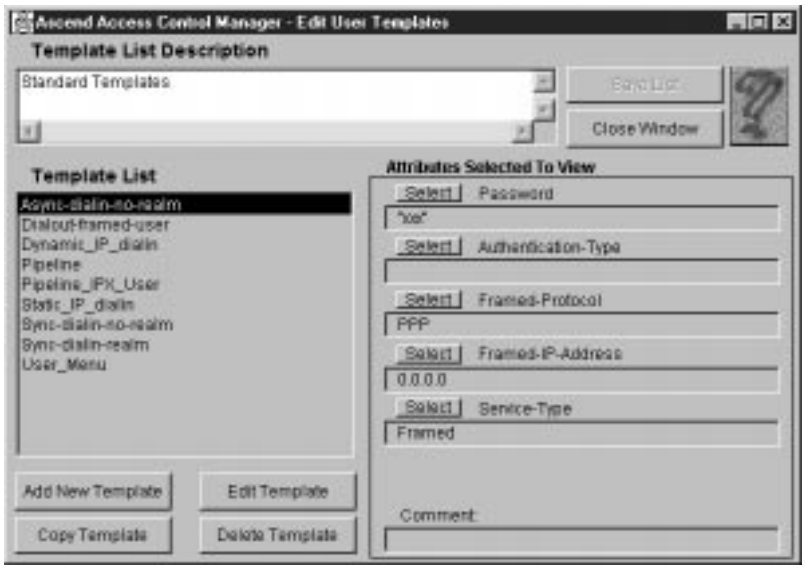


Figure 4-4. Access Control Manager primary Edit User Templates screen.

Figure 4-4, shows the components of the primary Edit User Templates screen.

User List Description

The textbox labeled User List Description contains general comments about the `users` file you selected to edit. These may categorize the users in the file, identify when `users` was last updated, or provide useful information about the `users`.

User List

The scrolling textbox labeled User List shows the `users` file's user profiles. The names of the profiles appear in the order they were added to the list. The most recent additions are at the bottom.

Editing buttons

The four buttons below the User List provide these functions:

- Add New User
  New users are added at the bottom of the list.
- Edit User
- Enables modification of user profile attributes and values.
- Copy User
  Copied realms are inserted below the realm from which they were copied.
- Delete User
  Before Ascend Access Control deletes a user from the list, a warning dialog box demands confirmation of the action.

Comment

The textbox labeled Comment is for comments about the selected user.

Save List, Close Window and Help buttons

Click on the Save List to save the attributes and values of all the user profiles in the open `users` file. If you click on the Close Window button before saving the

file a confirmation dialog box appears. You can choose to cancel changes or save the file. The Help button is your access to a text file that describes the functions you can perform with the Edit Users screen.

Attributes Selected To View

The attributes under the heading “Attributes Selected To View” provide a snapshot of the attributes and values you are most interested in seeing as you click on different templates in the Template List. The screen has space to display five attributes and their values. (There can be more than five attributes in any of the templates.) To change any of the Attributes Selected to View, click the Select button beside the attribute name, and choose a different attribute from the list that appears.

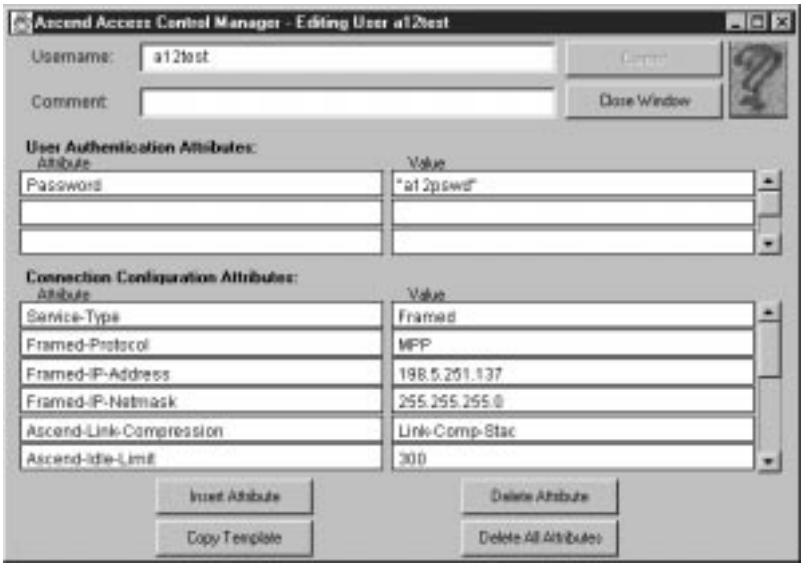


Figure 4-5. Access Control Manager secondary Edit User Templates screen.

Compare the secondary Edit User Templates screen in Figure 4-5 with Figure 4-2, the secondary Edit User screen. The only difference is that the Edit User Templates screen contains a column labeled *Type* between the attributes and

values. The significance of the *Type* column is discussed in “Assigning attribute-value editing types” on page 4-14.

Editing users files with User Account Wizard

Although system administrators can use the User Account Wizard, it was designed to guide those less familiar with Ascend Access Control through the steps of adding, modifying, or deleting user profiles. Just about anyone can productively use the wizard and the user templates after brief training.

All users can benefit from the text file containing information about the current User Account Wizard screen. Each screen displays the file in a scrolling textbox. The information describes the functions that can be performed on that screen and the format of the screen itself.

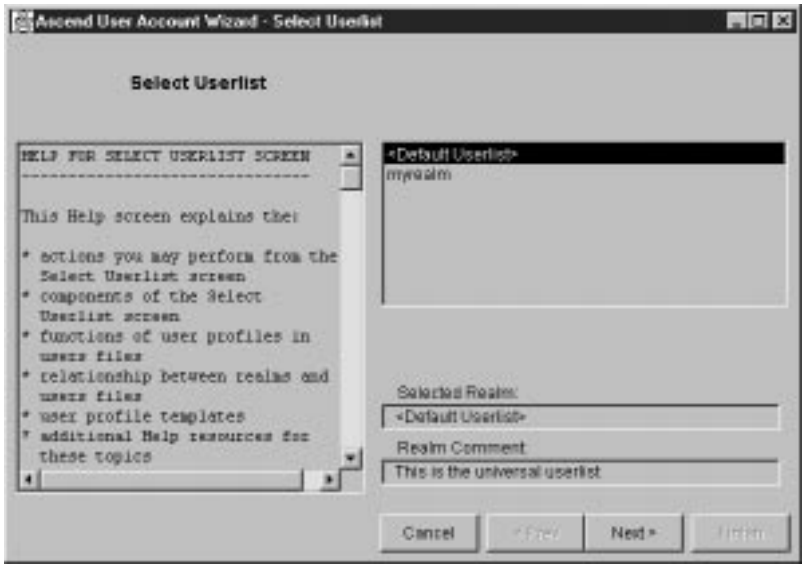


Figure 4-6. User Account Wizard Select Userlist screen.

Steps in User Account Wizard procedures

You can add, edit or delete a user profile with the User Account Wizard. Begin any User Account Wizard procedure by clicking the appropriate icon on the User Account Wizard's home screen.

Advanced Vs. Simple editing level configuration

As noted in Chapter 3, "Installing Ascend Access Control and its graphical user interfaces," you can configure the User Account Wizard to perform Simple or Advanced editing. In Simple mode, you can access only one `users` file. Your first step in creating a user profile is to select a user template. When editing or deleting a user profile in Simple editing mode, your first step is to select the user profile that will be affected. In Advanced mode, your first step in performing each procedure is to select a user list. This is comparable to selecting one of the available `users` files.

Adding a new user profile

To add a new user profile in Simple editing mode:

1 Select a user template.

2 Click the Next button at the bottom of the screen.

In Advanced mode:

1 Select a userlist.

2 Select the Next button at the bottom of the screen.

3 Select a user template.

4 Click the Next button.

The User Account Wizard is a series of screens, each labeled Define User (Figure 4-7). A Define User screen displays an attribute above a textbox. Enter an attribute's value if the textbox is blank, or change the Default value. User Account Wizard only presents attributes assigned the editing level *None* or *Default*. It does not display template attributes that have a *Fixed* value.

Figure 4-7. User Account Wizard Define User Screen.

After you enter a value for the attribute, click Next or press Enter. The Finish button is grayed out until you reach the last template attribute you can assign a value. Then the Next button grays out and Finish activates. When you click Finish the User Account Wizard displays the Add More Users screen (Figure 4-8), which asks if you want to continue or quit the wizard program. You can use the same template or a different template to add another user. If the User Account Wizard is in Advanced mode you can also choose to add another user in a different realm.

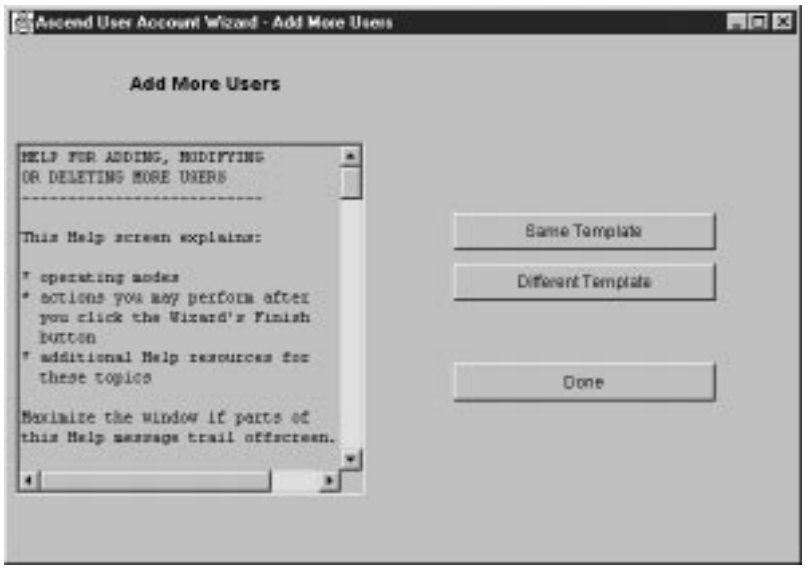


Figure 4-8. User Account Wizard Add More Users screen, Simple mode.

Modifying a user profile

Select the User Account Wizard's Modify a User icon to edit a user profile. The steps for editing attribute values in a user profile are similar to those for adding a new user profile. You must, of course, begin by selecting a user profile from the available userlist(s).

The Modify User screens the wizard presents when you edit a user profile look just like the User Define screens you use to add a new user profile. However, the Finish button at the bottom of a Modify User screen is always active, so you can save the user profile without editing all the profile's values.

For example, if you want to edit the value of the third attribute in the user profile, you click the Next button on the first two Modify Users screens to page to the third attribute.

You do not have to manually save the edited user profile. When you finish editing user profiles and select Done on the final screen, the wizard automatically saves the `users` files you have been working with then displays its home screen.

Deleting a user profile

To delete a user profile, you need only select the user and click Finish. As in the other procedures you can perform with the User Account Wizard, you may then continue to delete user profiles or return to the wizard's home screen.

Understanding authfile

The `authfile` is a list of the realms Ascend Access Control recognizes. Generally, a realm is a group of users who share a common characteristic, such as being customers of the same Internet Service Provider. Realm members' user profiles can be nearly identical, perhaps varying only in the values of their User-Name and Password attributes. Members of realms enter their user names in the format *username@realm*.

When one Ascend Access Control server supplies authentication, authorization and configuration services for multiple users, you can effectively control access to user profile information by limiting the viewing and editing privileges in each realm to the realm's `users` file.

Note: Ascend Access Control's realm feature is *the* solution when you should isolate different groups of users from one another on one Ascend Access Control server. The feature is not, however, the recommended solution for every Ascend Access Control environment. Many security policies specifically state that all Ascend Access Control user profiles must be stored in one centralized `users` file.

authfile format

Create an `authfile` file in the Ascend Access Control data-directory, `/etc/raddb`, if you want to use the Ascend Access Control realm feature. `authfile` is not created for you by the Install script or the `pkgadd` program, but a file containing examples of `authfile` entries is. You can copy examples of the entries from the `authfile.ex` file to the `authfile` file you create. `authfile` contains one line of information for each realm.

Each entry in the `authfile` must include values for `authfile`'s Realm-name and the Type fields. Each entry can also include optional values. Most values you

can enter for the type of authentication are incomplete without a reference to the location of a host or file, so you might also be required to provide a Kerberos realm name, a DNS hostname, or a filename in the `authfile` entry.

Following are the `authfile`'s required and optional fields:

```
Realm-name [( Alias[, Alias])] [-Protocol] Type
[Realm/DNS/File]
```

For example, an `authfile` could contain the following two lines:

```
umich.edu (wolverines) -pw afs-krb umich.edu mich

ohio.org  (buckeye, bucks) file buckeye
```

Editing authfile with Access Control Manager

You can edit entries in an `authfile` using Access Control Manager's Edit Realms screen. It appears when you click the Edit Realms icon on Access Control Manager's home screen (Figure 4-8). The main areas of the Edit Realms screen are the Realm List Description, the Realm List, and a group of realm fields in which you enter information about the realm selected in the Realm List.

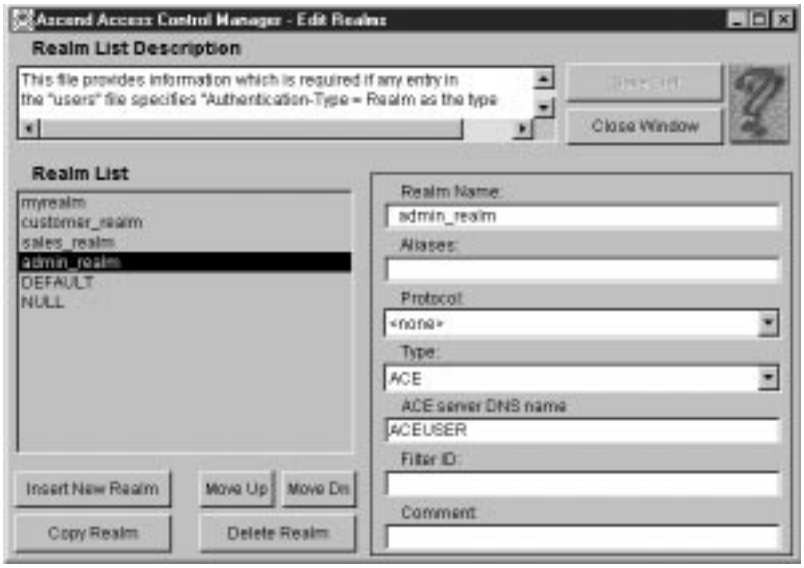


Figure 4-9. Access Control Manager Edit Realm screen.

Realm List Description

The textbox labeled Realm List Description at the top of the Edit Realms screen is for general comments about the `authfile` file. These may categorize the realms in the file, identify when `authfile` was last updated, or provide useful information about the `authfile`.

Realm List

The scrolling Realm List at the left of the screen shows the file's existing realms. The names appear in the order in which the realms were added to the list. Below the Realm List, five buttons provide the following functions:

Editing Buttons

The five buttons below the Realm List provide these functions:

- Insert New Realm

  New realms are added at the top of the list if no existing realm has been selected, otherwise the new realm is inserted in the list below the highlighted realm.
- Copy Realm

  Copied realms are inserted below the realm from which they were copied.
- Delete Realm

  Before Ascend Access Control deletes a realm from the list, a warning dialog box demands confirmation of the action.
- Move Up and Move Dn

  Each mouse click moves the selected realm one position up or down, respectively, in the list.

Realm field values

To the right of the Realm List are six textboxes where you may add or edit values for the required and optional `authfile` fields that define a realm. (“authfile(5)” on page A-2 in Appendix A, discusses `authfile` fields and values.)

Comment

The textbox labeled Comment, below the six field-value textboxes on the right side of the Edit Realms screen, is for comments about the realm highlighted in the Realm List.

Editing general and specific comments

You can add or edit general comments about the `authfile` or specific comments about a particular realm.

authfile comments

To add or modify comments about the `authfile`:

1 Click in the Realm List Description textbox.

The textbox scrolls so that you can overwrite, insert new lines between, or append new lines to the existing comments.

2 Type your comments.

Realm comments

To enter comments about one of the realms:

1 Click in the Comment textbox at the bottom of the screen.

The textbox displays one line of the comments at a time, but you can enter as many lines as necessary. The lines wrap automatically when you reach the edge of the textbox.

2 Enter your comments. If the textbox already contains comments you can overwrite them or insert new comments.

Editing realms

You can add a new realm by entering the data or by copying an existing realm's data and editing it. You can also modify a realm by editing it, and you can delete a realm.

Adding a new realm

To add a new realm:

1 In the Realm List, select the realm below which you want to add a new realm.

If the Realm List is empty, click in the textbox itself to activate it.

2 In the textboxes to the right of the Realm List, enter the realm name and other field values that define the new realm.

3 Click the Add New Realm button.

The new realm appears below the realm you selected in the Realm List.

Copying a realm

To copy a realm:

1 Select a user in the Realm List.

2 Click the Copy Realm button.

A new realm appears below the one you selected. It has the same name and field values as the realm you copied.

Editing a realm

To edit the field values of any existing realm, including one that you have copied from an original:

1 Select the realm from the Realm List.

2 Click in the textbox(es) of the field(s) whose values you want to change.

3 Type a new entry in the textbox and delete the old.

You can also double-click on a word in the textbox to select it, then type a new entry. The new entry automatically replaces the selected word.

Deleting a realm

To delete a realm:

1 Select the realm in the Realm List

2 Click on the Delete Realm button.

The Confirm Delete dialog box appears.

3 Click the OK button to confirm or the Cancel button to abort the deletion of the realm.

Editing field values

Six textboxes represent the required and optional realm fields. Four are plain textboxes in which you must type a value that is appropriate for your network, such as a realm or file name. The other two, Protocol and Type, display drop down lists containing all valid entries.

Edit Realm field textboxes

The Edit Realm textboxes representing `authfile` fields are:

- Realm (required)
- Alias (optional)

- Protocol (optional)
- Type (required)
- Realm/DNS/File (optional)

Editing authfile field values

To edit an `authfile` field:

1. Select a realm name from the Realms List, or use the Copy Realm or Add New Realm to create a new entry in the list.
2. Click in the textbox of a field you need to edit.
3. Enter the value, or select a value from the drop-down list, as required.
4. Repeat steps 2 and 3 until you've edited all the fields that need to be changed for that realm.
5. To edit additional clients, repeat steps 1-4.

Saving authfile or canceling changes

To save your `authfile` edits and additions, click the Save List button.

To abandon the changes you've made during the current session:

1. Click the Close Window button.
   The Save Changes to Realm List dialog box appears.
2. Click the No button.

Understanding the clients file

The `clients` file is a list of all the Network Access Servers (NAS) and remote Ascend Access Control servers that can send Access-Requests to the Ascend Access Control server. If a client is not represented by an entry its the server discards its messages.

Clients file format

You must create the `clients` file. Like `authfile` and `users` file, `clients` resides in the `/etc/raddb` directory. You can copy examples of `clients` file entries from `clients.ex`, which is copied on the server when Ascend Access Control is installed. Unlike `authfile`, it is not optional and you must not delete it. Entries in `clients` file may include five fields. Two, System-name and Key, are required. System-name has an optional component called Port. The Port component overrides Ascend Access Control's default authentication port number. The five fields, with example entries are:

```
System-name:Port  Key      [Type]   [Version][Prefix]

marlowe:1945      loring   type=nas v2       mystery.
```

Caution: The Prefix field entry in the `clients` file must contain a trailing period (.). If you enter the previous example in your `clients` file, Ascend Access Control searches for realms associated with the NAS named Marlowe in a file named `mystery.authfile.` If your prefix entry does not include a trailing period Ascend Access Control searches for a file named `mysteryauthfile.`"Prefix field (option)" on page A-10 also discusses the format of the `clients` file Prefix field.

Note: Although the function of an `authfile`'s Realm/DNS/File field entry can be similar to a `clients` file's Prefix entry, the `authfile` 's Realm/DNS/File field's entry does not require a trailing period. When the `authfile` Type field value is `file` you enter a name in the Realm/DNS/File field. The name is a prefix for a `users` file. The values `file` and *name* in the Type and Realm/DNS/File fields indicate that the profiles of a realm's users are stored in a file called *name*`.users`. Ascend Access Control assumes that the Realm/DNS/File field entry includes an implied trailing period. "authfile(5)" on page A-2 and "Other users files" on page A-35 contain more information about `authfile` entries and Realm/DNS/File.

Editing clients with Access Control Manager

For editing the `clients` file, Access Control Manager provides one Edit Clients screen. (Figure 4-9). It appears when you click the home screen's Edit Clients

icon. Aside from the field names over its textboxes, it is almost a duplicate of the Edit Realms screen discussed in "Editing authfile with Access Control Manager" on page 4-23. A Client List Description and Client List appear instead of the Realm List Description and Realm List, respectively, and the screen has client fields instead of realm fields.

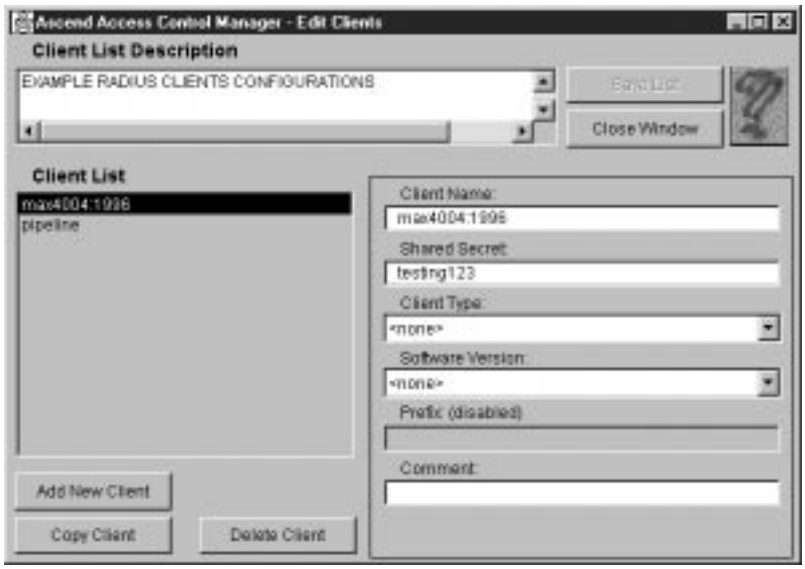


Figure 4-10. Access Control Manager Edit Clients screen.

Clients List Description

The Clients List Description textbox is for general comments about the `clients` file. These may categorize the clients listed in the file, identify when `clients` was last updated, or provide other useful information.

Client List

The scrolling Client List at the left of the screen shows the clients currently included in the file. The names appear in the order in which the clients were added to the list.

The three buttons below the Client List provide these functions:

- Add New Client

  Click Add New Client to add a client. The new client appears at the end of the client list.
- Copy Client

  Click Copy Client to copy the field entries of the currently selected client. Copied clients are inserted below the client that you copied.
- Delete Client

  Click Delete Client to remove the currently selected client from the `clients` file.

Field values

To the right of the Client List are five textboxes where you can add or edit values for the required and optional `clients` file fields. (`clients` file fields and values are discussed in “clients(5)” on page A-8).

Comment

The textbox labeled Comment, located below the five field value textboxes contains a comment about the client highlighted in the Client List.

Editing general and specific comments

You can add or edit general comments about the `clients` file or specific comments about a particular client.

clients file comments

To add or modify comments about the `clients` file:

1 Click in the Clients List Description textbox.

The textbox scrolls so that you can overwrite, insert new lines between, or append new lines to existing comments.

2 Type your comments.:

Client comments

To enter comments about a client:

1. Click in the Comment textbox at the bottom of the screen.
   The textbox displays one line of the comments at a time, but you can type as many lines as necessary. The lines wrap automatically when you reach the edge of the textbox.
2. Enter comment.
   If the textbox already contains comments, you can overwrite them or insert new comments.

Editing clients

You can add a new client by entering the data or by copying an existing client's data and editing it. You can also modify a client by editing it, and you can delete a client.

Adding a new client

To add a new client:

1. Click Add New Client.
   Values in the field textboxes disappear.
2. Click in the Client Name textbox to the right of the Client List and enter the client's name.
3. Press Enter or click in the next textbox in which you need to enter a value.
4. Repeat steps 2 and 3 until you have added all the values that define the client.
5. Click on the Add New Client button.
   The new client is added at the end of the Client List.

Copying a client

To copy a client:

1. Select a client in the Client List
2. Click the Copy Client button.

A new client appears below the one you selected. It has the same name and field values as the one you copied.

Editing a client

To edit the field values of an existing client, including one that you copied:

1 Select the client in the Client List.

2 Click in the textbox(es) of the field(s) whose values you want to change.

3 Type a new entry in the textbox and delete the old.
You can also double click on a word in the textbox and type a new entry, replacing the selected word.

Deleting a client

To delete a client:

1 Select the client in the Client List.

2 Click Delete Client
The Confirm Delete dialog box appears.

3 Click the OK button to confirm or the Cancel button to abort the deletion of the client.

Editing field values

Five textboxes represent the required and optional client fields. Four are plain textboxes in which you must type a value that is appropriate for your network, such as a client or file name. The other two, Version and Type, display a drop-down list containing all valid entries.

Edit Client field textboxes

The Edit Client textboxes representing `clients` fields are:

- System-name (required)
- Key (required)
- Type (optional)
- Version (optional)

- Prefix (optional)

Editing clients field values

To edit an clients field:

1. Select a client from the Client List, or use the Copy Client or Add New Client to create a new entry in the List.
2. Click in the textbox of a field you need to edit.
3. Enter the value, or select a value from the drop-down list, as required.
4. Repeat steps 2 and 3 until you've edited all the fields that need to be changed for that client.
5. To edit additional clients, repeat steps 1-4.

Saving clients file or canceling changes

To save your edits to the `clients` file click on the Save List button. Canceling changes

To abandon the changes you've made during the current session:

1. Click the Close Window button.
   The Save Changes to Client List dialog box appears.
2. Click the No button.

Understanding Ascend Access Control

5

Chapter 5 is an overview of these Ascend Access Control features:

- Authentication, authorization and accounting functions
- Support for alternative authentication methods

Who should read this chapter

This chapter provides information not included in the three quick start chapters, which are for people who have some understanding of the way that Ascend Access Control or RADIUS authentication, authorization and accounting services work. Read this chapter if you need some background information before plunging into creating user profiles, identifying clients, and configuring realms.

The chapter begins with brief overviews of Ascend Access Control's authentication, authorization and accounting services, and moves to descriptions of the program's foundations: the client/server messages and the field entries of each Ascend Access Control file. It closes with information about Ascend Access Control's support of proxy RADIUS and other authentication methods. This approach seeks to illustrate the way that many small pieces of data are collected to support Ascend Access Control's services, and the way those services can be joined with other products to strengthen network security.

Ascend Access Control overview

Ascend Access Control authenticates and authorizes remote users and, optionally, stores accounting information about the users' network connections.

Ascend Access Control authentication and authorization go hand-in-hand. They are conducted via four types of Access messages that pass between a Network Access Server (NAS) and an Ascend Access Control server. The messages, Access-Requests, Access-Responses, Access-Challenges and Access-Rejects, are composed of User Datagram Protocol (UDP) packets.

Ascend Access Control accounting is optional. When you make accounting operational, the NAS sends Accounting-Request messages to Ascend Access Control that include details about a user's network connection. Ascend Access Control acknowledges receipt of the NAS messages with Accounting-Response messages.

For explanations of Ascend Access Control and RADIUS Accounting messages, see "Understanding RADIUS messages" on page 5-9.

How Ascend Access Control works

Although very much simplified, the following steps explain how Ascend Access Control works:

1 An NAS, also referred to as a client, contacts the Ascend Access Control server and asks Ascend Access Control to verify the identity of a user who has requested network access.

2 Ascend Access Control searched its client-list file for a match with the client-identification information in the client's message. The information includes a secret key, on which Ascend Access Control performs an MD-5 checksum. If the result is valid, Ascend Access Control extracts user-identification information from the message.

3 Ascend Access Control searches a file of user profiles. If it finds a profile that matches the user information sent by the client, Ascend Access Control sends the client a user-authentication message.

4 The message verifies the user's identity, specifies the extent of the user's access to the network and to network services, and defines how the user's link to the network is to be configured.

Step 3 includes additional operations when the user's profile specifies one of the following conditions:

- User's profile is on a RADIUS server.

  Ascend Access Control becomes a proxy for the RADIUS server.
- Another form of authentication, such as Kerberos or TACACS is required.

  Ascend Access Control opens an authentication session with the appropriate server.
- Authentication requires a SecureID or other token key.
- Ascend Access Control send's the user's token-key information to the token card server.

Ascend Access Control files

To perform this way, Ascend Access Control needs access to a lot of information, including:

- who its clients and their users are

- what its clients and their users will provide as identifying information
- where to find matching information to identify clients and their users
- how its clients should configure their users' access and links

If you read the Chapter 1, "Introducing Ascend Access Control," you remember the example "story" about a telephone call from a building inspector who wants to visit a construction site. The story has two purposes. One purpose is to illustrate the many types of information you may collect for authentication and authorization. The second purpose is to relate the types of information to typical user attributes found in the Ascend Access Control `dictionary`. If you skipped the introduction, here is a list of the information collected during the call and the corresponding attributes from the Ascend Access Control `dictionary` file:

Information	**Attribute**
Caller's name	User-Name
Caller's means of identification	Password
Caller's location	Framed-IP-Address
Caller's telephone number	Calling-Station-ID
Your means of verifying the caller's TN	Ascend-Callback
Caller's requested destination	NAS-IP-Address
Caller's means of travel	Framed-Protocol
Activity for which caller requests approval	Service-Type
Your means of controlling caller's activities	Ascend-Data-Filter
Your means of restricting the length of caller's approved access	Expiration
Your means of keeping track of the caller's visits	RADIUS Accounting

Table 5-1. Converting information to Ascend Access Control attributes

After obtaining the information you can enter it in a file, or files, that reside in the Ascend Access Control data directory. The files are named `users`, or `prefix.users`, where prefix is the name of a realm which defines a group of users.

The data directory also contains other Ascend Access Control files named `dictionary, authfile` and `clients.` Ascend Access Control consults these files when performing the steps outlined in "How Ascend Access Control works" on page 5-3. The `clients` file, for example, is a list of all clients that Ascend Access Control can authenticate. `authfile` is a list of the user realms where Ascend Access Control stores the *prefix* in `prefix.users.` Each of these files is described in more detail later in this chapter.

Types of file entries

Ascend Access Control stores data file information as field values or attribute/value pairs. The format of the data depends on the data file.

You enter field values in the `authfile` and `clients` files. You must enter a value for some fields in each file because Ascend Access Control cannot parse the entry, or define the entry's realm or client, if the field is blank. Entering values in the other fields is optional. Ascend Access Control can parse the file entry and recognize what it describes if you leave these fields blank. Realm-Name and Type are required `authfile` fields. Version and Prefix are optional `clients` file fields. (The status of each `authfile` and `clients` field is discussed in Appendix A, "Ascend Access Control files and commands.").

You enter values that define attributes in all types of users files, including templates. The difference between an attribute and a field is slight, but significant. Attributes describe the users Ascend Access Control authenticates and the way the users can connect to other machines. A few attribute values are required. For example, Ascend Access Control must find the user's identity and an authentication method in the user profile. It is misleading to describe the rest of the attributes as optional, because user profiles almost always contain some authorization attribute/values pairs. Ascend Access Control sends the authorization attribute/values, which describe the user's connection configuration, to the NAS.

Understanding authentication

Ascend Access Control's primary function is to confirm that someone requesting a connection to or from the network has permission to make the connection and to use network services. Ascend Access Control authenticates users by comparing the user's name and the password with information in its own files. The user's name and address are sent by a NAS or a proxy server. The process that defines the messages that pass between the NAS and Ascend Access Control includes the following:

1 A NAS or proxy server sends an Access-Request message to the Ascend Access Control server. The message includes the names of the user and the NAS and the user's password. To learn more about Ascend Access Control proxy servers see "Proxy Ascend Access Control servers" on page 5-30.

Ascend Access Control compares information in the Access-Request message with data in the `clients` file and a `users` file. The `clients` file contains the names of all the NAS units that may request user authentication from the Ascend Access Control server. Ascend Access Control `users` files are databases containing information about legitimate users Ascend Access Control can authenticate. The value of a `clients` file field named Key is a secret shared by Ascend Access Control and the NAS, which they use to verify each other's identity. A `users` file stores information in user profiles containing attribute/value pairs. Ascend Access Control's key for finding a user profile in the `users` file is the value of the User- Name attribute.

Note: Ascend Access Control can utilize more than one `users` file. The user's name determines which of the `users` files Ascend Access Control consults when trying to match the information sent by the NAS.

2 Ascend Access Control sends the NAS an Access-Response message if the data in the Access-Request message matches the NAS information in the `clients` file and the user information in the appropriate `users` file.

or

Ascend Access Control sends the NAS an Access-Reject message if the name of the NAS is not in the `clients` file or the user's name or password does not match any corresponding entries in the `users` file.

Ascend Access Control authentication options

Ascend Access Control supports a variety of authentication methods. “Ascend Access Control authentication methods” on page 5-28, explains Ascend Access Control support for:

- PAP
- CHAP
- S/Key
- RADIUS proxy servers
- Kerberos
- TACACS and TACACS+
- Token Keys

Understanding authorization

The information Ascend Access Control stores in a `users` file defines the services that users may access and the connections they can make. Ascend Access Control might answer a NAS request by sending an Access-Response packet authorizing the NAS to allow the user to connect to a specific network machine, such as a Telnet server.

Authorization information that Ascend Access Control sends to a NAS might also tell the NAS how users are allowed to make internal and external connections. For example, Ascend Access Control’s authorization could instruct the NAS to allow an incoming user’s connection to a local Telnet server via an unframed protocol, but force another, outgoing, user to connect remotely with framed Point-to-Point Protocol.

Attribute/value pairs define the specific authorizations granted a user. The `dictionary` file explicitly lists Ascend Access Control’s attributes and their possible values. Some Ascend Access Control attributes come from the RADIUS standard, but most are Ascend’s vendor-specific additions. The RADIUS protocol includes a means of adding proprietary attributes. Vendor-specific attributes are generally associated with the capabilities of a particular NAS unit.

Ascend Access Control supports Database Management Systems that comply with the Open Database Connectivity (ODBC) standard. You can store user profile attribute and their values in database tables instead of `users` files. You can find more information about configuring Ascend Access Control connections to database tables in “Open Database Connectivity (ODBC)” on page 7-1.

Understanding accounting

Ascend Access Control’s third function is to serve as a repository of information about network connections. When it has authenticated a user and authorized the connection and services, Ascend Access Control might receive an accounting of the connection from the NAS. The accounting can include such things as the start and stop times of the connection and the number of packets and octets transmitted over the connection. This information can be valuable for evaluating security policies and network usage.

RADIUS accounting has its own set of attributes and, as with authorization attributes, provides more accounting attributes than those described in the RADIUS protocol. Accounting attributes and their values are also explicitly listed in the Ascend Access Control `dictionary` file.

If a NAS is configured for RADIUS accounting, it sends an Accounting-Request message that includes an Accounting-Start packet to Ascend Access Control which responds with an acknowledgment that the start packet was received. At the end of the accounting delivery, the NAS sends another Accounting-Request message that includes an Accounting-Stop packet. Ascend Access Control also acknowledges this packet. Ascend Access Control can also be a proxy accounting server, transmitting the NAS’s Accounting-Requests to another RADIUS accounting server.

There is no default limitation on the number of times the NAS may send Accounting-Request messages in the event that it receives no acknowledgment. You can specify a time frame the NAS will wait to receive an acknowledgment or limit the number of times the NAS can send an Accounting-Request, or both.

Ascend Access Control also allows you to store RADIUS accounting information in an ODBC DBMS table. “Open Database Connectivity (ODBC)” on page 7-1 contains important information about ODBC DBMS accounting tables.

Note: Some NAS units, such as the Ascend MAX, can be configured to send accounting information to more than one accounting server. This provides the NAS with an alternative if its primary accounting server is down or unreachable.

Understanding RADIUS messages

This section begins a discussion of some facets of the RADIUS protocol. RADIUS is a foundation for Ascend Access Control services, although the program extends those services and supports many features that are not found in the RADIUS protocol. The RADIUS protocol is defined in RFC 2058. Ascend Access Control passes messages between its servers and clients via the method outlined in that RFC. Like RADIUS, it also stores attribute/value pairs in files and packages them within the server's messages.

RADIUS packets

RADIUS is a User Datagram Protocol (UDP). Sending UDP packets rather than Transmission Control Protocol (TCP) packets, reduces the length of time the user must wait for authentication. To understand why, consider the communications that pass between the client and the server while the user waits.

Suppose that the NAS sends the server an Access-Request message that is garbled in transmission. In plain language the message the NAS, or another server acting as a client, sends is:

> "Here's some information about a user who wants me to set up a connection for him. Please authenticate this user for me. I'm a client of yours and here's the secret key that identifies me."

The garbled message the RADIUS server receives might be:

> "Here's some ...to set up a connection for him. Please ...this user for me. I'm a ... and here's the secret you can use to identify me."

This message doesn't make sense to the server, which has not received all the information it needs. Therefore it doesn't respond to the client. After a specified time, the client sends the Access-Request message again and it arrives intact.

The server compares the secret key it receives to one it has on file for the client. If the secret keys don't match, the server might send an Access-Reject packet to

the client explaining why it can't authenticate the user. If the secrets do match, the server responds in one of two ways:

1. The server sends an Access-Accept packet containing this message:
   "Yes, I can verify the identity of the user. Here is some information about the way to set up the user's connection."
2. The server sends an Access-Challenge packet containing this message:
   "Yes, I will try to verify the user's identity. Ask him to respond to this challenge."

The messages are so short the user doesn't know the Access-Request was transmitted twice. UDP doesn't add time to the exchange because the protocol does not require that the client and server negotiate how they will handle the connection. The client and server accept each other's messages with very little concern for transmissions errors.

TCP, the alternative to UDP, is connection-oriented and it does provide end-to-end error checking. If handled by TCP, the exchange described above would take longer because TCP requires negotiations and error-checking.

Types of RADIUS messages

The example client/server exchange in "RADIUS packets," above, identifies four types of RADIUS messages:

- Access-Request
- Access-Reject
- Access-Accept
- Access-Challenge

If you employ RADIUS Accounting, the client and server might also exchange the following types of messages:

- Accounting-Request
- Accounting-Response

The information in each RADIUS message is encapsulated in a UDP packet's data. A packet is a block of data set in a standard format for transmission. It is accompanied by other information, such as the origin and destination of the data.

By default the server's source and destination for a RADIUS packet is port 1645. The client may not have a default port for exchanging the packets, but may be configured according to the documentation that accompanies the unit. You may override the server's default port from the command line by starting the RADIUS daemon with the -p option. For a description of this daemon option, see "radiusd(8)," in Appendix A.

Each RADIUS packet contains five fields measured in octets, each of which is an eight-bit chunk of data representing an ASCII number or letter. The number of octets in the Attribute field is variable. The Authenticator field contains sixteen octets, and the other fields consist of one or two octets. The total number of octets in the packet is between 20 and 4096. Table 5-2 describes the five fields.

Table 5-2. RADIUS packet fields

Fields	Description
Code	One octet that identifies the message by type
Identifier	One octet used to match a client's Access-Requests and a server's replies
Length	Two octets representing the number of octets in the entire packet
Authenticator	Sixteen octets representing a value used to authenticate the server's reply
Attribute(s)	Variable number of octets representing the numerical equivalents assigned to attributes and their values

RADIUS packet Code field

The number in the packet's Code field indicates the type of message that has been sent. Clients only send RADIUS Access-Request messages or RADIUS Accounting-Request messages. Servers send three types of RADIUS reply messages or an Accounting-Response message. Table 5-3 is a list of the codes

and the message types they identify.

Table 5-3. RADIUS packet Codes and corresponding messages.

Code	Message
1	Access-Request (from client)
2	Access-Accept (from server)
3	Access-Reject (from server)
4	Accounting-Request (from client)
5	Accounting-Response (from server)
11	Access-Challenge (from server)

The NAS/server exchange described in “RADIUS packets” on page 5-9 illustrates when each type of RADIUS message may be sent.

The NAS sends Accounting-Request when it has information it would like the server to store and the server sends an Accounting-Response to acknowledge receipt of the request.

If the NAS receives no response from the RADIUS server or RADIUS Accounting server, it re-sends its Access-Request or Accounting-Request. The length of time the NAS waits between attempts to re-send, and the maximum number of attempts, may be configured in the NAS. The NAS may also be configured to have primary and secondary authentication and accounting servers.

Identifier

The Access-Request identifier field contains a value which is copied into the server’s response so that the NAS can correctly associate its requests and the server’s responses when multiple users are being authenticated.

Length

The length field is a simple error-checking device. The server silently drops a packet if it is shorter than the value specified in the Length field. If the packet is longer, the server ignores the octets beyond the value of the Length field.

Authenticator

The authenticator field contains a value for a Request Authenticator or a Response Authenticator, depending on the type of message being sent. The Request Authenticator is included in a NAS's Access-Request. It is an unpredictable and unique value that Ascend Access Control adds to the secret key before running the combination through a one-way MD5 hash algorithm. The result supplements the user's password to protect against authentication attacks.

A Response Authenticator is part of Access-Reject, Access-Accept and Access-Challenge messages sent by the RADIUS server. Its value is the result of a one-way hash of the packet's contents and the secret key.

Attributes

Attribute values are also related to the type of message being sent. The number of attribute/value pairs included in the packet's Attribute field is variable, depending on what is required or optional for the type of service requested. There is no minimum requirement for attributes in a message sent by the server to the NAS.

Understanding the dictionary file

The Ascend Access Control `dictionary` file is a list of the authentication, authorization and accounting attributes you can enter in a `users` file. Ascend Access Control's installation script installs the `dictionary` file and a companion file named `vendors`. You can not edit either file with Access Control Manager or User Account Wizard.

Each `dictionary` entry translates an attribute's human-readable name into an enumerated equivalent and lists all the values for that attribute. Ascend Access

Control uses the number associated with the attribute to parse incoming requests and generate responses. RADIUS protocol requires that the attribute's number be in the range of 1 to 255.

For example, the Framed-Protocol attribute's entry in the `dictionary` file translates it into the number 7 and lists the attribute's nine possible values. For discussion of the `dictionary` file's Ascend Access Control attributes see Appendix B, "Attributes Reference," and the Access Control Manager's HTML help files.

Vendor Specific attributes

Ascend Access Control follows the RADIUS protocol's method of supporting additional attributes. Ascend Access Control stores attributes developed by vendors such as Ascend in the `dictionary` file as values of number 26, the Vendor-Specific attribute.

Ascend Access Control also supports attributes vendors assigned non-standard numbers, such as Ascend-Data-Filter, which the vendor added to the `dictionary` as attribute number 242. Ascend Access Control maps Ascend-Data-Filter to a value of the RADIUS standard's Vendor-Specific attribute via information in Ascend Access Control `vendors` file.

Caution: Reply-item attributes that vendors develop for their own NAS machines, such as Ascend-Data-Filter, are not recognized by other vendors' machines. In addition, each NAS must be identified by its vendor name or Ascend Access Control will not send it a vendor-specific reply-item attribute. See "Understanding the clients file" on page 5-25.

dictionary format

Each translation consists of attribute/value pairs. Each attribute entry and each value entry has four fields. Following is an example of a `dictionary` entry.

```
Attribute attribute-name  integer-encoding type
Attribute Framed-Protocol 7             integer
Value     attribute-name  value-name integer-encoding
Value     Framed-Protocol PPP       1
```

An attribute value is expressed in one of four data types, as shown in Table 5-4:

Table 5-4. The four data types of attribute values.

Type	Description
string	0-253 octets
ipaddr	4 octets in network byte order
integer	32 bit framing in big endian order (high byte first)
date	32 bit value in big endian order (seconds since 00:00:00 GMT — Jan. 1, 1970)

Understanding an authfile

Ascend Access Control provides a means for grouping users together for authentication. The groups are called realms. An `authfile` is a list of the realms to which you can assign users. Members of realms may enter their user names in the format *user@realm* or *realm/user*. However, the separator in a realm-affiliated user's name does not have to be the @ or / character. You may choose different separators with the `radiusd` options `-r` and `-rr`.

Locating authfile

By default, `authfile` and the other Ascend Access Control data files reside in the server's `/etc/raddb` directory. Although you may change the data directory with the `radiusd -d` option. For more information about the RADIUS daemon and its options, see "radiusd(8)," in Appendix A, "Ascend Access Control files and commands,"

Support for multiple authfiles

You create the `authfile` file yourself with a text editor, or base it on the file named `authfile.ex` which is distributed with Ascend Access Control. By default, Ascend Access Control searches for `authfile` when a user profile includes the attribute/value pair, `Authentication-Type = Realm`.

You can create an association between a NAS client and a specific `authfile` named *`prefix`*`.authfile`. The file's name is derived from the Prefix field's value in the NAS's `clients` file entry. If an Access-Request from the associated NAS leads to a user profile containing `Authentication-Type = Realm`, Ascend Access Control searches for the realm in `prefix.authfile`. If Ascend Access Control does not find `prefix.authfile`, it looks for the realm in `authfile`.

Caution: Ascend recommends caution if you want to associate a NAS and a `prefix.authfile` file. If you do not include `prefix.authfile`'s list of realms in the `authfile`'s list, Ascend Access Control may not be able find the realm for a NAS that is not associated with `prefix.authfile`.

The steps for creating a NAS-prefix.authfile link are discussed in "Creating Example Client, User and Realm Entries" on page 6-1. You may use a similar process to link a `prefix.users` file and a realm. That link is created when you enter a value in the Prefix field of a realm entry in `authfile` (or `prefix.authfile`!).

Realms

Ascend Access Control supports many authentication methods, including Kerberos, TACACS, and electronic token keys. When you group users into realms you can select one of the supported authentication methods for all members of that realm. You can also limit editing and viewing privileges by realm to increase security for user profiles. A realm may include all the users in an entire company, or the users in a single corporate department.

For example, suppose a large company provides Ascend Access Control authentication for three smaller companies. Each of the smaller companies may be identified by an individual realm name in the server's `authfile` and each of these realms may use a different authentication method.

When one of the company A's users dials in with the username *jsmith@Aco*, the Ascend Access Control server finds the Aco realm in its `authfile`. The server then handles the authentication in the manner described in the `authfile`'s Aco realm entry. The entry might tell the Ascend Access Control server to send the user's information to another server or to search a local `users` file containing Aco's user profiles.

authfile format

The `authfile` contains a line of information for each realm. Each line has several white-space delimited fields. Comment lines begin with a leading pound sign (#) and are ignored, as are blank lines.

A line must begin with an entry for the Realm-Name field and include an entry for the Type field. It may also include other field entries as shown in the example below. Some entries in the Type field require that you enter a realm name, DNS hostname or IP address, or file name for the line's Realm/DNS/File field.

```
Realm-name [Alias] [-Protocol] Type [Realm/DNS/File]

wolves school -pw AFS-KRB umich

buckeye ohio file buckeye
```

Table 5-5. Authfile fields

Field	Description	Value
Realm-Name	Symbol or name for a realm	An ASCII string. DEFAULT indicates how Ascend Access Control handles requests for realms not listed in `authfile`. NULL realm-name indicates how Ascend Access Control handles user names that are not in the *username@realm* format. Wild card syntax **.realm* specifies several related realms. Example: `*.town.com` stands for `abc.town.com` through `xyz.town.com.` The format allows one entry to match any of the realms. Place **.realm* entries near end of `authfile` list.
Alias	Optional field of comma-separated realm names within parentheses. Each alias name is equivalent to the realm name and is provided for user convenience.	Example — for realm named California (Calif,CA,CAL) User names that match the realm California: jsmith@calif, jsmith/ca, jsmith@ca
–Protocol	Forces the processing order of otherwise identical entries	–PW, –CHAP, –DFLT

Table 5-5. Authfile fields

Field	Description	Value
Type	The method the Ascend Access Control server uses to authenticate users within a given realm.	All entries are case insensitive. • passwd - same as unix-pw • unix-pw - authentication using the UNIX password file Following types require an entry in the Realm/DNS/File field: • RADIUS — Authentication by another Ascend Access Control or RADIUS server. The Realm/DNS/File field must contain default RADIUS server DNS name. Corresponds to name in `clients` file. • MIT-KRB — Authentication via MIT Kerberos. The Realm/DNS/File field must contain default Kerberos realm name. • AFS-KRB — Authentication via AFS Kerberos protocol. The Realm/DNS/File field must contain default Kerberos realm name. • File — Local Ascend Access Control server consults local `prefix.users` file where `prefix` is derived from the entry in the Realm/DNS/File field. • TACACS —- Authentication at TACACS server via encrypted request. Realm/DNS/File field must contain default TACACS server DNS name.

Table 5-5. Authfile fields

Field	Description	Value
Type (continued)	The method the Ascend Access Control server uses to authenticate users within a given realm.	• TACPLUS — Authentication at TACACS+ server via encrypted request. Realm/DNS/File field must contain default TACACS+ server DNS name. • ACE — Authentication with user's SecureID card • DEFENDER — Authentication with user's SecureNet key card • S/Key — Authentication via one-time password generated by the S/Key program • ODBC — Authentication via user profiles stored in ODBC-compliant DBMS table

Table 5-5. Authfile fields

Field	Description	Value
Realm/DNS/File	Entries indicate the realm, hostname, or filename appropriate to the entry in the Type field.	ASCII text string or IP address in dotted quad notation. The entry in the Type field determines which of three kinds of Realm/DNS/File field entries is appropriate. • *Realm* is appropriate when one of the two types of Kerberos authentication is entered in the Type field. *Realm* is the name of the Kerberos realm. • *DNS* is appropriate when the Type field entry is radius and authentication is performed by a remote Ascend Access Control server. *DNS* is the hostname or IP address of the remote Ascend Access Control server. • *File* is appropriate when the Type field is RADIUS and user authentication is done by the Ascend Access Control server. *File* is the *prefix* of the `users` file, expressed in the format *`prefix`*`.users.`

Understanding users files

A `users` file is a list of user profiles containing attribute/value pairs. The people the profiles define are users Ascend Access Control can authenticate for a NAS or server listed in the `clients` file. By default, Ascend Access Control searches for a file named `users` when it needs to locate user profiles. You create the file and populate it with user profiles by entering the profiles with a text editor, by copying examples from the provided `user.ex` file, or by using one of the Ascend Access Control graphic interfaces.

You may create more than one `users` files for the Ascend Access Control server. Additional `users` files usually bear a name in the format

prefix.users. The prefix is derived from the value of the Realm/DNS/File field in the authfile because, usually, prefix.users files are associated with realms. For example, a users file associated with a realm called Ournet might have the name *ournet.users.*

If you organize users into realms as explained in "Understanding an authfile" on page 5-15, you might want to create a separate users files for each realm.

users file attributes

You can only enter in a users file the attributes that appear in the dictionary file. User profile attribute/value pairs are classified two ways:

- Check-Items — The attribute/value pairs Ascend Access Control compares to the attributes/values it receives from a client to authenticate a user.
- Reply Items — The attribute/value pairs Ascend Access Control sends the NAS to authorize a link and services if authentication is successful.

  If authentication fails, Ascend Access Control might send an attribute/value containing a message about the authentication failure.

users file format

Create the users file in the Ascend Access Control data directory. By default, the data directory is /etc/raddb, but you can install Ascend Access Control in another location. For more information about changing Ascend Access Control defaults see "Default Ascend Access Control settings" on page 2-3.

A users file may contain general comments about the file and separate comments about individual user's profiles. Lines containing comments begin with a pound sign #. Each user profile contains one or more lines. The first line contains authentication attribute/value pairs and can wrap if the entries cannot fit on a single line. Lines below the authentication attribute/value pairs contain authorization attribute/value pairs and must begin with whitespace. All lines between the first and last lines end with commas. The first and last lines of a user profile do not end with a comma. Table 5-6 lists the elements of a user profile. The format is as follows:

```
#Comment
users-name check-item [, <check-item>]...
   reply-item,
   reply-item
```

Example users file entry

```
#This user began it all.
gwash@whitehse Password=paterusa,
     Service-Type=Framed,
     Framed-Protocol=PPP,
     Framed-IP-Address=105.23.0.1,
     Framed-IP-Netmask=255.255.255.0
```

Table 5-6. Elements of a user profile.

Element	Description	Value
Comments • File comment • Profile comment	Description or notation	ASCII string
Lines • First line • New line • Final line	 Initial line of user profile Line(s) between first and final lines; end(s) with a comma Last line of user profile	 Check-Item attribute/value pair Reply-Item attribute/value pair Reply-Item attribute/value pair

Table 5-6. Elements of a user profile.

Element	Description	Value
Check-Item	Entered in first line of User profile Attribute/value pair compared by Ascend Access Control to pair sent by client in an Access-Request packet	Any attribute listed in the `dictionary` file can be used as a Check-Item. Some common Check-Item attributes are: • User-Name (required) • Authentication-Type • Password • Service-Type • Ascend-Send-Password • Ascend-Send-Secret • Calling-Station-ID • CHAP Password • Class • Client-Port-NAS • NAS-Identifier • NAS-Port
Reply-Item	User profile newline or final line entry User file attribute/value pair sent by Ascend Access Control to client in an Access-Response packet	May include any attribute which is not a check-item and its value

Understanding the clients file

The `clients` file is a list of all the Network Access Servers (NAS) and Ascend Access Control servers that can send Access-Requests to the Ascend Access Control server. You create the `clients` file. It is not created or copied to the server during the installation of Ascend Access Control. Each entry in the `clients` file's list may contain values for five fields, although only values for the Client-Name and Key fields are required. The five `clients` file fields are:

- `System-Name:[port]`
- `Key`
- `Type`
- `Version`
- `Prefix`

clients file format

By default, the `clients` file resides in the `/etc/raddb` directory. It has a simple format. Each entry is one line that consists of field values separated by whitespace that can by a tab or keyboard space. An example entry follows, with the field name shown above each field:

```
System-Name:[port] Key     Type        Version      Prefix
marlowe            loringl type=nas    V2           mystery
```

NAS types and vendor-specific attributes

If you put vendor-specific reply-item attributes in user profiles, you must identify the NAS's vendor with the *`vendor`***`:nas`** option. Ascend Access Control will not send vendor-specific reply-items to a NAS identified generically by the Type field's **`nas`** option.You can enter one of these values for the Type field:

- `nas`
- *`vendor`*`:`**`nas`**
- `proxy`

For example, Ascend-Idle-Limit is a vendor specific reply-item in Jan Power's user profile. The attribute's value specifies the number of seconds an Ascend MAX waits before clearing Jan's inactive sessions. Jan's Ascend-Idle-Limit is 30 seconds and she can request connections via two Ascend MAX units named A and B. Ascend Access Control's `clients` file contains these entries for the NAS clients:

```
A   inside nas
B   outside ascend:nas
```

Ascend Access Control sends the MAX named B the attribute and its value after authenticating Jan Powers. The server does not send the MAX named A the attribute or value after authentication because A is identified by the generic type option. Therefore, A never clears Jan Power's sessions because it never receives Ascend-specific attributes.

Configuring the clients file

Table 5-7 lists all the clients file fields and their possible values.

Table 5-7. Description of the fields in the `clients` *file.*

Field	Description	Possible Values
System-Name[:port]	Name of NAS which can send Access-Requests to a Ascend Access Control server. Port number option overrides radiusd -pp and -qq options specifying Ascend Access Control relay port and accounting relay port. `name1/name2` option allows the same `clients` file to be used by, and distributed to, different Ascend Access Control servers.	• IP address in dotted quad notation or valid DNS hostname. • Optional port number format: *name:n* where *n* = UDP or TCP port • Optional two-name entry format: *`name1/name2`* `name1/name2` option valid only if one name matches authentication request's source IP address and other name matches response to hostname command on destination server. `name1/name2` format precludes using the port number format.
Key	Secret key known by a NAS and a Ascend Access Control server or by two Ascend Access Control servers.	ASCII text string. Minimum of sixteen characters, maximum of 128 characters.
Type	Vendor name and/or type of Ascend Access Control machine sending requests to the server.	Format is `type=`*`x`* where *`x`* is `ascend:nas, nas,` or `proxy` If client type and vendor name are unspecified, the server will not send vendor-specific Reply-Items from user profile.
Version	Ascend Access Control version number.	Format is `V`*`n`* where *`n`* is 1 or 2 The default is 1.

Field	Description	Possible Values
Prefix	Associates the NAS with a user realm. This prefix makes it possible for different NASes to use the same Ascend Access Control server, but with access to different databases on the server.	Text string prefix

Ascend Access Control authentication methods

Ascend Access Control supports authentication via Password Authentication Protocol (PAP) and Challenge Authentication Handshake Protocol CHAP, as described in the original RADIUS protocol. Ascend Access Control also authenticates via one-time passwords, token cards, and proxy servers.

PAP and CHAP

Password Authentication Protocol (PAP) is a two-way handshake, ID-and-password protocol, controlled by the user attempting to connect to the network. Under the PAP protocol, the user's machine may repeatedly send an ID-and-password pair via a Point-to-Point Protocol (PPP) connection until the user is authenticated or rejected. The ID/password pair is unencrypted during transmission and the user is only authenticated once at the beginning of the session.

CHAP is more secure than PAP because CHAP requires a three way handshake and authentication is controlled by the Ascend Access Control server, which may randomly issue challenges to the user during the session. During the three way handshake the user sends his identification to server, receives a challenge from the server, and sends back an answer to the challenge. The user and Ascend Access Control share a secret key with which the NAS and the server perform a one way hash of the Ascend Access Control challenge. When Ascend Access Control receives the user's hashed challenge response, it compares it to the

hashed challenge it is expecting. If the expected and received values match, Ascend Access Control authenticates the user's connection to the server. The server may send additional challenges during the session, which the user must answer to remain authenticated and connected. Challenges and responses are encrypted during transmission.

You implement PAP or CHAP authentication by entering values for two Ascend Access Control attributes in a user's profile in the `users` file. You must enter a value for the User-Name attribute for PAP or CHAP authentication. PAP also requires a User-Password attribute value and CHAP requires a value for the CHAP-Password attribute.

For complete definitions of the PAP and CHAP authentication methods, see Internet Engineering Task Force (IETF) RFC 1334.

S/Key

Ascend Access Control supports S/Key, a method of authentication in which the user provides a new password each time he requests access through a NAS. Ascend Access Control and the user share a list of passwords that must be used sequentially, so that each side knows the current password. S/Key uses a one-way hash function to hide the user's password during transmission. S/Key was developed by Bell Communication Research, Inc.

S/Key's *key* operation produces the list of one-time passwords you distribute to the user and Ascend Access Control. Both Ascend Access Control and the user invalidate a password after it has been used, so that it cannot authenticate the user twice.

Be careful not to store S/Key one-time passwords in a manner that allows someone other than the user to see them.

Implementing support for S/Key

- The S/Key library linked to `radiusd` uses a file named `skeypolicy` to determine how to find the S/Key database of user passwords. `skeypolicy` is in the `/etc` directory.
- To set up a user profile for S/Key authentication, make the Authentication-Type attribute a check-item and enter `S/Key` as the attribute's value.

Proxy Ascend Access Control servers

Ascend Access Control supports proxy RADIUS authentication. Proxy Ascend Access Control servers enable you to authenticate a user whose profile is in a remote Ascend Access Control server's `users` file. In a proxy arrangement, the Ascend Access Control proxy server transparently routes NAS Access Request packets to the remote server which authenticates the user. The proxy server then sends the remote server's responses to the NAS. The authenticating server may be another Ascend Access Control server or a RADIUS server. When Ascend Access Control supports authentication with a token key, the Ascend Access Control server is not acting, strictly speaking, as a proxy. It may best be described as an agent, client or translator of an ACE or Defender server that supports the token card process. For more information, see "Token Keys" on page 5-33.

Configuring proxy authentication

In a proxy authentication arrangement, Ascend Access Control must be informed that a remote RADIUS server will authenticate the user. You must provide Ascend Access Control with values that define the remote authentication method and explain the location of the remote server. The user's membership in a realm determines where you must enter these values. For more information, see See "Understanding an authfile" on page 5-15.

If the user is identified by realm:

1. Enter **`RADIUS`** as the value for `authfile`'s Type field.
2. Enter the remote server's location as a Domain Name Service hostname in `authfile`'s Realm/DNS/File field.

Following is an example of a realm's `authfile` entry. *RADIUS* indicates a remote Ascend Access Control server will authenticate the realm's users and *copper.edu* is the server's location:

```
lincoln.com RADIUS copper.edu
```

If the user is not a member of a realm:

1. In the user's profile, enter **`RADIUS`** for the Authentication-Type attribute.

2 Enter a value for the default RADIUS server's location in the Default_RADIUS_server entry in `authfile`.

Other authentication methods supported by Ascend Access Control

TACACS and TACACS+

TACACS and TACACS+ are versions of an authentication protocol developed by Cisco Systems, Inc. TACACS is a protocol for controlling dial up access through a single, centralized database. RFC 1492 explains that TACACS is a simple client-server protocol that authenticates by comparing received user names and passwords to stored user names and passwords. TACACS is similar to, but less robust than its extension, TACACS+, and Ascend Access Control.

The TACACS+ protocol provides more RADIUS-like features than TACACS. These features include authentication, authorization and accounting. TACACS+ also supports TCP transport instead of UDP transport, password encryption, and third party token cards. For more information, see "Understanding authorization" on page 5-7 and "Token Keys" on page 5-33.

Following examples of `users` file and `authfile` file entries define a user and the TACACS server that authenticates him.

users file example

The example's `Authentication-Type=TACACS` check-item specifies that the user is authenticated by TACACS.

```
Paul Reynolds Authentication-Type=TACACS
    Password=philo,
    Framed-Protocol=PPP,
    ...
```

authfile file example

The example identifies a default TACACS server Ascend Access Control consults whenever an authfile entry contains the Type field value `TACACS`. The Realm/DNS/File field value indicates an Ascend Access Control client named Default_TACACS_Server authenticates all of the users in Paul Reynold's realm.

```
tacrealm TACACS Default_TACACS_Server
```

Note: Review your TACACS or TACACS+ documentation before sending authentication requests from Ascend Access Control to a TACACS or TACACS+ server.

Kerberos

A Kerberos authentication server is a trusted third party that enables users and servers to identify each other and encrypt the messages they send over a connection. The Kerberos server can identify the user and the server because it maintains a centralized database of users and servers and their secret keys. When it can identify both sides of a requested connection, the Kerberos authentication server supplies each side with a shared secret key for their session. The two sides use the secret key to encrypt and timestamp their transmissions, ensuring the integrity of their exchanged messages.

Ascend Access Control supports two incompatible versions of the Kerberos 4 authentication protocol, AFS Kerberos and MIT Kerberos. AFS-KRB and MIT-KRB, respectively, are the arguments you enter in the `authfile` *Type* field. AFS Kerberos is the authentication protocol for AFS, a distributed file system originally known as the *Andrew File System*. AFS is the basis for Open Software Foundation's Distributed File System, DFS, and is now marketed and maintained by Transarc Corporation. MIT Kerberos is the version of Kerberos developed at Massachusetts Institute of Technology.

Review your AFS or MIT Kerberos documentation if you want either version to authenticate users. The documentation should describe a configuration file named `/etc/krb.conf.` Make sure the `/etc/krb.conf` file contains valid entries for the Kerberos realms. AFS Kerberos cells are the equivalent of MIT Kerberos realms.

Configuring Ascend Access Control for user authentication by a Kerberos server is similar to configuring it for TACACS or TACACS+ authentication. Enter the Kerberos realm name in `authfile`'s Realm/DNS/File field instead of entering a DNS hostname for the remote TACACS or TACACS+ server.

Token Keys

Ascend Access Control supports these vendor's security token products:

- AssureNet Pathways Defender Security Server
- Security Dynamics ACE server

Like S/Key, security token keys take the CHAP challenge/response method a step further. Token cards are portable devices which usually contain a secret key and perform a computation that allows the user to respond to an authentication server's challenge. Token keys may be referred to as Two-Factor Identification, meaning there is something the user has (the card) and something the user knows (a PIN number).

Token keys often resemble credit cards or calculators with small entry keypads. They store information and computational elements in flash memory. In addition to requiring a Personal Identification Number (PIN), most token cards also have internal software that detects attempts to read or change information stored on the card.

Some security token methods also include a timing element. Security Dynamics' SecureID card and its companion Ace authentication server have matched internal clocks. The token's response is only valid for a short time, after which it is replaced by a new response.

AssureNet Pathways DSS Server and SecureNet Key

Ascend Access Control may be an agent for users who authenticate with AssureNet Pathways' Defender Security Server and SecureNet Key tokens. SecureNet keys use an encryption algorithm to provide users with a one time password that is the response for the Defender Security Server's challenge. The one time passwords are created in real time when the user requests access. For security, SecureNet Keys might require a user PIN.

In addition to authenticating users, Defender Security Servers provide user audits, accounting for billing services, and printed reports.

Ascend Access Control supports multi-threaded functionality for AssureNet Pathways Defender Security Server (DSS), meaning that multiple authentication requests may be in progress simultaneously. Single-thread processing requires that the current request be handled to completion before a new request is accepted.

To support Defender and SecureNet Keys you have place a file named `agent.cf` in the `/etc/raddb` directory. The file is created when you install your Defender server. The Defender server's documentation includes instructions for creating and configuring `agent.cf` and placing it on the Ascend Access Control server. The `agent.cf` file is akin to the Ascend Access Control clients file, containing information about the Ascend Access Control and Defender servers that enable them to recognize each other and work together.

Five different variables may be defined in the `agent.cf` file:

Table 5-8. AssureNet Defender agent.cf file entries.

Name	Type	Description
`agentkey`	key	The key used between the agent and DSS
`agentid`	string	The agent identifier
`dss_address`	string	The hostname or IP address of the DSS
`dss_port`	integer	The port number used by the DSS
`dss_timeout`	integer	The timeout in seconds to wait for a DSS response

Following is an example of an `agent.cf` file:

```
agentkey = 0x01, 0x23, 0x45, 0x67, 0x89, 0xab,
0xcd, 0xef
agentid = foobar
```

```
dss_address = 10.11.12.13
```

Security Dynamics SecureID and ACE server

Ascend Access Control can be a client to Security Dynamic's Ascend Access Control Encryption (ACE) servers. ACE/Server is a software program and ACE servers authenticate users who carry Security Dynamics' SecureID card. The carrier of a SecureID card uses a PIN and a password for authentication. The authentication procedure does not include challenge/response exchange between the user and the server.

SecureID card holders do not enter a PIN, or user name, and wait for a challenge from the ACE server. They enter a PIN and password together when requesting access. Through programming in its own memory, the SecureID card provides a different time-limited code, or password, every 30 to 60 seconds. Internal matching clocks in the ACE server and the SecureID card are incorporated into the Security Dynamics hash algorithm so that each entity knows the appropriate password at any given moment.

When the PIN and password code are entered together they form a whole authentication key. The key cannot be duplicated by someone who finds or steals a SecureID card because the PIN component will be missing. If someone steals a user's PIN and SecureID code as they are entered, they quickly become useless because the password code changes.

In addition to authenticating users, ACE servers provide accounting utilities and may monitor login and administrative activities.

ACE servers interact with ACE/Clients. These two entities resemble a Ascend Access Control server and a NAS because the ACE/Client is the user's interface and transparent agent for accessing a network. The ACE/Client initiates, transmits, and manages user authentication requests and the ACE server's responses. Requests and responses are encrypted.

Ascend Access Control supports multi-threaded functionality for ACE servers, meaning that multiple authentication requests may be in progress simultaneously. Single-thread processing requires that the current request be handled to completion before a new request is accepted.

Ascend Access Control supports New PIN mode which allows users to change their PIN.

Creating Example Client, User and Realm Entries

6

This chapter explains how you obtain an Ascend Access Control license key and configure Ascend Access Control's data files.

A series of examples provides the instructions for configuring data files. The examples start with a simple configuration for a Network Access Server, two users, and an Ascend Access Control server. Gradually, the examples add more clients and users, and introduce the concepts of realms, proxy servers, and ODBC-compliant Database Management Systems.

How to use this chapter

This chapter explains how to create entries in Ascend Access Control's `clients, users,` and `authfile` files. Follow the illustrations to learn which steps you should apply in building the files that provide Ascend Access Control authentication for your own user community. You should also read this chapter to see the relationship between Ascend Access Control components and the files that allow the components to connect and communicate

This chapter also describes three companion utilities and a feature of the RADIUS daemon. Two utilities, `radcheck` and `radpwtst`, test whether an Ascend Access Control server is operating correctly and whether it can recognize a specific user profile's Password attribute value. The third utility, `convert.pl`, converts user profiles created for RADIUS. The daemon feature is debugging, a troubleshooting tool which captures system commands as they are executed and stores them in a file called `radius.debug`.

The examples begin with a simple configuration, then add more Ascend Access Control features, such as support for user realms, proxy authentication, token card devices, and Database Management Systems (DBMS). To understand the user profiles created in the examples, you don't need to know about all the attributes that Ascend Access Control supports. However, you can refer to Appendix B, "Attributes Reference," for information about any of the attributes.

Before you create your own Ascend Access Control file entries, review gathering Ascend Access Control information in "Ascend Access Control overview" on page 5-2 Then refer to Appendix B, "Attributes Reference,"after collecting information about the users you want to authenticate. That section is a guide to all the attributes Ascend Access Control supports.

What the examples show

The examples are more than just lists of sample user profiles and `clients` file entries. They include explanations of the entries. For example, they describe such things as the proper format of file entries and the effect of entering a particular value in a file's field. They show how to separate check-items and reply-items in a user profile and how to create new `users` files by entering Prefix field values in the `authfile` file.

Why Ascend Access Control GUI's are not discussed

Ascend Access Control is distributed with two graphical interfaces that automate the tasks of editing the configuration files. However, this section's examples do not refer to the Access Control Manager or the User Account Wizard. Instead, they suggest that you edit the files with a favorite text editor, such as vi or emacs. There are several reasons for this, including the following:

- Many people are more comfortable editing files manually.
- Seeing actual file entries helps you understand what the graphic user interfaces do when you select an attribute or value from their proffered lists.
- The graphical interfaces are already described in detail in Chapter 4, "Configuring Ascend Access Control Files."

What you need before you start

Prepare for Ascend Access Control installation by reviewing lists in the following two subsections. Also, you need root privilege on the Ascend Access Control workstation when you install the program. You do not need root privilege to change Ascend Access Control's default configuration after installation.

Ascend Access Control installation and activation

To install and activate Ascend Access Control you need the following:

- Ascend Access Control CD ROM.
- Ascend Access Control license key.
- Workstation running one of the following operating systems:
  - AIX 4.1
  - Solaris Intel 2.5
  - Solaris SPARC 2.5
  - SunOS 4.1.4
  - HP-UX 10.x or 9.0
  - Windows NT 4.0

- TCP/IP connection between the Ascend Access Control server and Network Access Server (NAS) clients.

clients and users files configuration

To configure entries in the `clients` and `users` files, you need the:

- Clients' secret keys.
- Users' authentication and authorization information.

Graphical User Interfaces

To create and edit entries in Ascend Access Control data files with the graphical user interfaces, you need to install version 1.0A of Access Control Manager and User Account Wizard on a workstation running Windows95 or Windows NT 4.0.

Access Control Manager and User Account Wizard are Java applications. Version 1.0A of the applications run within the Java Virtual Machine on Windows 95 and Windows NT 32-bit operating systems. Later versions of the GUIs will run within a Java-capable browser across all platforms, including UNIX systems.

Installing Ascend Access Control

Use a text editor to open the README file on the Ascend Access Control CD-ROM. It contains instructions for installing Ascend Access Control and the Ascend Access Control graphical user interfaces.

The Ascend Access Control CD-Rom contains the program's binary files, documentation, installation scripts, graphical user interfaces and HTML help files. In addition, Ascend supplies some related utilities and a demonstration version of the Ascend Secure Access software for units that support the Ascend firewall security feature.

Ascend Access Control CD-ROM directories

Ascend Access Control CD-ROM's alphabetically arranged directories contain:

- Adobe Acrobat Reader
- Archived copies of the Ascend Access Control binary files and the Access Control Manager and User Account Wizard GUI's
- Documentation for Ascend Access Control and the RADIUS IETF RFC's
- GUI installation files, including a setup wizard for Windows 95 and Windows NT operating systems
- HP-UX binary Ascend Access Control files and Install script
- HTML help files based on Ascend RADIUS attributes
- Miscellaneous
- Secure Access Manager's program and installation wizard for Windows operating systems
- Solaris Ascend Access Control package
- Source code for perl language to compile and run a RADIUS-to-Ascend Access Control user profile conversion utility
- SunOS binary Ascend Access Control files and Install script

Adobe 2.1 and Adobe 3.0

All user guides and white papers on the Ascend Access Control CD-ROM are provided in postscript and PDF formats. The CD-ROM contains two versions of Adobe Acrobat Reader with which you can read and print the PDF documents. Both versions can be installed on Windows and UNIX operating systems. Version 3.0 enables you to view PDF documents in web browsers such as Netscape and Internet Explorer.

Install version 2.1 for Windows by double-clicking `Acroread.exe`. If you want to install 2.1 on a UNIX system, uncompress and untar the appropriately named file and follow the instructions in the archive.

Install version 3.0 for Windows by double-clicking `ar32e30.exe.` On UNIX systems, uncompress and untar both files which refer to your operating system, such as, `acrdsrch_hpux_30.tar.Z` and `acroread_hpux_30.tar.Z`.

Archives

This directory contains zipped versions of the Access Control Manager and User Account Wizard GUI's and tarred and zipped versions of Ascend Access Control for HP-UX, Solaris, and SunOS. You do use these archived files when you install the GUI's or Ascend Access Control. Those files are located in other CD-ROM directories.

Documentation

The Documentation directory contains postscript and PDF versions of the Ascend Access Control User Guide and the International Engineering Task Force Request For Comment documents for the RADIUS and RADIUS Accounting.

GUI

The GUI directory contains both Ascend Access Control graphical user interfaces. You can install Access Control Manager by going to the `Win32\ACM\disk1` subdirectory and double-clicking `setup.exe` to start an Install Shield wizard. Use the same process to install the User Account Wizard from the `Win2\UAW\disk1` subdirectory.

HPUX

The `hpux` directory contains the binaries for Ascend Access Control (in `ASNDac`) and perl (perl5). The software may be installed from the CD-ROM by following the instructions in the `Readme` file in the CD-ROM's base directory. The `Readme` file contains information about this version of Ascend Access Control and your preparations for installing the program.

swinstall command

You can use the swinstall command to install Ascend Access Control for HPUX 10.x. The `swinstall` command enables you to automatically or interactively install software. If you choose to interact with the installation process, you can do so through a terminal interface or a Graphical User Interface. The `swinstall` command and its options are described in detail in the HP-UX 10.x `swinstall` man page.

HTML

The HTML directory contains over 140 HTML files about the attributes you can use in user profiles. They provide on-line help you can view in your web browser, which can open them directly from the CD-ROM. The HTML files are derived from the documentation for Ascend MAX units and are not a complete help utility. The documentation was developed for Ascend RADIUS and you may find some examples in the files that Ascend Access Control does not support.

For instance, some examples may instruct you to set up token key authentication with attribute/values like `Password="ACE"` or `Password="SAFEWORD".` Ascend Access Control uses the Authentication-Type attribute to set up token key authentication. For more information about token key authentication, see "Example 3 — expanding the model again" on page 6-29 or "Ascend Access Control authentication methods" on page 5-28.

Miscellaneous

Miscellaneous contains postscript and PDF versions of a white paper on firewall security. It is included to complement the demonstration version of Secure Access Manager on the CD-ROM.

SAM

The SAM directory contains a demonstration copy Ascend's Secure Access Manager firewall program. You can install SAM and use it for 30 days after obtaining a license key from the Ascend Technical Support Center. Contact information for the center is in the front material of the Ascend Access Control User Guide.

With Secure Access Manager's Windows-based interface you can create firewalls for Ascend units running software that supports the SAM security feature. Install SAM by double-clicking `setup.exe` in the SAM directory to start an Install Shield wizard.

SAM features on-screen Windows help and the SAm directory contains the Secure Access User Guide in postscript and PDF formats.

Solaris

You can use the `pkgadd` command to install Ascend Access Control on Solaris machines.Follow the instructions in the `Readme` file in the CD-ROM's base directory. The `Readme` file contains information about this version of Ascend Access Control and preparations for installing the program.The `solaris` directory contains the binaries for Ascend Access Control (in `ASNDac`) and perl (perl5).

SunOS

Ascend Access Control's installation on a SunOS machine mirrors the HPUX description above. The `sunos` directory contains the binaries for Ascend Access Control (in `ASNDac`) and perl (perl5). You can install the software from the CD-ROM by following the instructions in the `Readme` file in the CD-ROM's base directory. The `Readme` file contains information about this version of Ascend Access Control and your preparations for installing the program.

Windows NT 4.0

You can install Ascend Access Control for Windows 4.0 from the CD-ROM's `ASNDacnt.exe` file. The file is self-extracting. It begins an *InstallShield* utility which guides you through the Ascend Access Control installation. InstallShield creates system directories and extracts the program's configuration files automatically.

InstallShield installs Ascend Access Control in the default directory, `C:\Ascend\Access_Control\` if you don't enter an alternative. InstallShield prompts you to enter your server's name, which you can find by typing `hostname` at the operating system prompt. Make sure that you enter the server's true hostname. It may not be the name by which you know the machine and you need the system's hostname to produce an Ascend Access Control license key.

If you install Ascend Access Control before you generate a key you must enter your key in a file called `licenses` which InstallShield places in the Ascend Access Control data directory. By default, InstallShield places the `licenses` file in the `C:\Ascend\Access_Control\Database d`irectory.

InstallShield instructions

Following are the InstallShield program steps:

1. Click *Next* to begin when the InstallShield appears
2. Enter your name and company.
3. Click *Next* to accept the default Ascend Access Control directory or Browse to choose a different location.
4. Click *Next* to accept *Ascend* as the folder InstallShield will create, or type another name for the folder
5. Accept your entries and selections or select *Back* to change them.
6. Enter server's hostname and key or click *Next*.

   The InstallShield creates the Ascend Access Control subdirectories and installs all Ascend Access Control files in them. It also installs distributed libraries (`*.dll` files) and drivers in other locations on the server's hard drive.

A dialogue box appears, asking if you want to restart the server. If you click *Yes*, the server reboots and adds *RadiusSrv* to the list of services on the server.

Directories and Files

Following are the subdirectories and the files the Install Shield wizard creates under the directory, `C:\Ascend\Access_Control`:

`\Accounting`

- The `\Accounting` subdirectory is empty.

`\Bin`

- The `\Bin` subdirectory contains the `AC_Admin.exe` and `radiusd.exe` files.

  These are the Ascend Access Control administration program and the RADIUS daemon, respectively. `AC_Admin` enables you to start, stop, refresh, and query *RadiusSrv,* the Ascend Access Control server (Figure 6-1).

`\Database`

- The \Database subdirectory contains the `authfile`, `clients`, `dictionary, templates, users`, and `vendors` files.

`\Examples`

- The `\Examples` subdirectory contains ten files which include examples of entries for the Ascend Access Control data files.

Figure 6-1. AC_Admin screen

Configuring the Ascend Access Control Service

To configure the Ascend Access Control service on Windows NT:

1 Click *Start* on the taskbar.

2 Click *Settings* and choose *Control Panel*.

3 Select the *Services* icon from the *Control Panel* icons.
A list of available services appears in a dialogue box (Figure 6-2).

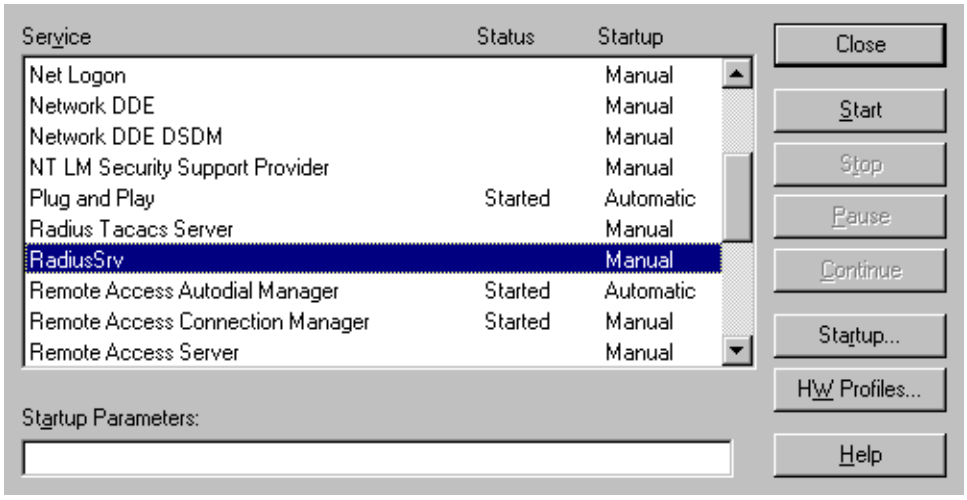


Figure 6-2. List of services on an NT server

Changing Ascend Access Control's default configuration

By default, the Ascend Access Control server, called *RadiusSrv* in the list of Windows NT services, is a Manual service. The alternative designation is Automatic service. An Automatic service starts when the server boots up. You can change RadiusSrv to an Automatic service:

1 Click *Startup...*

2 Click *Automatic*.

Figure 6-3. Startup textbox.

Changing Ascend Access Control parameters

You can also change the options of the RADIUS daemon by typing new options and values in the Startup Parameters textbox in the Services dialogue box (see Figure 6-2). For example, by default, the RADIUS daemon listens for authentication requests at port 1645. If you want to change the port number to 5625, type -p 5625 in the Startup Parameter textbox. You can change as many different RADIUS daemon options and values as you want in the textbox.

If you want to change a default or current Ascend Access Control path name you must type two backslashes between each segment of the path name. The first backslash is an escape character. For example, to change the data directory from `C:\Ascend\Access_Control\Database` to `C:\Ascend\AC\Data`, type the following in the parameters textbox:

```
-d C:\\Ascend\\AC\\Data
```

Obtaining an Ascend Access Control license key

1. Using a Web browser that supports HTML documents with frames, contact:
   `http://www.ascend.com/products/accesscontrol`
2. Jump to the Ascend License Server by following links for downloading software.
3. Select Ascend Access Control from the Product List and Permanent from the Key Type list.
   For information about obtaining a temporary license for a demonstration version of Ascend Access Control, see "Obtaining a temporary Ascend Access Control license key" on page 3-4.
4. Click Go.
   A frame containing Ascend's End User License Agreement appears.
5. Click I Agree at the bottom of the agreement.
6. Enter the serial number of your Ascend Access Control CD-ROM.
   A frame containing a message that includes you license key appears.
7. Create a file named `licenses` in Ascend Access Control's data directory.
   If you change the default directory, `/etc/raddb`, add `licenses` where you install Ascend Access Control.
8. Make `licenses` mode 600 with root ownership
9. Add a line to `licenses`, following the format:
   ```
   your_hostname your_license_key
   ```

Caution: Ascend Access Control does not recognize file names such as `licenses.txt` or `licenses.doc`. The name must be `licenses`. If you create the licenses file with a text editor that automatically assigns an extension to the file name, you must remove the extension before you start Ascend Access Control.

Example 1 — a simple model

The first example explains the preparations for authentication of two users, DEFAULT and Victoria. They contact a NAS, named George. The NAS is supported by one Ascend Access Control server called Martha. Victoria is a member of a small, ten person work group that performs administrative duties. The elements used in this example are displayed in Figure 6-4.

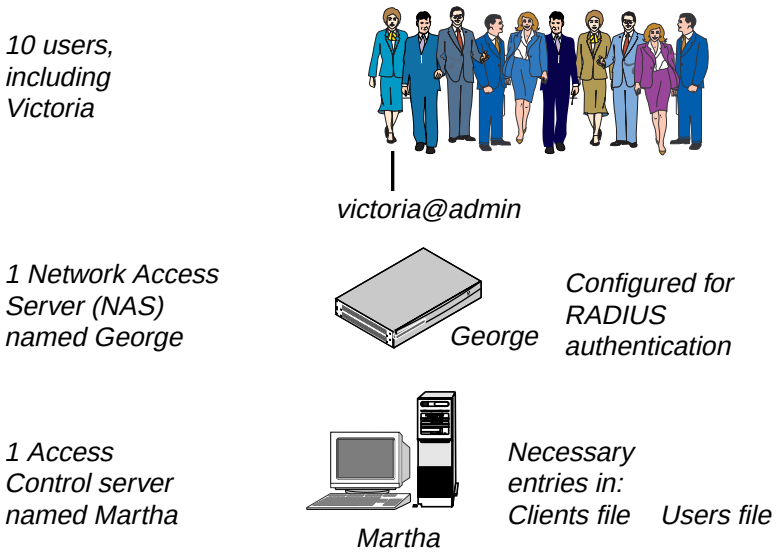


Figure 6-4. Users, client and Ascend Access Control server in example 1.

Note: configuring the client for authentication

The NAS in this example is represented by a router that supports authentication via Ascend Access Control. This user guide does not describe configuration of the router or a generic step-by-step guide for configuring a NAS. Many vendors' units can fill the role of the generic NAS in this example. Each type of NAS has its own interface, or suitable method for configuring authentication support, so you should consult the vendor's documentation if you require information about the NAS.

Please remember to configure your own NAS unit(s) to support user authentication by Ascend Access Control. If you are using an Ascend unit, such as a MAX 4000 or TNT router, authentication configuration is described in the documentation's security supplement.

Example 1 — the steps

You must perform the following steps to completely configure the NAS and the Ascend Access Control server before attempting to authenticate a user.

- Configure the NAS according to the instructions in its documentation.
- Edit the `clients` file on the Ascend Access Control server named Martha, using vi, emacs, or another text editor.
- Edit Martha's `users` file with your text editor.

Example 1's clients file

Figure 6-5 displays the `clients` file entry that creates the client NAS named George. Individual entries in the `clients` file are separated by whitespace. Ascend Access Control recognizes a tab or space as whitespace. Comments must begin with a pound sign (#).

Note: The `clients`, `authfile` and `users` files are installed at the same time as the Ascend Access Control software. By default, the installation places these files in the server's `/etc/raddb` directory.

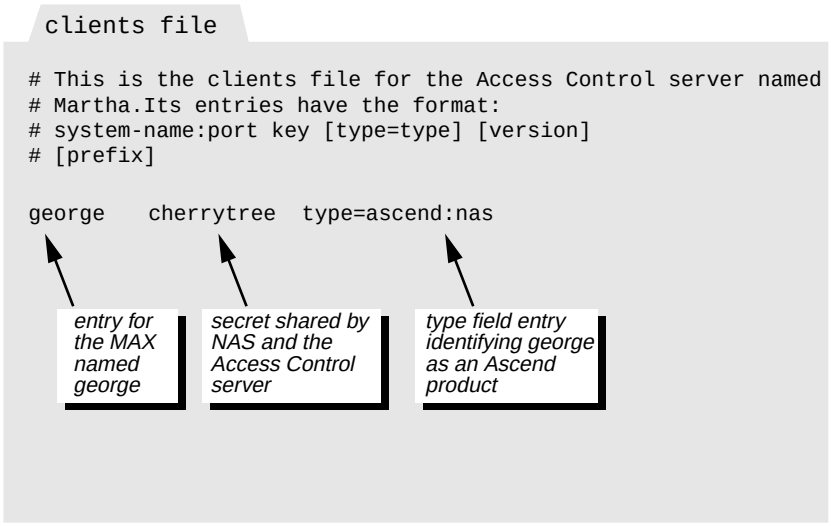


Figure 6-5. `clients` *file entry for the NAS in example 1.*

Understanding example 1's clients file entry

The entry includes three fields of information about the NAS. The *System-name:[port]* field specifies that the name of the NAS is *george*.

You may, in this field, also include the port from which the NAS sends its Access-Requests to the Ascend Access Control server. If the client, george, should always send Access-Requests from port 5325 enter:

```
george:5325
```

The *Key* field specifies the secret key shared by the NAS and the Ascend Access Control server. The NAS always sends an encrypted form of the secret key to the Ascend Access Control server.

The *Type* field has a value of **`ascend:nas`**, which identifies the client's vendor and type. The word **`nas`** must be preceded by a vendor name and a colon if the NAS is to receive vendor-specific attributes in Access-Accept responses. If you

only enter **`nas` in the Type field,** the server does not send the client vendor-specific attributes.

You can also enter **`proxy`** in the Type field, which specifies that the client is another Ascend Access Control server.

Example 1's users file

Figure 6-5 displays the Ascend Access Control `users` file entries that create user profiles for the DEFAULT user and victoria.

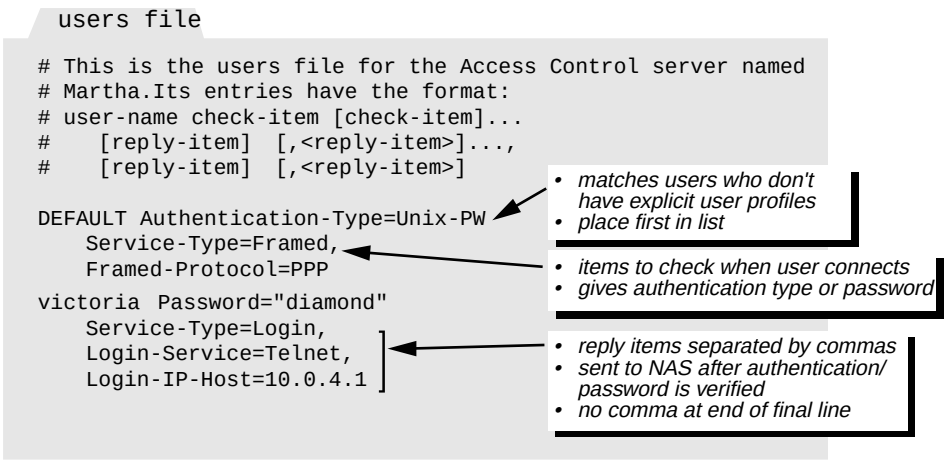


Figure 6-6. users file entries for DEFAULT and Victoria in example 1.

Victoria's co-worker's profiles would be very similar to hers because their activities on the network require the same access to hosts and services. In fact, it is possible to authenticate a small, very similar group of users with only a DEFAULT profile that includes an Authentication-Type attribute with a value such as Unix-PW.

users file format

The initial line of each entry in the `users` file is left-aligned. Subsequent lines in each entry begin with whitespace. Ascend Access Control recognizes a tab or space as whitespace. You may use either whitespace or commas to indicate the continuation of a series in a list. You may not use them after the last authentication check-item or the last configuration reply-item. See "Components of a users file entry," below for more information about check- and reply-items. Comments must begin with a pound sign (#).

Components of a users file entry

The user profiles for Victoria and DEFAULT include authentication and configuration information. Ascend Access Control uses information from the first line of each profile to authenticate Victoria and DEFAULT. Ascend Access Control sends the information on the subsequent lines in its replies to George, the NAS which uses the information to configure the connection it provides the DEFAULT user or Victoria.

Check-items or reply-items

The attribute/value pairs on the first line of a user profile are called check-items, and the attribute/value pairs on the subsequent lines are called reply-items. Attribute/value pairs are defined in many sections of this user guide. For more information, see the sections "users(5)," and "dictionary(5)," in Appendix A, "Ascend Access Control files and commands." user

You may enter as many check-items as you wish in a user profile, but they all must appear on the first line. The first line can wrap to a second line if the list of check-items is long. But you cannot artificially cause the line to wrap by entering a line break or carriage return. The first line in the following example is correct, but the second line is not.

```
johnblanker Password=apihfniali, Calling-Station-
ID=6145551212
```

```
johnblanker Password=apihfniali,
Calling-Station-ID=6145551212
```

Check-items are additive. Each condition set with a check-item must be met to authenticate the user. Authentication requirements grow more stringent as you place more check-items in a user's profile.

All lines that contain reply-items begin with whitespace. You may enter one reply-item per line, or many. If you do place more than one reply-item on a line, you may separate them with whitespace alone or with whitespace and commas. Commas are optional, but recommended for clarity in a long list.

Commas

Commas indicate continuation. You must add a comma at the end of line of reply-items if more reply-items appear the following line.

The last check-item in the first line and or the last reply-item in the user profile must not be followed by a comma. The absence of a comma indicates the end of the check-items and the end of the profile.

User-Name attribute

Ascend Access Control always interprets the first attribute in a user profile as the User-Name. The attribute is represented only by its value. For example, the DEFAULT user profile begins with the value DEFAULT rather than the attribute/value pair, User-Name = DEFAULT.

The DEFAULT user profile

The DEFAULT entry ensures that everyone can be matched to a profile in the `users` file. For example, there is no individual entry in the `users` file for Jane, one of Victoria's nine coworkers. When the NAS asks Ascend Access Control to authenticate Jane, the program searches for an entry that begins with the word Jane, finds none, authenticates Jane based on the DEFAULT check-items, and sends George a response containing the reply-items in the DEFAULT profile.

Located beneath the comments, the DEFAULT entry begins with the User-Name attribute and one check-item attribute, Authentication-Type. Following the first line are the reply-items Service-Type and Framed-Protocol. The User-Name attribute, DEFAULT, identifies the user described by this profile.

The DEFAULT user profile should be at the beginning of the user profiles so it can quickly be found when the user named in an Access-Request does not have a personal profile. Ascend Access Control searches the entire file for the non-existent profile then returns to the beginning of the file to find a DEFAULT profile. Placing it first reduces Ascend Access Control's search time.

Authentication-Type Check-item

The check-item `Authentication-Type = Unix-PW` tells Ascend Access Control to authenticate the user if information in an Access-Request packet from the client matches the password for DEFAULT in the server's `/etc/passwd` file.

Only check-items may appear on the first line of a user profile. Ascend Access Control uses DEFAULT and the Authentication-Type attribute/value pair to authenticate a user who matches the DEFAULT profile.

The Authentication-Type attribute and the Password attribute discussed in "Victoria's user profile" on page 6-22 are common Ascend Access Control authentication check-items, but they are rarely used together in the same profile. The Authentication-Type values "Realm" and "ACE" appear in user profiles in examples 2 and 3, which discuss user realms and token card devices.

Service-Type reply-item

The reply-item `Service-Type=Framed` indicates that a caller who matches the DEFAULT profile must use a framed protocol such as Point-to-Point Protocol (PPP), AppleTalk Remote Access (ARA) or Frame Relay (FR).

This attribute /value pair is indented, or preceded by whitespace, so it is a reply-item. Ascend Access Control will send this information to the client George in an Access-Accept packet. George will use this to configure the caller's connection, preventing the caller from connecting as a login user.

Framed-Protocol reply-item

The `Framed-Protocol=PPP` reply-item indicates that a caller who matches the DEFAULT profile must use the framed Point-to-Point Protocol (PPP).

Ascend Access Control also sends this information to the client.

Victoria's user profile

Victoria's user profile is as simple and uncomplicated as the DEFAULT profile. She must be authenticated so she can Telnet into the client's terminal server to start a Telnet session on another host with the IP address of 10.0.4.1.

User-Name check-item

The check-item `victoria` is the value for the User-Name attribute that must begin Victoria's user profile.

Password check-item

This `Password = "diamond"` check-item identifies the string that Victoria must provide as her password.

The password must be surrounded by quotes although Victoria does not need to type them when she is prompted for her password.

You must not enter a quotation mark within the password string when manually editing the `users` file because the second quotation mark identifies the end of the string. For example, if you use vi to change Victoria's password to "diam"ond" Ascend Access Control will accept the string "diam", but reject "diam"ond".

Service-Type reply-item

The `Service-Type=Login` reply-item indicates that George must create a Login connection for Victoria.

George may not set up a framed connection like the one given the DEFAULT user, who connects via the framed protocol PPP.

Login-Service reply-item

The `Login-Service = Telnet` reply-item allows Victoria to immediately begin an asynchronous Telnet session with the host specified by the Login-Host attribute after she is authenticated.

Login-IP-Host reply-item

The `Login-IP-Host = 10.0.4.1` reply item identifies the host that George connects Victoria with via Telnet after she is authenticated.

Example 2 — building on the simple model

In our second example, Victoria's work group has grown, and a realm called admin has been created to distinguish Victoria's group from another that contains a user named Albert. Another NAS, a router named Tom, has also been added to the network. Like George, Tom is supported by the authentication server called Martha. The elements used in this example are displayed in Figure 6-7.

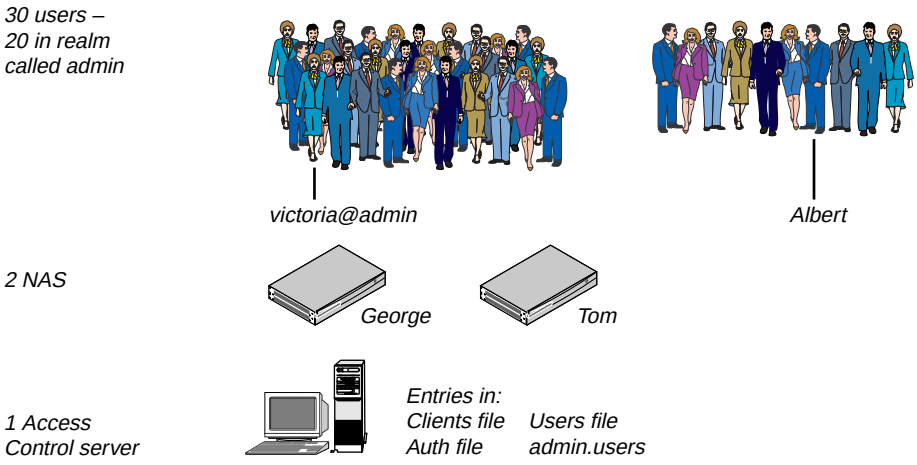


Figure 6-7. Example 2. A Realm called Admin and a second NAS appear.

Example 2 — the steps

You must perform the following steps to configure the new NAS, Tom, and the Ascend Access Control server Martha, before attempting to authenticate.

- Configure the NAS named Tom according to the instructions in its documentation.
- Edit the `clients` file on Martha, the Ascend Access Control server, using vi, emacs, or another text editor.
- Edit the `authfile` file on Martha with your text editor.
- Edit Martha's `users` file.

Example 2's clients file

Figure 6-8 shows the `clients` file on Martha, the Ascend Access Control server. It has been edited to add the new client named Tom. Tom and George are identical machines, and their entries are the same. You could add comments to describe each NAS. Comment lines begin with a pound sign (#).

clients file

```
# This is the clients file for the Access Control server named
# Martha.Its entries have the format:
# <system-name:[port] key [type=type] [version]
# [prefix]

george    cherrytree    type=ascend:nas

tom       unifova       type=ascend:nas
```

addition of second NAS named Tom in clients file

Figure 6-8. Example 2 `clients` file, with the entry for the NAS named Tom.

Example 2's authfile file

An `authfile` is the means by which Ascend Access Control supports user realms. It is similar to the `clients` file, in that each entry consists of values for fields that, together, describe a single entity. Example 1 did not include a step to create an entry in the Ascend Access Control `authfile`, because Victoria's work group was small and there was no need to divide it into realms.

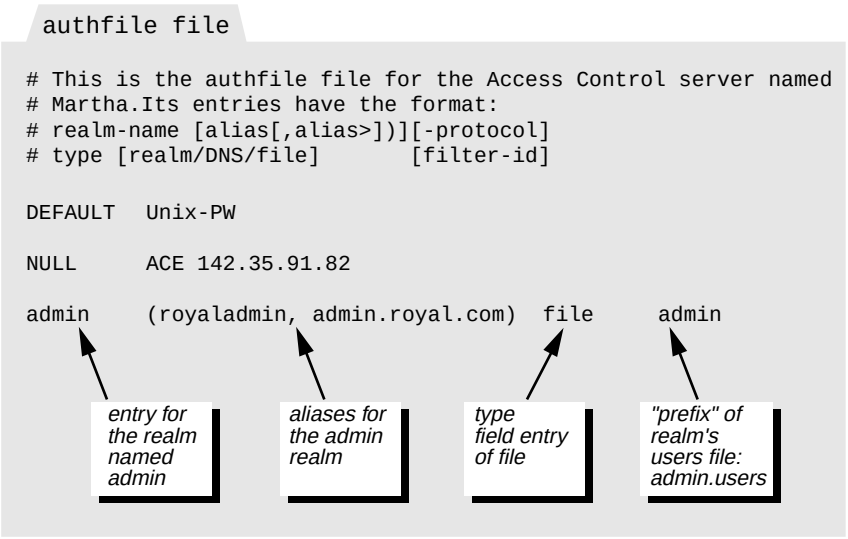


Figure 6-9. Example 2 `authfile` entry creating the admin realm and the users file named admin.users, which will contain Victoria's user profile.

Creating multiple users files

A file named `users` is created when Ascend Access Control is installed, but Ascend Access Control also supports additional `users` files you can create after installation. The files are created when you enter `File` in the `authfile`'s Type field and a name in the `authfile`'s Realm/DNS/File field. The Realm/DNS/

File entry is added as a prefix to the suffix `users`, creating a new `users` file. In this example, the new file is `admin.users`.

Examining the admin authfile entry

This one-line entry has far-reaching effects. In addition to creating the admin realm and the `admin.users` file, it defines the user names admin realm's users will provide to be authenticated.

- `admin`
  - This entry for the Realm-Name field is the name assigned to the realm
- `royaladmin, admin.royal.com`
  - This entry for the optional Alias field provides alternatives which can be used interchangeably with the actual realm name, admin. The purpose for allowing aliases is described in the section "Realm user name formats" on page 6-27
- `File`
  - This entry for the Type field causes Ascend Access Control to search for a `users` file with a prefix that matches the entry for the Realm/DNS/File field.

  You must enter a value for the Type field, choosing from a long list of options that includes: Passwd, Unix-PW, RADIUS, MIT-KRB, AFS-KRB, File, TACACS, TACPLUS, ACE, DEFENDER, S/KEY, and ODBC. These options are described in "authfile(5)," in Appendix A, "Ascend Access Control files and commands." Most of the options require that the Realm/DNS/File field also contain an entry that identifies the location of a server or a file name. For example:
  - If the realm's Type is RADIUS, Ascend Access Control acts as a proxy to a RADIUS server. The Realm/DNS/File field must contain a Domain Name Service address for the RADIUS server.
  - If the realm's Type is ACE, members of this realm are authenticated with a SecureID card. Do not enter information in the Realm/DNS/File field. A file named /`var/ace/sdconf.rec` on the Ascend Access Control server contains all the information about the ACE server.
- `admin`

– This entry for the authfile Realm/DNS/File field prompts Ascend Access Control to create a new file called `admin.users`. The file will contain the admin realm's users' profiles.

Realm user name formats

In example 1, the only individual user name in the `users` file's is Victoria. This simple name is enough to identify her profile when she requests her Telnet session. Now she is a member of the admin realm and the `authfile` entry for admin provides an identifier to add to her username.

Victoria can use either of two default formats to match the User-Name attribute in her user profile, `victoria@identifier` or `identifier/victoria`. The @ and the / characters are Ascend Access Control's default user name separators for members of realms.

The `authfile` entry allows Victoria to choose from among three identifiers that she can use interchangeably. The three identifiers in the admin entry are `admin, royaladmin`, and `admin.royal.com`., so Victoria can enter any of the following user names:

- `victoria@admin, admin/victoria`
- `victoria@royaladmin, royaladmin/victoria`
- `victoria@admin.royal.com, admin.royal.com/victoria`

Other authfile entries

`authfile` should contain at least two special entries, DEFAULT and NULL. DEFAULT is similar to `users` file DEFAULT user profile. If users supply a realm name that is not in `authfile`, they match the DEFAULT `authfile` entry. NULL provides a match for those users who:

1 provide a user name unaffiliated with a realm

2 match a DEFAULT profile with an Authentication-Type value of `Realm`

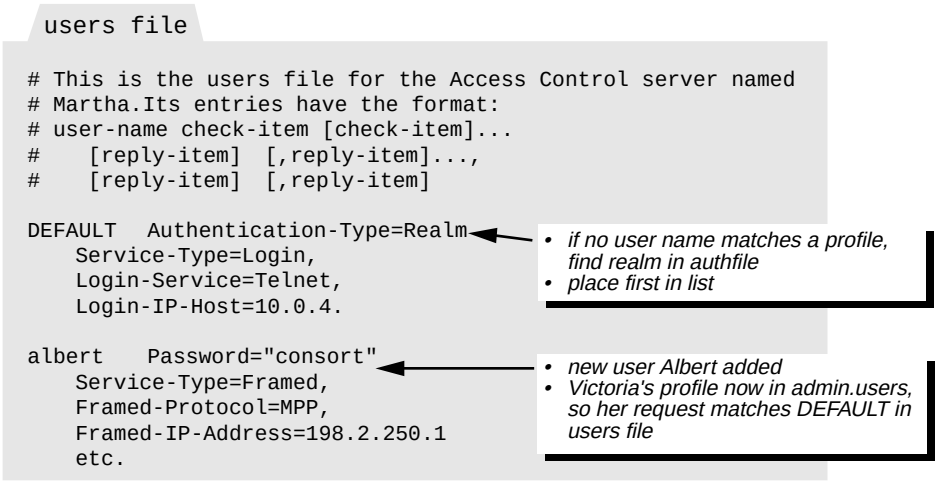
Typically, there are two reasons to use the NULL realm:

1 You can create a minimal `users` file containing only DEFAULT entries to speed up processing of a realm's user profiles.

2 You can ease the migration from an environment with no realms to one that does have realms.

Example 2's users file

Figure 6-10. Example 2's edited `users` file.



Examining the users file again

Figure 6-10 displays the Ascend Access Control `users` file following the creation of the realm for Victoria's work group and the addition of Albert's work group. The file has been changed in many ways:

- Victoria's user profile has been deleted from the `users` file and added to the file named `admin.users`.

  Her User-Name in that file is not, as you might expect, `victoria@admin`, or any of the other possibilities shown in "Realm user name formats" on page 6-27. Ascend Access Control strips the realm identifier from her user name before sending it to `admin.users`.

- The DEFAULT profile has also been edited. Its Authentication-Type value is now `Realm`. `authfile` is consulted when Ascend Access Control cannot find an individual's personal user profile in `users` file. All of the members

of Victoria's admin realm match DEFAULT because their profiles are now in `admin.users`.

- Albert's user profile has been added.

Example 3 — expanding the model again

In the third example, Victoria's work group has grown again. Albert's group, while not a realm, now authenticates using an token card device called SecureID. A different vendor's router, named Abe has been added to the network as a client and an ACE server handles SecureID authentication for Albert's group. The elements used in this example are displayed in Figure 6-11.

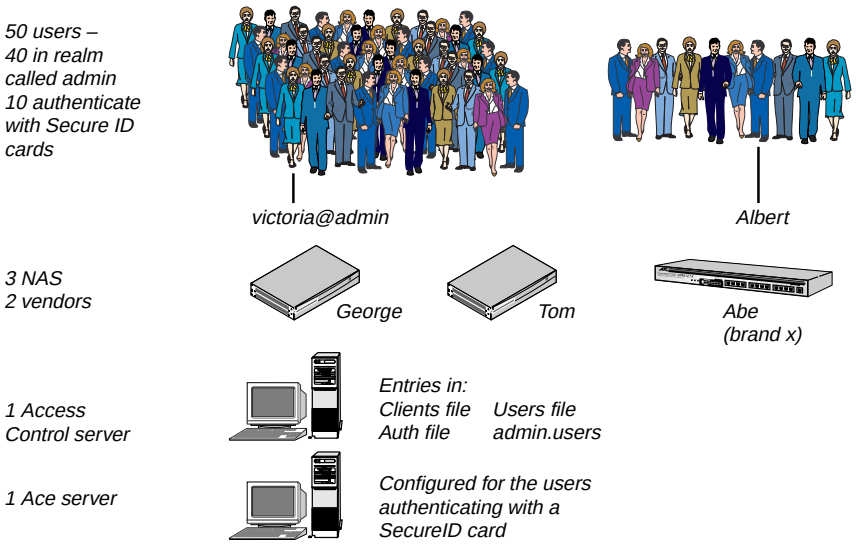


Figure 6-11. Example 3: More users, a new clients, a new server, and a new authentication method, electronic keys.

Example 3- the steps

You must perform these steps to configure the new NAS, Abe, and the Ascend Access Control server Martha, prior to authenticating users.

- Configure the NAS named Abe as instructed by its documentation.
- Edit the `clients` file on the Martha, the Ascend Access Control server.
- Edit Martha's `users` file.
- Add a binary file named `sdconf.rec` to Martha.
  The file is created on the ACE server when you install the Security Dynamics program. Copy the file to Martha.

Example 3's clients file

Figure 6-12 displays Martha's `clients` file after it has been edited to add Abe. Abe's entry is different from the Ascend units, George and Tom. They understand the `dictionary` file's vendor-specific Ascend attributes. The comment about Abe explains that this NAS only understands attributes from the standard

RADIUS protocol. Abe ignores vendor-specific attributes sent to it as reply-items from user profiles.

Figure 6-12. Example 3's clients file with the addition of the NAS, Abe.

clients file

```
# This is the clients file for the Access Control server named
# Martha.Its entries have the format:
# <system-name:[port] key [type=type] [version]
# [prefix]

george    cherrytree    type=ascend:nas

tom       unifova       type=ascend:nas

# Abe is not an Ascend unit. It ignores vendor-specific
# attributes

abe       iameman       type=nas
```

- *new NAS named Abe*
- *type= nas, not ascend:nas*

Example 3's users file

users file

```
# This is the users file for the Access Control server named
# Martha.Its entries have the format:
# <user-name> <check-item> [check-item>]...
#    [<reply-item>]    [,<reply-item>]...,
#    [<reply-item>]    [,<reply-item>]

DEFAULT




albert    Authentication-Type="ACE"
    Service-Type=Framed,
    Framed-Protocol=MPP,
    Framed-IP-Address=198.2.250.1
    etc.
```

Albert's profile now includes the check-item "Authentication-Type" with a value of "ACE"

Figure 6-13. Example 3's `users` file showing Albert's new user profile attribute allowing him to authenticate via a SecureID card. (The DEFAULT entry has been truncated for this illustration, but it would contain valid attribute/value pairs.)

The Authentication-Type value of "ACE" is necessary for anyone who uses a SecureID card to authenticate. Ascend Access Control also supports devices distributed by AssureNet Pathways. If a user has an AssureNet Pathways device, the appropriate Authentication-Type value is "DEFENDER", which is the name of the AssureNet server.

A note about Ascend Access Control proxy servers

When Ascend Access Control works in concert with servers like ACE and DEFENDER, it is not really operating as a proxy server. That can only truly be said if Ascend Access Control is working with a RADIUS server or another Ascend Access Control server. The pertinent factor is whether or not the other server actually does contain user profiles that supply a NAS with reply-item attributes. ACE, DEFENDER and Kerberos servers play a part in authentication of users when they operate in concert with Ascend Access Control, but they do

not send through the Ascend Access Control server, the attribute/value pairs the NAS uses to configure the user's connection.

Ascend Access Control server's sdconf.rec file

The Ascend Access Control server's `sdconf.rec` file is not a component of Ascend Access Control itself. You install the file on the Ascend Access Control server when you configure an ACE server for users authenticating with SecureID token cards. This file must be added to any server which, like Ascend Access Control, supports ACE/SecureID user authentication. This user guide is not the proper source of information about configuring the `sdconf.rec` file or the ACE server. Please refer to the documentation supplied by the vendor of that product and other products like it.

Compatibility with Ascend RADIUS

The differences between Ascend's free RADIUS server source code and Ascend Access Control are explained in the following sections.

Changing Passwords

Ascend RADIUS supports the Ascend-PW-Expiration attribute, but Ascend Access Control does not. Ascend Access Control replaces Ascend-PW-Expiration with the Expiration check-item. Ascend Access Control does support password changing and the associated attributes, Ascend-PW-Warntime and Ascend-PW-Lifetime.

A user can change his password during the Ascend Access Control authentication process if you run the RADIUS daemon with the `-P` command line option and store the password in the user's profile. Ascend Access Control does not support password changing if the password in stored in another location, such as the UNIX password file or a database file.

This daemon command line supports password changing:

```
radiusd -P
```

This user profile allows password changing:

```
fredie Password="icwtifacgts", Expiration="Jun 10 1997"
    Ascend-PW-Warntime = 5
    Ascend-PW-Lifetime = 60
    Framed-Protocol = SLIP
```

Specifying a Token Card

Ascend RADIUS reserves Password attribute values such as "ACE" and "DPI" if you enable the reserve value feature when you compile the RADIUS source code. You can use these reserved values to specify the token card a user carries. Although Ascend Access Control recognizes these Password values, it does not reserve a special significance for them. Instead, Ascend Access Control automatically recognizes Authentication-Type attribute values that perform a similar function.

If you switch from RADIUS to Ascend Access Control, you can use a script called `convert.pl` to convert RADIUS token card users' Password values to Authentication-Type values. See "AppleTalk Remote Authentication (ARA)" on page 6-34.

Table 6-1 illustrates the change:

Table 6-1. Different means of specifying token cards

Ascend Access Control	Free RADIUS
Authentication-Type=UNIX-PW	Password="UNIX-PW"
Authentication-Type=ACE	Password="ACE"
Authentication-Type=DEFENDER	Password="DEFENDER"
Ascend Access Control does not support SAFEWORD	Password="SAFEWORD"

AppleTalk Remote Authentication (ARA)

Ascend RADIUS assigns two meanings to this reply-item entry in a user profile:

```
Framed-Protocol=ARA
```

One meaning is obvious; the authenticated user connects via the ARA protocol. But RADIUS also deduces from the attribute's value that the authentication method for this user is ARA.

Ascend Access Control separates the ARA protocol and the ARA authentication method. If a user is authenticated by ARA, the user profile must contain two attribute/value entries. Authentication-Type is a check-item that appears on the first line of the profile and protocol is a reply-item that appears below the first line, as this example illustrates:

```
arauser Authentication-Type= ARA-DES, Password="dsma-
jbyl"
      Framed-Protocol=Ascend-ARA
      Ascend-Send-Secret= "dsmajbyl"
```

Identifying Network Access Servers (NAS) Vendors

Ascend RADIUS does not provide a means for identifying a NAS vendor. The server sends to the NAS client all the standard and vendor-specific reply-items it discovers in a user profile, even though the vendor-specific attributes might not be understood by the client.

Ascend Access Control supports an entry in the `clients` file `Type` field that identifies the NAS vendor. When the vendor name appears in the entry, as shown below, Ascend Access Control only sends the user profiles' appropriate vendor-specific and standard reply-items to the NAS client.

```
larry tsksbtnas type=Ascend:NAS
```

Converting RADIUS user profiles

Ascend Access Control supports user profiles files created for the Ascend RADIUS server. The Ascend RADIUS and Ascend Access Control `dictionary` files are slightly different because Ascend Access Control conforms with the RADIUS RFC standard, but Ascend RADIUS source code is based on the standard's draft documents. The IETF RADIUS RFC standard

modifies a few of the attribute names and values that were proposed in the standard's draft documents. Table 6-2 and Table 6-3 compare Ascend Access Control and Ascend RADIUS attribute and value names.

Table 6-2. Attribute name changes

Attribute Number	Ascend Access Control	Ascend RADIUS
3	CHAP-Password	Challenge-Response
6	Service-Type	User-Service
8	Framed-IP-Address	Framed-Address
9	Framed-IP-Netmask	Framed-Netmask
11	Filter-ID	Framed-Filter
14	Login-IP-Host	Login-Host
20	Callback-ID	Callback-Name
30	Calling-Station-ID	Client-Port-DNIS

Table 6-3. Attribute value name changes

Value	Attribute	Ascend Access Control	Ascend RADIUS
1	Service-Type	Login	Login-User
2	Service-Type	Framed	Framed-User
3	Service-Type	Callback-Login	Dialback-Login-User
4	Service-Type	Callback-Framed	Dialback-Framed-User
5	Service-Type	Outbound	Dialout-Framed-User

Table 6-3. Attribute value name changes

Value	Attribute	Ascend Access Control	Ascend RADIUS
6	Service-Type	NAS-Prompt	Shell-User
1	Framed-Compression	Van-Jacobson-TCP-IP	Van-Jacobsen-TCP-IP
255	Framed-Protocol	Ascend-ARA	ARA

A perl language script called `convert.pl` automatically converts the Ascend RADIUS attributes and values so they match the standard's documentation.The `convert.pl` script is distributed with Ascend Access Control and is placed in the server's `/etc/raddb` directory when you install the program.

Note: You can use the `convert.pl` script's `-s` option to change old reserved Password values to reserved Authentication-Type values. Use the option cautiously, though, because the Password values were only reserved if you enabled the feature when building the `radiusd` executable when compiling the source code.

Running convert.pl

You can run `convert.pl` two ways. One method converts the selected `users` file's entries and overwrites the file. The other method creates a backup of the original file before the converting the file's entries.

Install a copy of the perl interpreter on the system before you run the `convert.pl` script. The script should run with PERL v4 or PERL v5.

Without backup

Invoke the `convert.pl` script by typing this on the command line, substituting the users file name as the variable. The lesser than and greater than signs are part of the command and you must enter them The converted file is sent to stdout.

```
convert.pl < users.old > users.new
```

With backup

Run this way, the script copies the `users` file and adds the extension.`bak` to its name. Then it converts the original file's entries and saves the file with the original file's name. If `users.bak` already exists, it is overwritten.

```
convert.pl users
```

Testing Ascend Access Control

Ascend Access Control provides two diagnostic tools called `radcheck` and `radpwtst` for testing an Ascend Access Control server. Run these diagnostic tools from the workstation's command line after installing Ascend Access Control and configuring its files. `radcheck` determines if your Ascend Access Control server, or any other you can access, is operational. `radpwtst` confirms that the server can authenticate a specific user. You can run each command with a variety of options to test a particular Ascend Access Control configuration. (Both commands are discussed in Appendix A, "Ascend Access Control files and commands," `radcheck` in "radcheck(8)" on page A-23 and `radpwtst` in "radpwtst(8)" on page A-26.)

Verifying Ascend Access Control is operational with radcheck

The `radcheck` command starts a process on an Ascend Access Control server to test if another Ascend Access Control server is operational. The target of the test does not have to be registered in the `clients` file on the server running the test. Type `radcheck` and the target server's Domain Name Service hostname. You can run the command with options that change `radcheck`'s default settings (Table 6-4). When debugging and version are enabled, `radcheck` prints the information to the server's standard output.

The command has the following format:

```
radcheck  [ -d] [ -p] [ -r] [ -t] [ -v] [ -x]
          servername
```

Option	Description	Default
`-d`	Ascend Access Control directory on server being tested	`/etc/raddb`
`-p`	Ascend Access Control port on server being tested	1645
`-r`	Number of verification attempts `radcheck` makes	10
`-t`	Length of time before `radcheck` times out	3 seconds
`-v`	Version of Ascend Access Control	Not Enabled
`-x`	Turn on debugging	Not Enabled

Table 6-4. `radcheck` *options and defaults*

radcheck example

The RADIUS daemon on an Ascend Access Control server named potter is running with the `-d` and `-p` options. The arguments for potter's `-d` and `-p` options are `/etc/aacrd` and `6495`. These arguments indicate that potter's Ascend Access Control files are in a directory named `/etc/aacrad` and that its authentication port is 6495.

You must `radcheck` with the same arguments as the daemon you want to test, so you might test potter by running the following command on another Ascend Access Control server.

```
radcheck -d /etc/aacrad -p 6495 potter
```

The example generates the following response:

```
auth queue: 9/7, acct queue: 3/3, maxtime: 0 (Fri Oct 25
16:28:36 1996)
authfile: 5, clients: 10, users: 200, fsmid: Ascend, Fri Oct
25 16:28:36 1996
```

```
Version 3.0 NOSHADOW sun
"potter(6495)" is responding
```

In addition to confirming that potter is operational, the response provides the following statistics about the server's status and configuration:

- Number of authentication requests and replies handled
  - 9 and 7 (from auth queue)
- Number of authentication requests and replies handled
  - 3 and 3 (from acct queue)
- Date and time of the test
  - Fri Oct 25 16:28:36 1996
- Number of entries in
  - authfile: 5
  - clients: 10
  - users: 200
- Finite State Machine Identification
  - Ascend
- Version of Ascend Access Control on potter
  - Version 3.0
- Operating system on potter
  - SunOS (from sun)

If the test were unsuccessful, the response would be:

`"potter(6495)"` *`message`*

Message has the following four variations:

1. `No reply from Ascend Access Control server "potter(6495)"`
   Although its request has been sent to the server, `radcheck` has timed out waiting for a response.You might try changing the timeout setting.
2. `Received non-matching id in server response`
   The server's reply packet contained an authenticator that did not match the hashed shared secret key that `radcheck` expects to receive from the server. `radcheck` cannot verify that the response is from the server named potter.

3. `Received invalid reply digest from server`

   The server's reply packet contained a digest code that did not match the digest code of the request packet sent by `radcheck`. `radcheck` cannot verify that the server's reply is a response to this specific `radcheck` request.

4. `No such server: "potter(6495)"`

   `radcheck` cannot find an Ascend Access Control daemon listening at UDP port 6495 on the server named potter or Domain Name Service cannot locate the server named potter.

Verifying user passwords on an Ascend Access Control server with radpwtst

You can use `radpwtst` to verify any user's password on a server running Ascend Access Control or RADIUS. `radpwtst` performs the verification on any user name that is entered on the command line as a `radpwtst` option. You can enter the username in the individual or realm format. The server prompts you to enter the user's password after it has located the user's profile, then sends a message confirming or denying the password you entered.

radpwtst options

Other `radpwtst` options allow you to specify where you want to search for the user's password information and where you want the server to send its answer. The options are very similar to those you can use with the `radcheck` command and are generally associated with changing the settings for:

- Server's data directory
- Users file, which might be named `users` or `prefix.users` if the username indicates membership in a realm
- Communications port
- UDP port
- Address of the client expecting the answer
- Number of retries
- Timeout limit

The format of the radpwtst command is:

```
radpwtst  [-c code] [-d directory] [-f file] [-g group]
          [-h] [-i client IP address] [-l async-port]
          [-p UDP_port] [-r retries] [-s servername]
          [-t timeout] [-u type] [-v [1|2]]
          [-w password] [-x] [-:<attribute>=<value>]
          username[@realm]
```

radpwtst example

```
radpwtst  -f admin.users -i 173.157.2.11 -r 5
          -t 5 kate
```

The command sets the number of retries to five and the timeout to five seconds. It also tells the client to pass the following message to the server:

Look up the password of a user named Kate in a file named admin. users. Send a prompt for the password to IP address 173.157.2.11.

If authentication of the user password succeeds, the message displayed is

```
authentication OK
```

If the authentication fails the message is

```
“userid” authentication failed
```

Debugging Ascend Access Control

You can capture a list of commands the system executes during Ascend Access Control authentication, authorization and accounting operations by enabling a feature of the RADIUS daemon called debugging. The list of commands is a tool for reviewing system activity and investigating Ascend Access Control configuration errors. You can also control what, and how much, information the list contains by setting the debugging level. Output from the debugging process is stored in a file you can read with any text editor. The file that stores debugging output is `radius.debug,` which is created when you enable debugging. You cannot change this default name or direct the debugging output to a different file.

By default, debugging is not enabled. You can enable it and set the debugging level by restarting the daemon process or by sending the process a signal

Enabling debugging from the command line

Following is the command line entry for restarting the daemon, enabling debugging, and setting the debugging level to 1:

```
radiusd -x
```

You can type the -x option on the command line more than once. Each additional -x increases the level of debugging, adding to the depth and variety of the information collected in the `radius.debug` file. This entry raises debugging to the third level:

```
radiusd -x -x -x
```

Level 3 debugging captures minimal debugging output, attribute/value pairs sent and received, high level output of the Finite State Machine, and function tracing

Note: You can enter more than one `radiusd` option at a time. The following entry changes the data directory, allows Token-caching and sets debug at level 3:

```
radiusd -d /etc/raddb/data -C -x -x -x
```

Enabling debugging with signaling

You can enable debugging while the daemon is operating by sending `radiusd` a SIGUSR1 signal. This signal affects debugging like the -x command option, increasing the debugging level one step every time you send the signal. You set the debugging level to 3 by sending `radiusd` three SIGUSR1 signals.

Disabling debugging

Disable debugging by restarting `radiusd` without the -x option or set the debugging level to 0 by sending the daemon a SIGUSR2 signal.

Comparison of debug and accounting detail information

`radius.debug` does not capture the same information as the accounting log, which collects data about authenticated connections from the NAS client. You enable RADIUS Accounting during the Ascend Access Control installation. Following are truncated examples from a `radius.debug` file and an accounting detail file. Debugging is set to level 2.

radius.debug example

```
directory = /etc/raddb Program = /usr/sbin/radiusd
rad_recv: entered
get_radrequest: entered
rad_recv: entered
get_radrequest: entered
rad_recv: entered
get_radrequest: entered
gen_valpairs: entered
    User-Name = “t031982”
    User-Password = “\x16 \xe9u\xf0”
    NAS-IP-Address = 192.0.0.1
    NAS-Port = 10501
    Service-Type = Framed
    Framed-Protocol = PPP
    State = “”
    Called-Station-Id = “5551212”
    Acct-Session-Id = “29600”
```

Accounting detail example

```
Sat Feb 15 07:50:46 1997
          User-Name = “t031982”
          NAS-IP-Address = 144.158.43.168
          NAS-Port = 10122
```

```
                Acct-Status-Type = Start
                Acct-Delay-Time = 0
                Acct-Session-Id = “224602551”
                Acct-Authentic = RADIUS
                Calling-Station-Id = “6307362368”
                Called-Station-Id = “7653150”
                Framed-Protocol = PPP
                Framed-IP-Address = 192.168.135.129

Sat Feb 15 07:50:55 1997
                User-Name = “t031982”
                NAS-IP-Address = 144.158.43.168
                NAS-Port = 10122
                Acct-Status-Type = Stop
                Acct-Delay-Time = 0
                Acct-Session-Id = “224602551”
                Acct-Authentic = RADIUS
                 Acct-Session-Time = 10
```

Open Database Connectivity (ODBC)

7

This chapter explains Ascend Access Control support for Database Management Systems that comply with the specifications for Open Database Connectivity ODBC.

Ascend Access Control and ODBC

Ascend Access Control `users` files perform sufficiently as databases for your user profiles if you are authenticating a manageable groups of users. However, if you authenticate thousands of users with Ascend Access Control, you can store Ascend Access Control user profile information in DBMS tables rather than `users` or `prefix.users` files. Scripts for creating DBMS tables are included in the appendix of the Ascend Access Control User Guide.

When you link Ascend Access Control and a DBMS you gain powerful data management capabilities in a central location. A DBMS provides the following advantages for administering user profiles:

- Most important DBMS vendors support the Open Database Connectivity (ODBC) standard. Open Database Connectivity allows you to use the same Application Programming Interface to store data in, or retrieve data from, any major DBMS database included in the table in Table 7-1.
- DBMS applications support the common Structured Query Language (SQL), language for requesting database output.
- DBMS applications support data access by multiple users.
- DBMS applications include security features that control DBMS access and transactions, preventing simultaneous editing the same user profile record.

Here are some important points to consider if you want to store user profiles and accounting information in an ODBC-compliant DBMS:

- You must provide the DBMS. You can use more than one DBMS if each supports the ODBC standard.

  Note: Although you can install Ascend Access Control and your DBMS on separate servers, Ascend recommends that you install them on the same server to improve security.
- Each DBMS may include multiple user profile tables.
- Each DBMS must include only one accounting table if Ascend Access Control's accounting option is used.
- You must provide a DBMS client and install it on the Ascend Access Control server.

- Each DBMS requires a Driver Manager and drivers that are compatible with the Driver Manager. INTERSOLV's Driver Manager won't work with Microsoft's drivers and vice versa. More information on Driver Managers and drivers is in "DBMS Driver Managers and drivers" on page 7-7.

Note about the RADIUS builddbm utility

Ascend Access Control does not support `builddbm`, a utility that creates an index of user profiles in the `users` file. When the `users` file has been indexed by `builddbm` the RADIUS daemon can more quickly search the file for a matching user profile. RADIUS programs that you must compile might permit you to use `builddbm` before you compile the program's source code.

Ascend Access Control does not support indexing and the `builddbm` utility because Ascend Access Control is delivered as a binary application, ready to install and run. You do not have to compile Ascend Access Control. Moreover, Ascend Access Control supports multiple `users` files and ODBC compliant DBMS, which provide much more powerful and flexible solutions for authenticating and authorizing large numbers of users than does a single, indexed text file.

Utilizing Ascend Access Control ODBC support

In a typical utilization of Ascend Access Control's ODBC support, one company might supply authentication services for several customers' users via one Ascend Access Control server. For security and control, the customers of the company providing authentication and authorization services might want to manage their own end user data, leaving configuration and maintenance of the authentication server and DBMS to the provider. If the provider uses Ascend Access Control, and takes advantage of its support for ODBC, each customer can rest assured that the integrity of its user profiles will be safely maintained in its own table in one DBMS.

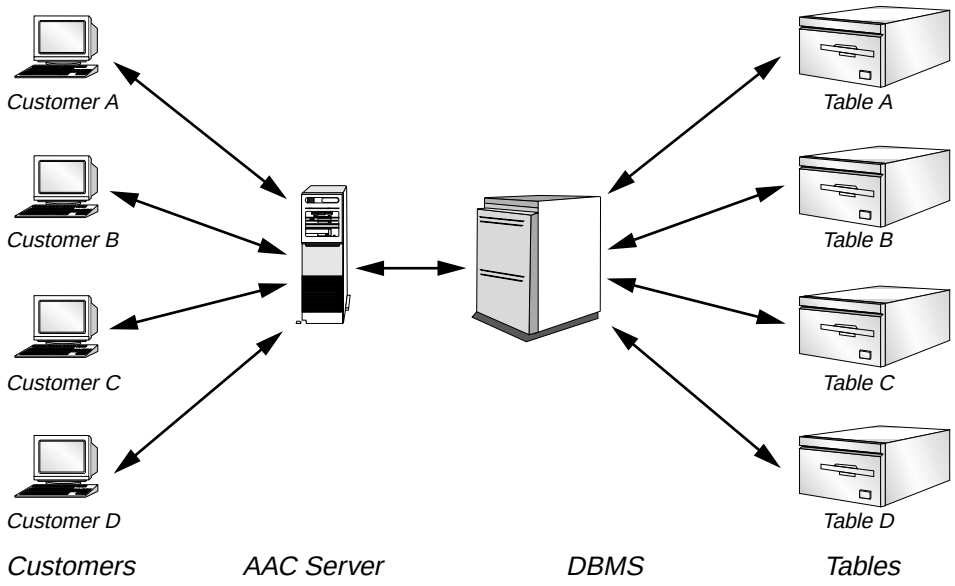


Figure 7-1. Customer access of ODBC DBMS tables via the Ascend Access Control server.

In Figure 7-1, customers A through D can access their own respective data sources, or DBMS tables. Anyone seeking access to a data source must provide an access name and access password. The customers manage the user profiles stored in the DBMS table. When end users need to be authenticated and authorized, Ascend Access Control contacts the appropriate data source to retrieve the user's profile.

Ascend Access Control/DBMS architecture

Following is a discussion of the Ascend Access Control server's ODBC-related components and the way SQL requests pass between the authentication server to the DBMS server. Figure 7-2 illustrates the Ascend Access Control-ODBC architecture on the Ascend Access Control server when the DBMS is on a different machine. The authentication and accounting processes are more secure if Ascend Access Control and the DBMS are on the same machine, but you may install them on different network machines as shown in Figure 7-3.

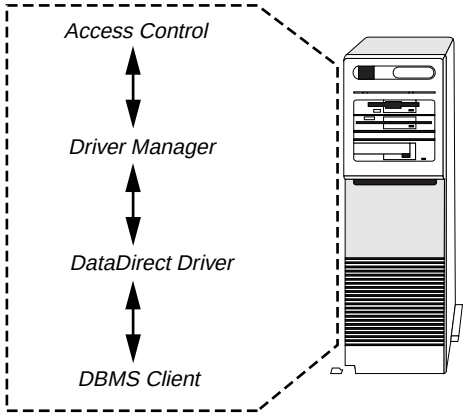


Figure 7-2. ODBC components on the Ascend Access Control server. Note that the Driver Manager might be provided by Access Control's server (UNIX) or the operating system (Windows NT 4.0).

Ascend Access Control

Ascend Access Control does not include a user interface for creating Structured Query Language (SQL) requests. However, it does create and send SQL requests to a data source and retrieve the results. The Driver Manager installed with Ascend Access Control is the direct recipient of these requests. Ascend Access Control recognizes the need to contact the Driver Manager when it searches a `users` file or `prefix.users` file and finds ODBC and data source information in a user profile A DBMS and its tables are jointly referred to as a data source.

Driver Manager

The Driver Manager receives the SQL request from Ascend Access Control. The request includes information about the data source with which Ascend Access Control must communicate. The data source information tells the Driver Manager which driver is needed for connection with the DBMS. For example, if the information says that the data source is an Oracle 7 table, the Driver Manager

loads the Oracle 7 driver. Then the Driver Manager calls from the driver the SQL function that Ascend Access Control has requested.

Driver and DBMS client

One of the functions that must be called sets up a connection with the DBMS. Working through a DBMS client, the driver establishes and closes the connection between the Ascend Access Control server and the ODBC-compliant data source. Other functions performed by drivers include:

- Providing information about the DBMS tables, columns and objects.
- Providing standard error codes.
- Delivering configuration information about file transaction isolation levels, which affect whether a file may be read and written to simultaneously by multiple users.
- Determining when edits in files are committed, or saved.

The client and the DBMS communicate through a data protocol. The DBMS client application must write and read the protocol, so that Ascend Access Control and the DBMS can communicate.

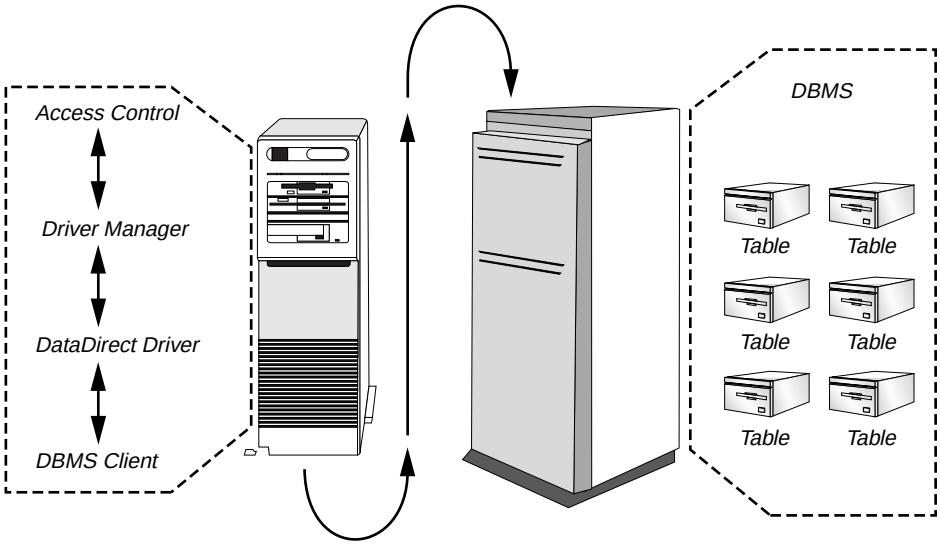


Figure 7-3. Flow of SQL request when Ascend Access Control and DBMS data source are on different servers.

DBMS Driver Managers and drivers

The Ascend Access Control server for UNIX operating systems includes an INTERSOLV Driver Manager so you must use INTERSOLV drivers for UNIX installations. The Ascend Access Control for Windows NT 4.0 server does not contain a Driver Manager because the operating system provides Microsoft's Driver Manager and Microsoft drivers for some ODBC DBMSs.

INTERSOLV drivers for UNIX Ascend Access Control

INTERSOLV drivers support most DBMSs that comply with the Open Data Base Connectivity (ODBC) standard. The drivers are not Ascend Access Control components. You must purchase the INTERSOLV drivers and install them on the Ascend Access Control server. Read the INTERSOLV documentation so that you can correctly install the drivers.

Table 7-1 includes INTERSOLV Version 2.x drivers for all the operating systems supported by Ascend Access Control, including Windows NT 4.0. Although you can install Ascend Access Control on a machine running SunOS 4.1.4, there are no INTERSOLV drivers, as yet, for that OS. The table is current as of February 1997. If you have questions about INTERSOLV drivers call an INTERSOLV distributor or visit INTERSOLV's World Wide Web site. Currently, the INTERSOLV address is

`http://www.intersolv.com.`

Table 7-1. INTERSOLV supported DBMS's and platforms. "All" includes AIX 4.1, HP-UX 10.x and 9.x, Solaris 2.5 for SPARC and x.86 machines, and Windows NT 4.0

DBMS	Platforms
Btrieve 5, 6.x	Win NT
Clipper	All
DB2/2, DB2/NT, DB2/UNIX	AIX 4.1, Win NT
DB2 for MVS	AIX 4.1
DB2 for OS/400	AIX 4.1
dbase III, IV, and V files	All
Excel	Win NT
FoxBASE FoxPro	All
FoxPro3.0	Win NT
Gupta SQL Base	Win NT
INFORMIX	All but Solaris x.86 and HP-UX 10.x, 9.x
Ingres	Solaris SPARC
Open Ingres 1.2	Win NT, Solaris SPARC
Oracle	All
Paradox	Win NT

Table 7-1. INTERSOLV supported DBMS's and platforms. "All" includes AIX 4.1, HP-UX 10.x and 9.x, Solaris 2.5 for SPARC and x.86 machines, and Windows NT 4.0

DBMS	Platforms
PROGRESS	Call INTERSOLV for availability
MS SQL Server 6	Win NT
Sybase SQL Server 4.9	All
Sybase System 10, 11	All
Text files	All

Installing and configuring your DBMS

You must install a DBMS and create a database and its tables before you can edit initialization files and configure drivers that enable Ascend Access Control to utilize ODBC DBMS servers and tables. The ODBC initialization file and driver configuration tools must be given the names of the database and tables that will contain authentication and accounting information. The Ascend Access Control User Guide does not contain instructions for performing these tasks, but you should log on as the *System Administrator* for the server where you will create the ODBC database and tables. If you log on as a user named *John* to create a database named *AccessControl* you may find that you must refer to the database as `John.AccessControl` when you edit the initialization file and configure your DBMS driver.

Creating the accounting table

You can use the SQL script in this section to create the accounting table. The table must contain all the fields listed in the script because each field matches a RADIUS attribute that the NAS sends the Ascend Access Control server. The server then forwards the NAS accounting information to the DBMS *AccessControl* database accounting table. You will receive an error if Ascend Access Control sends the accounting table an attribute that is not represented by an accounting table field.

The accounting table receives the same information the server sends to its `Details` file. This file is not superseded by the table. Both receive the accounting information, so their field names and attribute names must match, although the hyphens in the attribute names become underscores in the table's field names. These examples illustrate the proper substitution of underscores for hyphens when you create the accounting table:

Attribute Name	**Field Name**
`Acct-Authentic`	`Acct_Authentic`
`Acct-Delay-Time`	`Acct_Delay_Time`

You can use the Ascend Access Control attribute names as the accounting table's field names, or map new field names to the attribute names. "Mapping attribute names to database field names" on page 7-17 describes way to link different attribute and field names.

Following is the SQL script for creating the accounting table. The table that follows the script describes each attribute that can appear in an accounting packet sent by the NAS to Ascend Access Control.

```
create table Accounting(
    Acct_Authentic varchar (8) NULL,
    Acct_Delay_Time varchar (8) NULL,
    Acct_Input_Octets varchar (16) NULL,
    Acct_Input_Packets varchar (16) NULL,
    Acct_Link_Count int NULL,
    Acct_Multi_Session_Id varchar(20) NULL,
    Acct_Output_Octets varchar (16) NULL,
    Acct_Output_Packets varchar (16) NULL,
    Acct_Session_Id varchar (10) unique,
    Acct_Session_Time varchar (11) NULL,
    Acct_Status_Type varchar (14) NULL,
    Acct_Terminate_Cause int NULL,
```

```
Ascend_Connect_Progress varchar (3) NULL,
Ascend_Data_Rate varchar (20) NULL,
Ascend_Dial_Number varchar(20) NULL,
Ascend_Disconnect_Cause varchar (3) NULL,
Ascend_Event_Type int NULL,
Ascend_First_Dest varchar (15) NULL,
Ascend_Multilink_ID varchar (3) NULL,
Ascend_Num_In_Multilink varchar (10) NULL,
Ascend_Number_Sessions varchar(5) NULL,
Ascend_Pre_Input_Octets varchar (5) NULL,
Ascend_Pre_Input_Packets varchar (5) NULL,
Ascend_Pre_Output_Octets varchar (5) NULL,
Ascend_Pre_Output_Packets varchar (5) NULL,
Ascend_PreSession_Time varchar (5) NULL,
Ascend_Session_Svr_Key varchar(20) NULL,
Ascend_User_Acct_Base int NULL,
Ascend_User_Acct_Host int NULL,
Ascend_User_Acct_Key int NULL,
Ascend_User_Acct_Port int NULL,
Ascend_User_Acct_Time int NULL,
Ascend_User_Acct_Type int NULL,
Called_Station_Id varchar (10) NULL,
Calling_Station_Id varchar(20) NULL,
Class varchar(20) NULL,
Framed_IP_Address varchar (15) NULL,
Framed_IP_Netmask varchar (15) NULL,
Framed_IPX_Network varchar (30) NULL,
Framed_Protocol varchar (6) NULL,
NAS_Identifier varchar (15) NULL,
NAS_IP_Address varchar (15) NULL,
```

```
    NAS_Port varchar (5) NULL,
    Proxy_State varchar(20) NULL,
    Service_Type int NULL,
    Start_Time varchar (30) NULL,
    Stop_Time varchar (25) NULL,
    User_Id varchar (10) NULL,
    User_Name varchar (20) NULL,
    User_Realm varchar (20) NULL
)
```

Table 7-2. Attributes the NAS can send in accounting packets.

Attribute Name	Description
Acct-Authentic	Indicates how the client authenticates an incoming call: RADIUS (1) specifies RADIUS authenticates. Local (2) specifies authentication via a local Connection profile, TACACS profile, or TACACS+ profile, or no authentication.
Acct-Delay-Time	Specifies the number of seconds between the time an event occurred and the time the client sent the packet. If RADIUS does not acknowledge the packet, the client resends it and the value of Acct-Delay-Time changes to reflect the proper event time.
Acct-Input-Octets	Indicates the number of octets the client received during the session.
Acct-Input-packets	Indicates the number of packets the client received during the session.
Acct-Output-Octets	Indicates the number of octets the client sent during the session.
Acct-Output-packets	Indicates the number of packets the client sent during the session.
Acct-Session-Id	A unique numeric string between 1 and 2,137,383,647 identifying the bridging, routing, or terminal server session reported in the Accounting packet that RADIUS uses to correlate Start and Stop packets.
Acct-Session-Time	Specifies the number of seconds the session has been logged in.
Acct-Status-Type	Identifies Start and Stop packets. Stop can indicate a Stop packet or a Failure packet.
Ascend-Connect-Progress	Indicates the state of the connection before it disconnects.
Ascend-Data-Rate	Indicates the data rate of the connection in bits per second.
Ascend-Dial-Number	Specifies the phone number of the device that originated the connection.

Table 7-2. Attributes the NAS can send in accounting packets.

Attribute Name	Description
Ascend-Disconnect-Cause	Specifies the reason a connection was taken off-line.
Ascend-Event-Type	Indicates a coldstart notification, informing the accounting server that the client has started up.
Ascend-First-Dest	Records the destination IP address of the first packet the client received on a connection after authentication.
Ascend-Multilink-ID	Reports the ID number of the Multilink bundle when the session closes.
Ascend-Num-In-Multilink	Records the number of sessions remaining in a Multilink bundle when the session closes.
Ascend-Number-Sessions	Specifies the number of active user sessions of a given class (as specified by the Class attribute). In the case of multichannel calls, such as MP+ calls, each separate connection counts as a session.
Ascend-Pre-Input-Octets	Records the number of octets the client received before authentication.
Ascend-Pre-Input-packets	Records the number of packets the client received before authentication.
Ascend-Pre-Output-Octets	Records the number of octets the client sent before authentication.
Ascend-Pre-Output-packets	Records the number of packets the client sent before authentication.
Ascend-PreSession-Time	Indicates the length of time in seconds from when a call connected to when it completed authentication.
Ascend-Session-Svr-Key	Identifies the user session in which a client sends a disconnect or filter change request to the RADIUS server.

Table 7-2. Attributes the NAS can send in accounting packets.

Attribute Name	Description
Ascend-User-Acct-Base	Specifies whether the numeric base of the RADIUS Acct-Session-ID attribute is 10 or 16.
Ascend-User-Acct-Host	Specifies the IP address of the RADIUS server to use for this connection.
Ascend-User-Acct-Key	Specifies the RADIUS client password as it appears in the clients file.
Ascend-User-Acct-Port	Specifies a UDP port number for the connection.
Ascend-User-Acct-Time	Specifies the number of seconds the client waits for a response to a RADIUS accounting request.
Ascend-User-Acct-Type	Specifies the RADIUS accounting server(s) to use for this connection.
Called-Station-Id	Specifies the called number, indicating the phone number the user dialed to connect to the client.
Calling-Station-Id	Specifies the calling-party number, indicating the phone number of the user that has connected to the client.
Class	Enables access providers to classify their user sessions, such as for the purpose of billing users depending on the service option they choose. The default value for the Class attribute is null.
Framed-IP-Address	Specifies the IP address of the user starting the session. The default value is 0.0.0.0.
Framed-IPX-Network	Specifies the network number of the router at the remote end of the connection. The default value is null.

Table 7-2. Attributes the NAS can send in accounting packets.

Attribute Name	Description
Framed-Protocol	Specifies the kind of protocol the connection uses: PPP (1) SLIP (2) MPP (256) EURAW (257) EUUI (258) COMB (260) FR (261) ARA (262) FR-CIR (263). By default, the client does not restrict the type of protocol a user can access.
NAS-IP-Address	IP address of the Network Access Server, or client. This attribute does not appear in an Accounting-Stop packet for a Failure-start-session event.
NAS-Port	Indicates the interface and service the session is using with a 5-digit value in this format: <service> <line number> <channel> This attribute does not appear in an Accounting-Stop packet for a Failure-start-session event.
Service-Type	This attribute specifies the type of services the link uses.
Start-Time	Specifies the time Ascend Access Control received an Accounting-Start packet.
Stop-Time	Specifies the time Ascend Access Control received an Accounting-Stop packet.

Table 7-2. Attributes the NAS can send in accounting packets.

Attribute Name	Description
User-Id	Specifies the name of the user. Appears before the separator in the User-Name when the format is *user@realm*.
User-Name	Specifies the name of the user starting the session. Includes both the User-ID and the User-Realm.
User-Realm	Specifies the name of the user's realm. Appears after the separator in the User-Name when the format is *user@realm*.

Creating an index for the accounting table

You can create a table index by selecting a table field that is unique in every record. We recommend that you select the field, or column, called Session-ID to create the accounting table index. The syntax of a script for creating an index for a table is:

```
create index  <index_mname> on <table_name> (<column_name>)
```

Following is a script that uses Session-ID to create an accounting table index:

```
create index joesindex on Accounting (Session_ID)
```

By creating this index, the ODBC driver doesn't have to create an index before it tries to locate the proper records. This saves time and could save some space in the DBMS *tempdb* database.

Mapping attribute names to database field names

If you choose to create column headings in your database table that are different than the names of Ascend Access Control attributes, you must map the names you create to the attribute names. A file named `radodbc.map` provides the mapping facility. This file is installed in the Ascend Access Control data directory, or should be moved to the same directory in which you placed the Ascend Access Control `dictionary` file.

Caution: Be careful when using the `radodbc.map` file to map Ascend Access Control attribute names to names of table column headings. Ascend Access Control will use either the `dictionary` file or `radodbc.map` as its database of legitimate attributes for authentication and accounting. It will not use both, checking the `dictionary` file for attribute names it cannot find in `radodbc.map`. If you map attribute names to column heading names `radodbc.map` must contain all of the authentication and accounting attributes that you will enter in user profiles or capture in accounting messages. Remember that you cannot instruct the NAS to send only specific accounting attributes to the accounting table. The NAS determines which accounting attributes it places in accounting messages it sends. Table 7-2 includes all the accounting attributes you must place in `radodbc.map` if you map attribute names to column heading names.

The Ascend Access Control attribute name and table column name that you want to map to one another must appear on one line in the `radodbc.map` file. The file's format is:

```
Access_Control_attribute name   ODBC_Column name
User-Name                       Uname
Password                        Secret
```

Configuring Ascend Access Control for ODBC

To make Ascend Access Control and a DBMS work together you must install and configure Ascend Access Control, the ODBC Driver Manager and drivers, the DBMS client and the DBMS tables. Following describes the steps for configuring Ascend Access Control to use ODBC DBMS tables. Specific information about completing the steps begins in the section "ODBC libraries and initialization files" on page 7-20.

To install and configure Ascend Access Control to use ODBC DBMS for authentication and accounting:

1 On UNIX systems, set environment variables for the ODBC libraries and the ODBC initialization file. These variables specify the locations of the libraries and the initialization file so the RADIUS daemon can find the libraries and the Driver Manager can find the drivers.

Note: Step 1 may not be necessary on Windows NT 4.0 systems. See the explanation in "ODBC libraries and initialization files" on page 7-20.

2 Edit the ODBC initialization file so that it includes all the ODBC data sources, database names, server names, and LogonIDs. The file is usually named `.odbc.ini` on UNIX operating systems. On Windows NT 4.0 machines you can edit a file called `odbc.ini` by selecting the ODBC icon in the Control Panel.

3 Add to the `users` file all the necessary user profiles to point Ascend Access Control toward the DBMS when an Access-Request packet is sent to authenticate a user. The DEFAULT user profile may be used to indicate that user profiles for all authentication requests are in a DBMS table. (See "users file profiles that point to DBMS tables" on page 7-24).

   Add a user profile called ODBCACCT to the `users` file if you want to send accounting information to a database table. (The user profile name ODBCACCT is reserved for this purpose. See "users file profiles that point to DBMS tables" on page 7-24).

4 Install and configure the DBMS client to work with the ODBC drivers. Review the DBMS client documentation for instructions.

5 Create an authentication table in the DBMS. You must also create an accounting table if you turn on RADIUS accounting.

6 Create fields in each table you create. Each attribute that you will enter or capture in a table becomes a table column and each user or accounting record is a table row.

   The Ascend Access Control User Guide's appendix contains scripts you can use to create authentication tables for an ODBC DBMS.

7 (Optional) Edit a file named `radodbc.map,` which maps the names of Ascend Access Control attributes to field names you develop for the DBMS authentication tables.

   Note: If you edit `radodbc.map` to map attribute names to field names, you must include in the file all of the authentication and accounting attributes that you will enter or capture in any of your user authentication or accounting records. "Mapping attribute names to database field names" on page 7-17 explains the function of the `radodbc.map` file.

ODBC libraries and initialization files

The Ascend Access Control daemon requires a number of libraries to support ODBC. If you install Ascend access Control on a UNIX machine you must specify the path to the libraries and the location of the initialization file called ODBC_INI. You do this by setting environment variables as explained in the section “Setting UNIX environment variables.”

When you install Ascend Access Control on a Windows NT 4.0 system you do not have to define the path to the Driver Manager or the ODBC if they have been installed in the default directory, which is probably the SYSTEM or SYSTEM32 directory. If you install them in another directory you might need to list that directory in your path command.

Setting UNIX environment variables

By default, ODBC libraries are placed in the directory `/opt/odbc/dlls` when Ascend Access Control is installed on a UNIX system and you must inform `radiusd` of the fully qualified path to the libraries. The examples below, for UNIX machines running Bourne and C shells, include `LD_LIBRARY_PATH`, the name of the Solaris environment variable. The variable’s name on AIX systems is LIBPATH and on HP-UX it is SHLIB_PATH.

Bourne shell:

```
LD_LIBRARY_PATH=/opt/odbc/dlls; export LD_LIBRARY_PATH
```

C-shell:

```
setenv LD_LIBRARY_PATH /opt/odbc/dlls
```

The Driver Manager built into the Ascend Access Control daemon needs to know where to find the driver for your DBMS. This information is kept in a plain text file called `.odbc.ini`. An example `.odbc.ini` file is installed with Ascend Access Control.

By default, the ODBC Manager looks for `.odbc.ini` in the home directory of the user who starts `radiusd`. If you change the name of `.odbc.ini` or its location on the Ascend Access Control machine, you must set the ODBC_INI environment variable so the ODBC Manager can locate the file. The following

examples show how to set the environment variable to indicate that you have placed `.odbc.ini` somewhere other than the default location.

Bourne shell:

```
ODBC_INI=/opt/odbc/odbc.ini; export ODBC_INI
```

C-shell:

```
setenv ODBC_INI /opt/odbc/odbc.ini
```

Editing the .odbc.ini and odbc.ini files

The ODBC initialization file contains information about all the odbc drivers installed on the Ascend Access Control server machine. The names of the UNIX and Windows NT 4.0 files are similar, but not exactly the same. The UNIX file begins with a period and the Windows NT 4.0 does not. The file entries are also slightly different, but contain the same kinds of information, including the name of the driver, the name of the driver's object library or distributed library, and the name of the DBMS server with which the driver communicates.

An example `.odbc.ini` file is copied to the default location when you install Ascend Access Control on UNIX machines. You must edit the example `.odbc.ini` with a text editor, such as vi, to specify the entries each driver. An `odbc.ini` file is installed with the Windows NT 4.0 operating system and you can edit entries for the drivers you install on the machine by selecting the ODBC icon on the Windows NT 4.0 Control panel.

.odbc.ini format

Following is the format of the `.odbc.ini` file on a UNIX machine. The format of the Windows NT 4.0 file is similar. Comments which describe the entries are preceded by a semi-colon, such as "; lists data sources available to ODBC" which follows "[ODBC Data Sources]" on the first line. The format of the Windows NT 4.0 file is similar. Periods between entries indicate that intervening entries have been left out.

```
[ODBC Data Sources]  ; lists data sources available to ODBC
ds_name1=driver_desc1; lists each data source name followed
```

```
                    ; by a description
ds_name2=driver_desc2
...
[ds_name1]          ; defines the actual ODBC driver source
                    ; example: Oracle
Driver=path/dll     ; defines the path to the driver dll
Description=desc    ;briefly describes the Data Source
...
[ds_name2]
Driver=path/dll
Description=desc
```

Example of UNIX .odbc.ini file

Following is an example of an `.odbc.ini` file on a UNIX machine. UNIX drivers have the following characteristics:

- File names are lowercase
- The prefix for all file names is `qe`
- The extension for file names is `.so` or `.sl,` representing *shared object* or *shared library.*

```
[ODBC Data Sources]
qess=SQLServer
qedbf=dBase
qeor7=Oracle

[qess]
Driver=qess07.so
Description=INTERSOLV SQL server driver
ServerName=alice
LogonID=sysadmin
```

Example of Windows NT 4.0 odbc.ini file

Following is an example of an `odbc.ini` file on a Windows NT 4.0 machine.Windows NT 4.0 drivers have the following characteristics:

- File names are uppercase
- The prefix for all file names is `qe`
- The extension for file names is `.dll,` for distributed linked library.

```
[ODBC Data Sources]
MS Access Databases=Access Data (*.mdb)
FoxPro Files=FoxPro Files (*.dbf)
dBase Files=dBase Files (*.dbf)
Paradox Files=Paradox Files (*.db )
NWind=dBase Files (*.dbf)
[MS Access Databases]
Driver=C:\WINNT\SYSTEM\SIMBA.DLL
FileType=RedISAM
SingleUser=False
UseSystemDB=False
[FoxPro Files]
Driver=C:\WINNT\SYSTEM\SIMBA.DLL
FileType=FoxPro 2.5
SingleUser=False
[dBase Files]
Driver=C:\WINNT\SYSTEM\SIMBA.DLL
FileType=dBase4
SingleUser=False
```

users file profiles that point to DBMS tables

Ascend Access Control always begins authentication by searching a `users` file, so you must enter at least one user profile in a `users` file when you store profiles in DBMS tables to tell Ascend Access Control that the requested user profile is in an ODBC DBMS. The necessary information is provided by the values in a user profile's Authentication-Type and Password attributes. If the value of the profile's Authentication-Type attribute is the string *`ODBC`* it is a flag indicating that Ascend Access Control should contact an ODBC DBMS to authenticate users. The value of the Password attribute provides the location of the DBMS data source. (For more information, seeTable 7-3.)

Profiles for Authentication

You can enter the required Authentication-Type and Password values that direct Ascend Access Control to contact a DBMS table in an individual's user profile or a DEFAULT user profile. A DEFAULT profile matches any user that does not have a profile in the `users` file. If a DEFAULT profile that points to a DBMS table is is the only entry in the `users` file, Ascend Access Control connects with a DBMS table to answer all authentication requests. Place the DEFAULT user profile at the end of the `users` file if you want to create user profiles in the `users` file for special users. Ascend Access Control will match the users to their profiles before encountering the DEFAULT profile and authenticate the special users with the check-items in their profiles in the `users` file, rather than with information from the database table.

Profile for accounting

If you turn on RADUS accounting and want to store accounting information in a DBMS table you must place a user profile called ODBCACCT in the `users` file. The profile name ODBCACCT is reserved and can only be used as the link between Ascend Access Control and a table that receives connection accounting information from the NAS. When you place ODBCACCT in the users file all RADIUS accounting information will be stored in table specified by the ODBCACCT profile's attribute values.

Creating the user profiles

All user profiles that point Ascend Access Control to an ODBC DBMS table must contain the Username, Authentication-Type and Password attributes. The values of the Username and Password attributes specify who the user is and where the table is located. You can enter reply-items in individual profiles that override those you enter in the table entry. Following is an example that shows the format of a profile that contains the required attributes:

username `Authentication-Type=ODBC Password="`*`database source name:database table name:table access name/table access password`*`"`

Note: The entire entry for the Password value must be enclosed in quotation marks. Table 7-3 contains descriptions of the components of the Password attribute value.

Caution: The Password attribute in the example wraps because of the Ascend Access Control User Guide's margins. The line of a user profile can only wrap to the next line because it is too long to fit on one line. Do not manually break the line by entering a line break or carriage return.

Table 7-3. Components of the Password attribute value.

Value	Description
`database source name`	The database source name indicates which ODBC DBMS server to consult.
`database table name`	The DBMS table name indicates which DBMS table to access. You can specify a unique name for each table which contains user name entries belonging to a realm. Ascend Access Control uses the realm name within the user name to query the respective table.
`table access name`	The table access name is the name Ascend Access Control uses to access a specific DBMS table. Each DBMS table must have a different table access name.

Table 7-3. Components of the Password attribute value.

Value	Description
`table access password`	The table access password is the password Ascend Access Control provides to access a specific DBMS table. Each DBMS table must have a different table access password.

Following are examples of a DEFAULT and an ODBCACCT user profile. The DEFAULT profile causes all users to be authenticated and authorized by information in a Sybase table called *RAD-Users*. The ODBCACCT profile sends all NAS accounting information to a Sybase table called *Accounting*.

```
DEFAULT Authentication-Type=ODBC Password=”qesyb:RAD-
Users:radius/radius”

ODBCACCT Authentication-Type=ODBC
Password=”qesyb:Accounting:radius/radius”
```

Installing a Sybase client

You must install a copy of your DBMS’s client software on the Ascend Access Control server machine because the driver uses the client software’s libraries to communicate with the DBMS server, even if Ascend Access Control and the DBMS are on the same machine. Each DBMS client will require different installation and configuration steps to enable the client to locate and communicate with the DBMS server. For example, to install a Sybase client on a UNIX machine you might be required to perform the following commands to set additional environment variables:

```
SYBASE=/n/hump/6/sybase; export SYBASE

LD_LIBRARY_PATH=${LD_LIBRARY_PATH}:/n/hump/6/sybase/lib

export LD_LIBRARY_PATH
```

Example Sybase client installation for Windows NT 4.0

This section, and those that follow, describe the steps you take to install and configure a Sybase client on a Windows NT 4.0 machine.The procedures for installing your DBMS client application might be similar to those explained here, but you will have to consult the your DBMS documentation to complete the installation and configuration of your client software. The Ascend Access Control User Guide cannot document procedures for all the ODBC-compliant DBMSs and other DBMS vendors might supply proprietary utilities and interfaces that require different information than appears in this Sybase example.

Following explains how to install the Sybase client on the Ascend Access Control server. “Configuring a Sybase client connection for accounting” on page 7-27 explains how to configure a connection between the Sybase client accounting table and the client on the ascend Access Control server.

To install Sybase client software from a zipped file on the Ascend Access Control server:

1. Copy the zipped Sybase client file into an empty directory on the Ascend Access Control server.
2. Extract the compressed files in the zipped file to the directory in which you placed the zipped file.
3. Run `setup.exe` from the Windows NT 4.0’s `Start>Run` textbox or double click `setup.exe` in Windows NT Explorer.

Configuring a Sybase client connection for accounting

You must use a Sybase utility called *SQLEdit* to configure the Sybase client/server connection. The utility is included with the Sybase DBMS. The client software uses TCP/IP Sockets to communicate with the DBMS server. You r client and DBMS server might use a different method to communicate, such as named pipes, multiprotocol or Banyon Vines. This example creates a client link to a server named *Sybase.* The information that is required for the example includes the server’s:

- IP address
- Name

- Port
- TCP/IP driver

Your DBMS documentation should provide the TCP/IP driver and Port information and you can get the server's IP address by using the `hostname` and `nslookup` commands.

Note: The name you enter for the server must be the same name you supply when configuring the ODBC driver.

The procedures in the example might not resemble the way you configure your own DBMS client. However, you must, in some way, configure the method of communication that the client and DBMS server will use and provide the port number on which the server listens for messages from its client. Table 7-4 displays the SQLEdit screen in which you enter the information listed in steps 2 through 7 of the example.

1 Open *SQLEdit*.

2 Enter `Sybase` in *Input Server Name*.

3 Click *Add*.

4 Select *Query* from *Service Type.*

5 Select *NT* from *Platform.*

6 Select *NLWNSCK* from *Net-Library Driver.*

7 Enter `192.0.0.1,7200` in *Connection Information/Network Address*.
Do not enter a space between the comma and the port number.

8 Click *Ping*.
`Ping` enables you to see if the Ascend Access Control server can find the DBMS server. If `Ping` succeeds you receive a message that the connection opens and closes and that the `NLWNSCK.DLL` dynamic link library loads.

Figure 7-4. SQLEdit screen for configuring a client on Windows NT 4.0 .

Assigning the Sybase driver's Data Source

The supplier of the Sybase driver will determine the method you must use to install the driver. Table 7-4 includes the information you must provide to assign the Sybase driver's Data source. The specific information listed here comes from the entries used in the example in "Configuring a Sybase client connection for accounting."

The information you supply for the driver corresponds with the information that you enter as the value of the Password attribute in the user profiles that tell Ascend Access Control to contact a DBMS to find authentication and accounting tables (See"users file profiles that point to DBMS tables" on page 7-24).

Table 7-4. Data Source information required by the driver.

Type of information	Example
Driver name	*ray-odbc.* This driver name is a combination of a server's name, *ray*, and the type of driver, *odbc*. You can create names for your own drivers.
DBMS server name	*SYBASE*
Database name	*AccessControl*
Database table name	*Accounting*
User LogonID	*spud.* The name that must be supplied to access the table.
User password	*dups.* The password that must be supplied to access the table.

After installing the driver on a Windows NT 4.0 machine, you must use the system's Data Source Administrator GUI to define the driver's data source. The Data Source Administrator GUI may appear as you install the driver. If it does not, open it from the Control Panel. Following are the steps for assigning the driver a data source.

1 Open the Windows NT Control Panel and click the *ODBC 32* icon.

2 Select the *System DSN* tab (Figure 7-5).

Do not select the *User DSN* tab because Ascend Access Control is a system service, not a user application.

3 Select a Data Source or click *Add* to create a new one.

4 Select a driver from the list of installed drivers.

Beyond this point, the GUI displays dialogs based on the driver you selected.

5 Enter information from Table 7-4 to identify the driver's data source.

Figure 7-5. ODBC Data Source Administrator dialog box.

Figure 7-6. List of ODBC drivers installed on the system.

Ascend Access Control files and commands

A

This chapter contains information about the Ascend Access Control files, commands and command options. The information is derived from the original UNIX manual pages.

authfile(5)

Name

`authfile` - Ascend Access Control file for mapping realms and authentication types

Synopsis

UNIX

`/etc/raddb/authfile`

Windows NT 4.0

`c:\Ascend\Access_Control\database\authfile`

Description

The `authfile` file is installed in the Ascend Access Control server's default directory, unless configured differently by the system administrator. `authfile` is read by `radiusd` at startup and whenever `radiusd` receives a `HUP` signal (UNIX) or the server is refreshed (Windows NT 4.0).

You can use the Access Control Manager's Edit Realms screen or a text editor to maintain the `authfile` file.

`authfile` contains a list of the names of all the realms to which users seeking authentication may belong. Ascend Access Control refers to the list of realms in `authfile` when authenticating incoming requests from anyone offering the *user@realm* pattern as a match for the Ascend Access Control User-Name attribute.

`authfile` may contain comments, which are indicated by leading pound sign (#) character. Comments and blank lines inserted in `authfile` are ignored.

`authfile` contains one line of information per realm entry. Each entry may include several, white-space delimited fields. Two fields, Realm-name and Type

must appear in the entry. Other fields are dependent on entries in the required fields. See the section on the Type field for more information.

The syntax for an `authfile` entry is:

```
Realm-name [(Alias [, Alias])] [-Protocol] Type [Realm/DNS/
File]
```

Example:

```
Realm-name [(Alias)] [-Protocol] Type [Realm/DNS/File]
umich.edu (wolverine) -pw AFS-KRB UMICH.EDU
ohio.org (buckeye, bucks) file buckeye
```

Realm-name field

A Realm-name entry may be any appropriate symbol or name. Note that it is highly recommended that the entry be a Domain Name System hostname when appropriate, because that would benefit users who are already familiar with the *user@realm* syntax through the use of email addresses.

DEFAULT

A single Realm-name entry of DEFAULT may be placed at the end of the `authfile`. The field entries for the DEFAULT realm indicate how Ascend Access Control should handle authentication requests that include Realm-name entries that are not found in `authfile`. DEFAULT usually includes Type and Realm/DNS/File entries for a remote server. Access-requests for DEFAULT entries are sent to the remote server, which authenticates the user and sends reply-item attributes back to the local server.

NULL

The NULL Realm-name entry is used to indicate to Ascend Access Control how it should handle user names that appear as *user* instead of *user@realm*.

Wild Card

The wild card syntax is `*.realm.` Wild card syntax allows you to indicate several related realms which are to be handled by one authentication Type entry

in the `authfile`. For example, a company may have several branches, including `east.foo`, `west.foo` and `south.foo`. The entry `*.foo` matches all three realms. It is highly recommended that wild card entries be listed toward the middle of the `authfile` so entries for specific realms, like `east.foo` will be matched before the wild card entry like `*.foo`.

Alias (option)

Alias entries are optional, comma-separated names which can be attached to the user name in lieu of the actual realm name. For example, if the Realm- name is `foobar` and its aliases are `foo` and `bar` the user could enter `jsmith@foobar`, `jsmith@foo`, or `jsmith@bar` to match the Realm-name. Aliases are allowed for wild card entries and are interpreted as `*.alias` rather than `alias.realm` or just `alias`.

-Protocol (option)

-Protocol is an optional indicator that identifies the authentication protocol which applies to the realm. The three allowable entries in the -Protocol option are `-PW`, `-CHAP` and `-DFLT`. These entries are searched in order, so you may distinguish between or among otherwise identical realm entries. `-PW` and `-CHAP` stand for *Password* and *Challenge Handshake Authentication Protocol*. By default an entry applies to both Password and CHAP, but using either of the `-PW` or `-CHAP` options limits the entry to that specific protocol.

Type field

Valid authentication types include `PASSWD, UNIX-PW, RADIUS, MIT-KRB, AFS-KRB, FILE, TACACS,` and `TACPLUS.` These authentication types are case insensitive.

PASSWD and UNIX-PW

Either of these entries refers to authenticating a user by comparing his entry to his password in the UNIX password file.

RADIUS

The entry RADIUS indicates authentication is done by a remote Ascend Access Control server. The remote server sends reply-items, or authorization attribute/value pairs, back to its client, the local Ascend Access Control server. The local Ascend Access Control server then sends the reply-items to the NAS that originally sent the Ascend Access Control Access-Request packet. A Ascend Access Control Type entry requires a Realm/DNS/File field entry. See Realm/DNS/File below.

MIT-KRB, AFS-KRB

Either of these Type entries indicates that kerberos authentication is done at the default kerberos realm. Note that the file named `krb.conf` on your system must have valid entries for the realm. Kerberos entries require an entry in the Realm/DNS/File field. See Realm/DNS/File below.

File

The File entry indicates that Ascend Access Control uses a flat file lookup, searching for encrypted passwords in the `users` file. A Type field entry of File requires a Realm/DNS/File field entry. See Realm/DNS/File below.

TACACS, TACPLUS

A TACACS or TACPLUS keyword entry in the Type field indicates that authentication is done by encrypted request to a TACACS or TACACS+ server. A TACACS or TACPLUS Type entry requires a Realm/DNS/File field entry. See Realm/DNS/File below.

ARA-DES

An ARA-DES entry requires that the Framed-Protocol entry is Ascend-ARA and this encryption must be performed by an Ascend Access Control server in direct communication with the NAS. It may not be performed via proxy authentication.

ACE

An ACE keyword in the Type field means that authentication involves an ACE server and a hand held SecureID device.

DEFENDER

This is similar to the ACE keyword. DEFENDER indicates that the user is authenticated by an AssureNet Defender server and SecureNet Key.

SKEY

This entry indicates that the user authenticates with a one time password method developed by Bellcore.

ODBC

This entry is half of the notice to Ascend Access Control that the user's profile in stored in a DBMS table. It requires that the Password attribute value include information about the data source. The data source is the ODBC-compliant DBMS and the table. The Password value also contain the access password shared by the DBMS and the Ascend Access Control server.

realm/DNS/file field

Entries in the Realm/DNS/File field are determined by the keyword entered in the Type field.

Table A-1. `Type` field and realm/DNS/file entry relationships

type Keywords	realm/DNS/file entries
AFS-KRB, MIT-KRB	Kerberos realm name
FILE	Prefix for the realm's `users` file in the syntax `prefix.users`. For example, the entry ***`flatland`*** indicates the user profiles for the realm are in the file `flatland.users` **Note:** Do not include a period at the end of the entry. See"Understanding the clients file" on page 4-28.

Table A-1. `Type` field and realm/DNS/file entry relationships

type Keywords	realm/DNS/file entries
RADIUS	DNS for remote Ascend Access Control server
TACACS, TACPLUS	DNS for the appropriate TACACS or TACACS+ server
ACE	DNS for the appropriate ACE server
DEFENDER	DNS for the appropriate DEFENDER server

Files

`krb.conf, authfile, dictionary, users`

See Also

dictionary(5), users(5), radiusd(8)

clients(5)

Name

`clients` - Ascend Access Control file for mapping clients to shared-secrets

Synopsis

UNIX

`/etc/raddb/clients`

Windows NT 4.0

`c:\Ascend\Access_Control\database\clients`

Description

The `clients` file is installed in the Ascend Access Control server's default directory, unless configured differently by the system administrator. `clients` is read by `radiusd` at startup and whenever `radiusd` receives a `HUP` signal (UNIX) or the server is refreshed (Windows NT 4.0)..

You can use the Access Control Manager's Edit Clients screen or a text editor to maintain the `clients` file.

`clients` contains a list of Ascend Access Control's clients, such as Network Access Servers (NAS) or other RADIUS servers.

`clients` may contain comments, which are indicated by leading pound sign(#) character. Comments and blank lines inserted in `clients` are ignored.

`clients` contains one line of information per Ascend Access Control client entry. Each line may include up to five white-space delimited fields. The first two fields, System-name[:port] and Key must appear in the entry. The other three fields are optional.

The syntax for a `clients` entry is:

```
System-name[:port] Key Type Version Prefix
```

Example:

```
System-name[:port] Key      Type     Version Prefix

merit.edu:7       badges0  type=nas  v2      pfx

10.1.2.3:256       test    type=nas  v2      pm1
```

System-name[:port} field

This entry may be a valid Domain Name System hostname or an IP address in dotted-quad notation. The entry may also be followed by a colon (:) and a UDP/TCP port number on the client or server. The System-name port number option overrides the default port numbers 1645 and 1646, or the ports defined by the `radiusd` `-pp` or `-qq` options. These ports define the Ascend Access Control and Ascend Access Control accounting ports, respectively. If you use the System-name port number option, the port number you enter should be for the Ascend Access Control port because the accounting port is assumed to be one greater than the number entered as the option.

A pair of Ascend Access Control clients or servers may be specified using the alternate System-name notation `name1/name2:`

```
Italia/Italy bgmsbkym type=nas
```

The alternate notation allows the same `clients` file to be distributed to physically different Ascend Access Control servers that have been identically configured. A request from a Ascend Access Control machine only matches this alternate notation if the packet's source IP address matches the IP address of `name1` or `name2` and the hostname of this server, as returned by the hostname command, matches `name1` or `name2`. You must not use the port number option if you use the alternate `name1/name2` notation.

Key field

The Key field is the encryption key or shared secret known by a Ascend Access Control server and a client, or by Ascend Access Control and another RADIUS server. The secret field may be sixteen (16) characters long.

Type field (option)

The optional Type field specifies the client's vendor name and/or the type of the Ascend Access Control machine sending requests to this server. If the Type field is omitted, the client type and vendor name are unspecified. Note that this may be vitally important, since the Ascend Access Control server only honors a vendor-specific attribute if the vendor's name is in the Type field of the associated `clients` file entry. Currently, Ascend Access Control recognizes three values for the Type field:

- NAS
- PROXY
- ASCEND

Version field (option)

The optional Version field specifies the Ascend Access Control version number. If this is omitted, it defaults to version one. Version one is described in the IETF RADIUS standard document. Version two is described in the IETF document titled `draft-calhoun-enh-radius-00.txt`. Currently, `v1`, `v2` and `v3` are allowed as values in the Version field.

Prefix field (option)

The Prefix field value is a text string. When you enter a string in Prefix field Ascend Access Control can only search for the client's realms in a specific `authfile`. The value of the Prefix field is added to the beginning of `authfile` to create the file's name. If the value of the Prefix field is `ascend` the file that Ascend Access Control will search is named `ascendauthfile`. If you have entered the client's list of realms in an `authfile` named `ascend.authfile` you must you must add a period at the end of the Prefix field entry so `ascend.` is the field's value. "Clients file format" on page 4-29 contains a discussion of the differences between entries in the `clients` file Prefix field and the `authfile`'s Real/DNS/File field. Both fields are used to create prefixes for file names.

Files

```
authfile, clients, users
```

See Also

authfile(5), users(5), vendors(5), radiusd(8)

dictionary(5)

Name

`dictionary` - translations for parsing Ascend Access Control requests

Synopsis

UNIX

`/etc/raddb/dictionary`

Windows NT 4.0

`c:\Ascend\Access_Control\database\dictionary`

Description

The `dictionary` file is installed in the Ascend Access Control server's default directory, unless configured differently by the system administrator. `dictionary` is read by `radiusd` at startup and whenever `radiusd` receives a `HUP` signal (UNIX) or the server is refreshed (Windows NT 4.0).

The `dictionary` file is distributed with Ascend Access Control and can not be edited via the graphical user interface screens. You can edit the `dictionary` with a text editor such as vi (UNIX) or Notepad (Windows NT 4.0)

`dictionary` contains a list of Ascend Access Control attribute/value pair translations the Ascend Access Control server uses to parse incoming authentication requests and generate outgoing authorization responses.

`dictionary` may contain comments, which are indicated by leading pound sign("#") character. Comments and blank lines inserted in `dictionary` are ignored.

Each attribute's value is specified as one of four data types:

- string - 0-253 octets
- ipaddr - 4 octets in network byte order

- integer - 32 bit value in big endian order (high byte first)
- date - 32 bit value in big endian order - seconds since 00:00:00 GMT, Jan. 1, 1970

Attribute entries consist of four required fields and one optional fifth field:

```
Attribute Attribute-name Integer-encoding Type [Pruning]
```

Value entries consist of four fields

```
Value attribute-name value-name integer-encoding
```

Example:

```
Attribute Framed-Protocol 7 integer (1,0)
Value Framed-Protocol PPP 1
```

The Attribute line's optional `Pruning` field has a unique syntax:

```
[ ( [<ack>] [ [ [, ][<nak>] ] [ [,]
[MAY\MUST\CONFIG] ] ] ) ]
```

`ack` values affect the RADIUS server's Access-Accept replies and `nak` values affect its Access-Reject replies. If the whole expression is omitted, the default `(0,0 MAY)` is assumed. The keywords `MAY` and `MUST` are only meaningful for RADIUS versions 2 and 3. Table A-2 lists the meanings of the values for the `ack` and `nak` keywords.

Table A-2. Meanings of the ack and nak values in a RADIUS server's replies.

Value	Meaning
0	No attributes of this kind are part of the final reply.
1	At most, one attribute of this kind may be part of the final reply.
*	Any number of attributes of this kind may be part of the final reply.
MUST	The NAS must reject the Access-Request if it does not understand this attribute.

Table A-2. Meanings of the ack and nak values in a RADIUS server's replies.

Value	Meaning
MAY	The NAS may reject, not reject, or silently discard the Access-Request.
CONFIG	This attribute is a configuration item only.The CONFIG keyword is only for the internal use of the Ascend Access Control server and mustappear by itself (i.e., (`config`) at the end of the attribute line.

Vendor Specific Attributes

Ascend Access Control supports this syntax for handling vendor-specific attributes:

```
vendor:attribute-string
```

`vendor` is the vendor's name and `attribute-string` is a unique string for that vendor. Vendor specific attribute and value identifier strings are defined in the `vendors` file and these strings may be used in place of default attribute/value strings.

Example:

```
Ascend.attr Ascend.value 529 Ascend 26 172
```

Files

`dictionary`

See Also

users(5), vendors(5), radiusd(8)

radiusd(8)

Name

`radiusd` - Remote Authentication Dial In User service daemon

Synopsis

```
radiusd [ -d database_directory]
[ -a accounting_directory]
[ -c current_working_directory ]  [ -p radius_port]
[ -q accounting_port] [ -ffsm_file]
[ -pp radius_relay_port ] [ -qq accounting_relay_port]
[ -g 'syslog' / 'logfile' / 'stderr' ] [ -ttimeout ]
[ -s] [ -x] [ -v] [ -z] [ -h] [ -u]
```

Description

`radiusd` handles Access-Requests for user authentication from Ascend Access Control clients. These clients can be Network Access Servers (NAS) or other RADIUS servers. Authentication requests come to `radiusd` in the form of UDP packets conforming to the Ascend Access Control protocol.

`radiusd` collects authentication requests and processes them depending on their type. "Description" on page A-12 describes the types of authentication requests. If requested, `radiusd` can authenticate a user by calling upon other RADIUS servers, authentication services such as Kerberos, and operating system services, such as the UNIX system subroutines which access the `/etc/passwd` file.

When `radiusd` receives an authentication request from a client, in the form an Access-Request packet, it validates the client. Then `radiusd` consults a local database of users in a `users` file to find a user name that matches the one in the request, (see "users(5)" on page A-31). The matching user entry in the `users` file contains a list of requirements which must be met before `radiusd`

authenticates the user. These requirements are called check-items. Usually, one of the check-items is the user's password. For example, if the user's profile in the `users` file indicates the the user's password is a check-item, the password received by `radiusd` must match the value of a user password attribute in the `users` file or the user will not be authenticated. There is no set list of requirements for all users and each may be entirely different, although some users with common connection needs may be nearly identical.

If any condition of the requirements is not met, `radiusd` sends an Access-Reject response to the client that requested authentication. If all the conditions are met, `radiusd` places a list of configuration values called reply-items in an Access-Accept packet and sends it to the client.These reply-items often include the type of service the user is allowed to use and other values necessary to deliver that service, such as the link protocol.

Ascend Access Control files

A number of files are installed with Ascend Access Control and used by `radiusd`. The `authfile`, `clients`, `dictionary`, and optionally, the `users` files, are read into resident memory tables.

The RADIUS server is refreshed whenever `radiusd` receives a HUP signal or the service is refreshed. Table A-3 lists other signals `radiusd` can receive and their effect.

Table A-3. Signals the RADIUS server can receive.

Signal	Effect
INT	Initializes only the AATV modules.
USR1	Turns on debugging, much as the `-x` option does, except that repeating the USR1 signal increases the debugging level. (See below for more information about the `-x` flag.)
USR2	Turns off debugging.
TERM	Provides an orderly way of shutting down the RADIUS server.

Ascend Access Control Installation

Ascend Access Control Ports

The following lines are added to a UNIX system's `/etc/services` file when Ascend Access Control is installed. The same information is entered in an appropriate place on a Windows NT 4.0 server. The information indicates that `radiusd` listens for Access-Requests at port 1645 and receives Accounting packets from the Ascend Access Control clients on port 1646.

```
radius  1645/udp
radiusacct  1646/udp
```

Ascend Access Control Timeout

As installed, the default timeout for `radiusd` is fifteen minutes. You can set a longer value for the `radiusd -t` option to manually configure a longer timeout. Or, to make the Ascend Access Control server run automatically when requests arrive, you can enter the value 0 (zero) for the `-t` option. On UNIX systems, install the following line in your `/etc/inetd.conf` file:

```
radius dgram udp wait root /usr/private/etc/radiusd
radiusd
```

Running as other than root

Note that the Ascend Access Control server need not run as root (UID 0), although it normally does. It may be safer to pick a less powerful user who has no password and is used only for administrative purposes, unless the server needs superuser privilege to access a shadow password file.

Also, do not forget to send a HUP signal to your running `inetd` process to force it to re-read its own database file, `/etc/inetd.conf`, into memory.

Options

Table A-4 lists the `radiusd` options and their effect on the RADIUS server.

Table A-4. `radiusd` *options*

Option	Description
`-a` accounting_directory	Allows the user to override the default accounting directory. Specify an alternate directory to contain the Ascend Access Control accounting detail files.
`-c` current_working_directory	Allows the user to override the current working directory, or the default. Specify an alternate directory name. In UNIX this option only affects file system operation for files specified with relative file names that don't contain a leading forward slash (/) character.
`-d` database_directory	Allows the user to override the default database and configuration file directory. Specify an alternate directory name to house the Ascend Access Control `authfile`, `clients, dictionary,` and `users` files. See `authfile(5), clients(5), dictionary(5),` and `users(5)` for more information.
`-f` fsm_file	Allows user to specify an alternate *finite state machine* table instead of the default `*.fsm` file. This option is supported by the Ascend Access Control software, but Ascend does not document the creation of alternative *finite state machine* tables.
`-g` 'syslog' | 'logfile' | 'stderr'	Allows the user to specify whether to use `syslog(3)` style, logfile style or stderr logging for warning, error and informational messages. It is possible to specify daily or weekly renaming. . You can also specify which weekday starts the week. Archiving, with compression of the Ascend Access Control logfile, is also supported. See the RADIUS_COMPRESS and TRUNCATION_DAY macros in the `radius.h` include file
`-h`	Causes the Ascend Access Control server to place a usage (help) message into stdout.

Table A-4. `radiusd` *options*

Option	Description
`-oa` ODBC_acct_flag	Causes the server to forward information it receives from NAS accounting packets to a Database Management System table.
`-p` port	Allows user to specify an alternate authentication port number instead of the default port 1645.
`-pp` port	Allows user to specify an alternate authentication relay port number instead of the default port 1645.
`-q` acct_port	Allows user to specify an alternate accounting port number instead of the default port 1646.
`-qq` acct_port	Allows user to specify an alternate accounting relay port number instead of the default port 1646.
`-r` realm_separator	Allows user to specify the character the server recognizes as separator between a user name and a realm name.
`-rr` realm_separator	Allows user to specify the character the server recognizes as separator between a user name and a realm name.
`-s`	Places the Ascend Access Control server into the single process (non-spawning) mode, versus the multi-tread process mode.
`-t` timeout	Allows the user to specify a timeout value for the `select(2)` system call which is different from the default timeout value of fifteen minutes. Giving the `-t` option a value of zero (`-t0`) puts the server into a blocking mode. `radiusd` never times out and terminates, but waits at the `select(3)` call forever.

Table A-4. `radiusd` *options*

Option	Description
`-u`	Specifies to NOT read the `users` file into the internal data structures. This function is supported. However, it is generally used in conjunction with `dbm(3)` support library, which causes indexing of the `users` file. Ascend Access Control does not support indexing of the `users` file. "Note about the RADIUS builddbm utility" on page 7-3 describes the reasons Ascend Access Control does not support indexing.
`-v`	Causes the Ascend Access Control server to place its version information into stdout.
`-x`	Allows the user to turn on the debugging output. The `-x` option can be repeated on the command line to increase the level of debugging information you receive. • `-x` provides minimal debugging output, send/receive a/v pairs, etc. • `-x-x` provides `-x` level debugging and *finite state machine* high level output and some function tracing • `-x-x-x` provides `-x-x` level debugging and the remaining function tracing • `-x-x-x-x` provides `-x-x-x` level debugging and *finite state machine* low level output and low level config files Note: Debugging output is directed to the `radius.debug` file. Since the `-x` option turns off some of the daemon behavior of the server, such as disconnecting from the controlling terminal, etc., it is not a good idea to try running the server from `(x)inetd(`8) and specifying more `-x` options.
`-z`	Causes the Ascend Access Control `logfile` and `debug` file to be emptied, but only if the debugging option `-x` is enabled. This option has no effect on the `logfile` if the `-g` option specifies `syslog`(3) style logging

Exit Status

Table A-5 lists the `radiusd` exit status codes and associations. You can also find information about error termination conditions in `logfile` or `syslog` entries, depending upon the server's configuration.

Table A-5. `radiusd` exit status values.

Codes	Association
255 (-1)	dict_init
254 (-2)	config_init
253 (-3)	init_fsm
252 (-4)	config_files
251 (-5)	disconnect
250 (-6)	open PID file
249 (-7)	SIG_FATAL
248 (-8)	usage
247 (-9)	user_update
246 (-10)	version
245 (-11)	setupsock (can't bind, Ascend Access Control already running?)
244 (-12)	init_id_to_key
243 (-13)	list_copy
242 (-14)	find_state
241 (-15)	chdir
240 (-16)	hostname

Files

Table A-6 lists files which are related to `radiusd` configuration.

Table A-6. Files associated with `radiusd` configuration.

Files	Description
`/etc/passwd`	UNIX file containing user passwords.
`/etc/raddb`	UNIX directory containing Ascend Access Control configuration and database files.
`C:\Ascend\Access_Control\database`	Windows NT 4.0 directory containing Ascend Access Control configuration and database files.
`/etc/services`	File which contains list of TCP/UDP services and their port numbers.

See Also

authfile(5), clients(5), dictionary(5), users(5), radcheck(8), radpwtst(8)

radcheck(8)

Name

`radcheck` - determines whether an Ascend Access Control server is operational

Synopsis

```
radcheck [ -d directory] [ -p port] [ -r retries] [ -t time-
out] [ -x] [ -v] [ -n] servername
```

Description

`radcheck` determines if the Ascend Access Control server whose DNS name is entered on the command line is operational. `radcheck` may be executed on any host, even if it is not registered in the Ascend Access Control `clients` file. See `authfile(5)` for more information.

If the server is operational, `radcheck` displays the following on standard output:

```
auth queue:a/b, acct queue: c/d, maxtime: t (date)
authfile: x, clients: y, users: z, date
Ascend Access Control version version config codes
“servername” (port-number) is responding
```

If the number of retries is greater than zero, `radcheck` will also display:

```
(n retries)
```

otherwise, `radcheck` displays

```
“servername” (port-number) some message
```

where one of these, among others, may be some message:

```
No reply from Ascend Access Control server “<host-
name>(port)”
```

```
Received non-matching id in server response
Received invalid reply digest from server
No such server: “<hostname>”
```

Options

Table A-7 lists the options with which you can run the `radcheck` program.

Table A-7. `radcheck` options and descriptions.

Option	Description
`-d` directory	Allows user to specify an alternate directory instead of the default, `/etc/raddb`
`-p` port	Allows user to specify an alternate port number instead of the default, 1645
`-r` retries	Allows user to specify a number of retries instead of the default, 10
`-t` timeout	Allows user to specify a maximum timeout different than te default, 3 seconds
`-x`	Allows user to turn on debugging output
`-v`	Prints the version of Ascend Access Control used to build the program

Exit Status

Table A-8 lists the `radcheck` exit status codes.

Table A-8. `radcheck` exit status values and descriptions.

Status	Description
-2	Ascend Access Control server response errors
-1	Local server errors
0	Normal successful completion

Table A-8. `radcheck` *exit status values and descriptions.*

Status	Description
1	Timeout errors

See Also

authfile(5), clients(5), dictionary(5), users(5), radiusd(8), radpwtst(8)

radpwtst(8)

Name

`radpwtst` - authenticates a user's password

Synopsis

```
radpwtst [ -c code] [ -d directory] [ -f file] [ -g group]
[ -h] [ -i client_ip_address] [ -l aysnc_port]
[ -p UDP_port] [ -r retries] [ -s servername] [ -t timeout]
[ -u type] [ -v[1 | 2]] [ -w password] [ -x]
[ -:<attribute>=<value>] userid[@realm]
```

Description

`radpwtst` uses a Ascend Access Control server to authenticate a user. Following is the process when the userid of the user being authenticated has been entered on the command line the authentication:

- `radpwtst` prompts for the password that matches the userid
- `radpwtst` forwards the userid/password tuple to a Ascend Access Control server

An exact match is required for successful authentication.

userid@realm format

When the userid is given in the format `user@realm`, it is assumed that the user is a member of an authentication realm listed in the Ascend Access Control server's `authfile` file. This file is searched for a matching userid/password combination. `authfile` is further assumed to be in the Ascend Access Control default directory. See "authfile(5)" on page A-2 for more information.

userid format

When the optional *@realm* is omitted from the userid, the userid is sought in the Ascend Access Control server's `users` file.

DEFAULT user

In either case, *userid@realm* format or userid format, an exact match of the userid/password tuple is required. If the match fails, the Ascend Access Control server checks the appropriate file for a DEFAULT entry. The DEFAULT entry should contain information about how to authenticate the user.

`radpwtst` displays one of two messages on standard output, depending on the success of the authentication:

```
authentication OK
```

```
userid authentication failed
```

Options

Table A-9 lists the `radpwtst` options and their descriptions.

Table A-9. `radpwtst` options and their descriptions

Option	Description
`-c` code	Allows user to specify several Ascend Access Control packet type codes : • 1 - (Access-Request) • 4 - (Accounting-Request) • 7 - (Password-Request) • 12 - (Status-Server)

Table A-9. `radpwtst` options and their descriptions

Option	Description
`-d` directory	Allows the user to specify an alternate directory for the Ascend Access Control `authfile`, `users`, `clients` files. This replaces the default directory which is `/etc/raddb`. An error is displayed on stdout if the Ascend Access Control configuration files are not found. **Note:** If the machine running `radpwtst` is different than the machine runnning the Ascend Access Control server, make sure that the contents of one machine's configuration files are identical to the contents of the other machine's configuration files.
`-f` file	Allows the user to specify a prefix for a file in the `users` file format. See"users(5)" on page A-31. The file name is assumed to be `prefix.users` and it is assumed to be in the Ascend Access Control configuration file directory, (see `-d` above). This file contains arbitrary check-items and reply-items (attribute and value pairs) for psuedo-users whose names may be specifed by the `-g` option. If no `-g` option is given, the DEFAULT entry is used if it is present. This is the way arbitrary attribute/value pairs are communicated to remote Ascend Access Control servers.
`-g` group	Allows the user to specify an arbitrary pseudo-user named group in the file named by the `-f` option. See -f option for more about sending arbitrary attribute/value pairs to remote Ascend Access Control servers.
`-h`	Causes a usage (help) message to be placed in stdout.
`-i` client_IP_address	Allows the user to specify a client IP address that's different than the default IP address of the originating machine.
`-l` async_port	Allows the user to specify a an async port number that's different than the default async port of 1.
`-p` UDP_port	Allows the user to specify a UDP port on the server that's different than the default, 1645.

Table A-9. `radpwtst` *options and their descriptions*

Option	Description
`-r` retries	Allows the user to specify that the maximum number of retries be something other than the default 10 retries
`-s` servername	Allows the user to specify an alternate server other than the default
`-t` timeout	Allows the user to specify an alternate timeout value other than the default 3 seconds. Timeout values are x seconds.
`-u` type	Allows the user to specify one of the following Service-Type values instead of the default auth value: • `admin, auth, dumb, exec, kchap, outbound, ppp, slip, dbadmin, dbdumb, dbppp, dbslip` (`db` stands for dial back.) **Note:** The default auth fails if the Access-Request produced by `radpwtst` contains no password or an empty password (`default` or `-c1`). When the Service-Type is Authenticate-Only, the Ascend Access Control server requires a valid, non-empty password in Access-Request packets.
`-v`	Prints the Ascend Access Control version used to build the program. If the option is -v1 or -v2 the request is built according to version 1 or 2 of the RADIUS protocol, respectively.
`-w` password	Allows the user to provide a password on the command line. The user is not prompted for a password.
`-x`	Allows the user to turn on the debugging output
-:<attribute>=<value>	Text following the colon (:) character specifies the value of any attribute in the `dictionary`. The syntax is identical to that of reply-items, as described in “users(5)” on page A-31.

Exit Status

Table A-10 lists the exit status values `radpwtst` returns to the system.

Table A-10. radpwtst exit status values.

Value	Description
1	timeout error
0	successful completion
-1	local error
-2	Ascend Access Control server error

Files

`/etc/raddb, C:\Ascend\Access_Control\database`

See Also

authfile(5), client(5), dictionary(5), user(5), radcheck(8), radiusd(8)

users(5)

Name

`users` - Ascend Access Control user security and configuration file

Synopsis

UNIX

`/etc/raddb/users`

Windows NT 4.0

`c:\Ascend\Access_Control\database\users`

Description

The `users` file is installed in the Ascend Access Control server's default directory, unless configured differently by the system administrator. `users` is read by `radiusd` at startup and whenever `radiusd` receives a `HUP` signal (UNIX) or the server is refreshed (Windows NT 4.0).

You may create or edit entries in `users` file with a text editor, the Ascend Access Control Manager's Edit Clients screens, or the User Account Wizard.

`users` contains a list of the users the Ascend Access Control server can authenticate for clients and other servers. Ascend Access Control clients are Network Access Servers (NAS), like routers, or other Ascend Access Control servers.

`users` may contain comments, which are indicated by leading pound sign (#) character. Comments and blank lines inserted in `users` are ignored.

Commas may be used to separate items in any line, or at the end of any line. Ascend Access Control treats commas as though they are whitespace.

Initial Lines

`users` may contain one or more lines of information per Ascend Access Control user entry. The first line of each user entry consists of one or more fields, in the sequenceshown below. The fields are separated by whitespace.

```
<user-name> <check-item> [, <check-item>]...
```

Example:

```
george Password="casablanca"
```

Special user names

Ascend Access Control recognizes four special user names which are used for these reasons:

- the default for all user names which do not match any previous entries
- to hold non-framed reply-items
- to hold PPP reply-items
- to hold SLIP reply-items

The special user names include , DEFAULT which specifies how to authenticate user names which do not match any previously parsed entries. DEFAULT should be the last entry in the `users` file.

The special user name ODBCACCT specifies that accounting information will be sent to the data source indicated by the value of the profile's Password attribute. "users file profiles that point to DBMS tables" on page 7-24 contains more information about the ODBCACCT user profile.

The other special user names `dumbuser, pppuser` and `slipuser` allow a user seeking authentication to submit the same account name for for any of the framed or non-framed protocols.

Additional lines

The initial line of a user entry may be followed by additional lines containing reply-items, or attribute/value pairs, that the Ascend Access Control server sends back to the requesting Network Access Server (NAS) or another Ascend Access Control server. The additional lines must begin with white space. The reply-

items may include PPP configuration values, the name of the host to which the user wishes to connect, or any other appropriate attribute/value translations listed in the `dictionary` file.

Additional lines in a `users` file entry have this syntax.

```
whitespace reply-item,
```

Example:

```
Framed-Protocol=PPP
```

Authentication-Type attribute and ODBC support

The Authentication-Type attribute provides the link between the `users` file's user profiles and authentication and accounting attributes stored in the table(s) of a Database Management System (DBMS) that complies with the Open Database Connectivity (ODBC) standard. The support of ODBC tables brings the power and speed of relational database computing to Ascend Access Control authentication, authorization and accounting.

The initial line of the user profile that provides a connection to the table has a unique format. The value of the Password attribute include four entries that enable Ascend Access Control to access the table's information. The format of the initial line is:

```
<username> Authentication-Type = "<database source
name>:database table name>:<table access name>/<table access
password>
```

Example:

```
jsmith@ascend  Authentication-Type = "qesyb:atable:
aname/apasswd
```

The username may be that of a single user such as `jsmith@ascend`, a realm, `ascend.com` or DEFAULT.

Table A-11. Required Password value for support of ODBC tables

Value	Description
ODBC	Flag telling Ascend Access Control to search for a related database table
database source name	Name of database server the Ascend Access Control ODBC Manager consults • begins with the letters “qe” • Examples: qesyb, qedbf, qeor7 (Sybase, dBase, Oracle 7) • Readme for ODBC drivers contains list of acceptable entries
database table name	Name of database table • may be one of several on server • may be associated with realm name • Example: ascendtabl for ascend.com realm
table access name	Name provided by Ascend Access Control server when accessing a database table • different for each table
table access password	Password provided by Ascend Access Control server when accessing a database table • different for each table

Vendor-specific attributes

Vendor specific attributes may be used in place of normal check-item and reply-item attributes in the user entry. Vendor specific attributes have the form `<vendor>:<attribute>`.

Example:

```
Ascend:Ascend-Metric
```

Other users files

Although `users` is installed with Ascend Access Control and is the first file consulted by Ascend Access Control when it receives an Access-Request, there may be other `users` files which are related to separate realms listed in the `authfile` file. These other `users` files share the naming convention `prefix.users`, where `prefix` is usually the name of the realm with which the users are associated.

Example:

Realm	**`Prefix.Users` file name**
ISP1	`ISP1.users`
admin	`admin.users`

Files

```
dictionary, users
```

See Also

dictionary(5), radiusd(8), radcheck(8), radpwtst(8)

vendors(5)

Name

`vendors` - Ascend Access Control file for mapping vendors to vendor codes

Synopsis

UNIX

`/etc/raddb/users`

Windows NT 4.0

`c:\Ascend\Access_Control\database\users`

Description

The `vendors` file is installed in the Ascend Access Control server's default directory, unless configured differently by the system administrator. `vendors` `users` is read by `radiusd` at startup and whenever `radiusd` receives a `HUP` signal (UNIX) or the server is refreshed (Windows NT 4.0).

The `vendors` file is distributed with Ascend Access Control. You cannot edit the `vendors` file via the Ascend Access Control GUIs, but you can use text editors such as vi or Notepad to edit the `vendors` file.

`vendors` contains a list zero or more vendor entries. Each vendor entry contains a vendor name and a vendor number. The vendor numbers are SMI Network Management Private Enterprise Code numbers as described in the RADIUS DRAFT RFC and RFC 1700. Each entry optionally contains an interim way of mapping attribute numbers assigned by vendors outside the RADIUS DRAFT conventions to the RADIUS vendor-specific attribute, which is defined in the RADIUS DRAFT as attribute number 26. This optional mapping is used on Ascend Access Control server inbound and outbound requests.

`vendors` may contain comments, which are indicated by leading pound sign (#) character. Comments and blank lines inserted in `vendors` are ignored.

The file contains a line of information for each vendor in the following form:

```
[ <attribute-string> <value-string> ] <vendor-code>
<vendor-name> [ ( [ <standard-value>
<vendor-specific-value>...] ) ]
```

Example:

```
61 MERIT (211 211 213 213)
Ascend.attr Ascend.value 529 Ascend
(
172 172
156 156
)
```

attribute-string and value-string options

The `attribute-string` and `value-string` are optional strings which default to `Attribute` and `Value` when not specified. Non-default strings may be used to specify vendor specific attributes and values in the `dictionary` file.

vendor-code field

The `vendor-code` field contains a number assigned to the vendor in the Assigned Numbers (IANA), RFC 1700.

Example:

Table A-12. Vendor Codes from RFC 1700

Vendor Name	Vendor Code
MERIT	61
Ascend	529
US Robotics	429

vendor-name field

The `<vendor-name>` field is the vendor name. The vendor name may appear in the `clients` file as a `type=vendor:nas` entry or in vendor-specific attribute names in the `dictionary` and `users` files.

standard-value and vendor-specific value options

The `standard-value` option is the external, or common, attribute number as seen in Ascend Access Control requests on the network.

The `vendor-specific-value` option is the internal attribute number, or the number the vendor assigned to the attribute when it was developed and added to RADIUS.

`standard-value` and `vendor-specific-value` optional fields may be repeated an optional number of times within the parentheses. These numbers are used to map attributes from the common attribute space defined in the RADIUS RFC to internal, non-conflicting vendor-specific attributes. This is necessary because some vendors assign vendor-specific attributes in the standard attribute space instead of in the vendor-specific attribute position defined in the RADIUS RFC.

Files

`clients, users`

See Also

clients(5), dictionary(5), users(5)

Attributes Reference

B

This chapter contains an alphabetic list of Access Control attributes. The list's entries describe the attributes and the values you may assign to them. Each entry includes a section which describes the attribute and explians its use. The list contains all the attributes defined in the original RADIUS protocol, although the majority of the attributes are Ascend's vendor-specific additions to RADIUS.

Because many of the attributes are Ascend vendor-specific, they are based on parameters for the MAX router. The attribute descriptions and usage explanations of Ascend-specific entries refer explicitly to the MAX and you may obtain more information about MAX parameters by consulting the *MAX ISP and Telecommuting guide.*

Attribute Name

Description: The Description text explains the attribute.

Usage: The Usage text explains the values you can specify for the attribute.

Example: The Example text presents an example of how to use the attribute.

Dependencies: The Dependencies text tells you what other information you need in order to specify the proper value for the attribute.

Acct-Authentic (45)

Description: This attribute specifies whether an incoming call was authenticated by RADIUS, TACACS, or a local Connection Profile, or whether the MAX accepted the call without authentication.

Acct-Authentic is sent in an Accounting-Request packet under these conditions:

- At the start of a session (when Acct-Status-Type=Start)
- At the end of an authenticated session (Acct-Status-Type=Stop) when the Auth parameter is not set to RADIUS/LOGOUT

Usage: Acct-Authentic does not appear in a user profile. It can have either of the following values:

- RADIUS (1)

  This value indicates that RADIUS authenticated the incoming call. RADIUS is the default.
- Local (2)

  This value indicates that an incoming call was authenticated by a local Connection Profile or by TACACS, or that the call was accepted without authentication.

Acct-Delay-Time (41)

Description: This attribute specifies how many seconds the MAX has been trying to send this Accounting packet.

Acct-Delay-Time is sent in an Accounting-Request packet under these conditions:

- At the start of a session (when Acct-Status-Type=Start)
- At the end of a session or when a session fails to authenticate (Acct-Status-Type=Stop) and the Auth parameter is not set to RADIUS/LOGOUT

Usage: Acct-Delay-Time does not appear in a user profile. Its default value is 0 (zero).

Acct-Input-Octets (42)

Description: This attribute specifies how many octets have been received during the session.
Description: Acct-Input-Octets is sent in an Accounting-Request packet at the end of a session (Acct-Status-Type=Stop) when both of these conditions are true:

- The session has been authenticated.
- The Auth parameter is not set to RADIUS/LOGOUT.

Usage: Acct-Input-Octets does not appear in a user profile. Its default value is 0 (zero).

Acct-Input-packets (47)

Description: This attribute specifies how many packets have been received during the session. Acct-Input-packets is sent in an Accounting-Request packet at the end of a session (Acct-Status-Type=Stop) when all of these conditions are true:

- The session has been authenticated.
- The Auth parameter is not set to RADIUS/LOGOUT.
- A framed protocol is in use.

Usage: Acct-Input-packets does not appear in a user profile. Its default value is (zero).

Acct-Output-Octets (43)

Description: This attribute specifies how many octets have been sent during the session.

Acct-Output-Octets is sent in an Accounting-Request packet at the end of a session
(Acct-Status-Type=Stop) when both of these conditions are true:

- The session has been authenticated.
- The Auth parameter is not set to RADIUS/LOGOUT.

Usage: Acct-Output-Octets does not appear in a user profile. Its default value is (zero).

Acct-Output-packets (48)

Description: This attribute specifies how many packets have been sent during the session. Acct-Output-packets is sent in an Accounting-Request packet at the end of a session
(Acct-Status-Type=Stop) when all of these conditions are true:

- The Auth parameter is not set to RADIUS/LOGOUT.
- The session is authenticated.
- A framed protocol is in use.

Usage: Acct-Output-packets does not appear in a user profile. Its default value is (zero).

Acct-Session-Id (44)

Description: This attribute specifies a unique numeric string identified with the bridging, routing, or terminal server session reported in the Accounting-Request packet. RADIUS correlates the Accounting Start packet and Accounting Stop packet using Acct-Session-Id.

Acct-Session-Id is sent under these conditions:

- At the start of a session (when Acct-Status-Type=Start)
- At the end of a session or when a session failed to authenticate (Acct-Status-Type=Stop) and the Auth parameter is not set to RADIUS/LOGOUT

Usage: Acct-Session-Id does not appear in a user profile. Its value can range from 1 to 2,137,383,647. For every session, RADIUS generates a unique session ID, thereby preventing the same session ID from being used for more than one session.

Dependencies: Keep this additional information in mind:

- SNMP accounting uses session reference numbers to identify sessions; when an SNMP accounting session and a RADIUS accounting session have the same ID, they are identical.

However, SNMP records all calls, while RADIUS records only those calls that result in a successful login or authentication.

- Using the Acct-ID Base parameter in the Ethernet Profile, you can specify whether the numeric base of the Acct-Session-Id attribute is 10 or 16.

  This parameter controls how the Acct-Session-Id attribute is presented to the accounting server. For more information, see the *MAX Reference Guide*.
- The Acct-Session-Id attribute is defined in section 5.5 of IETF RFC 2059 for RADIUS accounting.

Acct-Session-Time (46)

Description: This attribute specifies how many seconds the session has been logged in.

Acct-Session-Time is sent in an Accounting-Request packet at the end of a session (Acct-Status-Type=Stop) when both of these conditions are true:

- The session has been authenticated.
- The Auth parameter is not set to RADIUS/LOGOUT.

Usage: Acct-Session-Time does not appear in a user profile. Its default value is 0 (zero).

Acct-Status-Type (40)

Description: This attribute specifies whether the Accounting packet sent to the RADIUS server is the beginning (Start) or end (Stop) of a bridging, routing, or terminal server session.

Acct-Status-Type is included under these conditions:

- At the start of a session (when Acct-Status-Type=Start)
- At the end of a session or when a session fails to authenticate (when Acct-Status-Type=Stop), and only if the Auth parameter is not set to RADIUS/LOGOUT

Usage: Acct-Status-Type does not appear in a user profile.

Ascend-Add-Seconds (240)

Description: This attribute specifies the number of seconds that average line utilization (ALU) for transmitted data must exceed the threshold indicated by the Ascend-Target-Util attribute before the MAX begins adding bandwidth to a session. The MAX determines the ALU for a session by using the algorithm specified by the Ascend-History-Weigh-Type attribute.

When utilization exceeds the threshold for a period of time greater than the value of the Ascend-Add-Seconds attribute, the MAX attempts to add the number of channels specified by the Ascend-Inc-Channel-Count attribute. Using the Ascend-Add-Seconds and Ascend-Remove-Seconds attributes prevents the system from continually adding and subtracting bandwidth, and can slow down the process of allocating or removing bandwidth.

Usage: Specify a number between 1 and 300. The default value is 5.

Dependencies: Keep this additional information in mind:

- Additional channels must be available, and the number of channels added cannot exceed the amount specified by the Ascend-Maximum-Channels attribute.
- Ascend-Add-Seconds and Ascend-Remove-Seconds have little or no effect on a system with a high Ascend-Seconds-Of-History value.

  If the value of Ascend-Seconds-Of-History is low, the Ascend-Add-Seconds and Ascend-Remove-Seconds attributes provide an alternative way to ensure that spikes must persist for a certain period of time before the system responds.

Ascend-Ara-PW (181)

Note: This attribute no longer appears in a user profile. The user profile at the end of this description does illustrate how you configure a user profile to specify the password of an incoming caller over AppleTalk Remote Access (ARA).

Description: This attribute specifies the password of the incoming caller over ARA (AppleTalk Remote Access). The ARA software in the MAX uses DES to encrypt and decrypt the password.

Example: This example sets up a TCP connection through ARA with dynamic IP address assignment:

```
Emma Authentication-Type=ARA-DES, Password=”pwd”
     Framed-Protocol=Ascend-ARA,
     Ascend-Send-Secret="pwd",
     Ascend-Route-IP=Route-IP-Yes,
     Ascend-Assign-IP-Pool=1
```

Ascend-Assign-IP-Pool (218)

Description: This attribute specifies the address pool from which RADIUS assigns the user an IP address.

A pool is a range of contiguous IP addresses on your local network. The MAX chooses an address from these pools and assigns it to an incoming call when Assign Adrs=Yes in the Answer Profile, or when the calling station requests an address assignment. Assigning an address to a device is called performing dynamic IP. Dynamic IP can apply when the calling end is a station; however, if the calling end is a router, that router usually rejects attempts to perform dynamic IP.

If you need to define more than two pools of addresses, you must use the RADIUS attribute Ascend-IP-Pool-Definition to configure the IP address pools.

Usage: Specify an integer corresponding to an address pool. The default value is 1.

Example: In the user profile, the host is configured to request an address from address pool #2:

```
emma Password="m2dan"
        Service-type=Framed
     Framed-Protocol=PPP,
     Ascend-Route-IP=Route-IP-Yes,
     Ascend-Metric=2,
     Framed-Routing=None,
     Ascend-Assign-IP-Pool=2
```

Ascend-Authen-Alias (203)

Description: This attribute sets the MAX unit's login name during PPP authentication.

When the MAX places an outgoing call, it identifies itself by a login name and password. The login name is either its system name (as specified by the Name parameter in the System Profile) or the value you specify for the Ascend-Authen-Alias attribute.

Usage: Specify a text string containing up to 16 characters. The default is the value of the Name parameter in the System Profile.

Example: This example uses the Ascend-Authen-Alias attribute in an outgoing profile:

```
homer-out Password="ascend", Service-Type=Outbound
        User-Name="homer",
        Ascend-Authen-Alias="myMAXcallingU",
        Ascend-Send-Auth=Send-Auth-PAP,
        Ascend-Send-Secret="passwrd1",
        Ascend-Dial-Number="31",
        Framed-Protocol=PPP,
        Framed-IP-Address=10.0.100.1,
        Framed-IP-Netmask=255.255.255.0,
        Ascend-Metric=2,
        Framed-Routing=None,
        Framed-Route="10.5.0.0/24 10.0.100.1 1",
        Ascend-Idle-Limit=30
```

Ascend-Backup (176)

Description: This attribute specifies the name of a backup profile for a nailed-up link when the physical connection fails. The MAX automatically diverts traffic to the backup connection. When the primary connection is restored, traffic again uses the primary connection.

When you use the backup connection, the MAX does not move routes to the backup profile. Therefore, the IP routes shown in the terminal server display may be incorrect, although statistical counts reflect the change.

Usage: Specify the name of the profile that you want to act as the backup. The backup connection can be switched or nailed up. The default value is null.

Dependencies: Keep this additional information in mind:

- Do not create nested backup connections.
- Attributes that you define for the primary profile do not automatically apply to the backup profile.

  For example, if you set the primary profile to filter Telnet packets, you must set the backup profile to filter Telnet packets as well. Outgoing Frame Relay packets are the only packets that follow the primary profile definitions. All other packets follow the backup profile definitions.

Ascend-Base-Channel-Count (172)

Description: This attribute specifies the initial number of channels the MAX sets up when originating calls for a PPP, MP+, MP, or Combinet multichannel link.

Usage: The maximum number of channels you can specify depends upon the nature of the link:

- For a PPP link, the maximum number of channels is always 1.
- For an MP+ or MP link, the amount you specify is limited by the number of channels available, but the device at the remote end of the link must also support MP+ or MP.
- For a Combinet link, you can specify up to two channels.

The default value is 1.

Dependencies: Keep this additional information in mind:

- The Ascend-Base-Channel-Count attribute does not apply when all channels of the link are nailed up (Ascend-Call-Type=Nailed).
- For optimum MP+ performance, both sides of a connection must set these parameters and attributes to the same values:
  - Base Ch Count (in the Connection Profile) or Ascend-Base-Channel-Count (in RADIUS)

- Min Ch Count (in the Answer Profile and the Connection Profile) or Ascend-Minimum-Channels (in RADIUS)
- Max Ch Count (in the Answer Profile and the Connection Profile) or Ascend-Maximum-Channels (in RADIUS)

Ascend-Billing-Number (249)

Description: This attribute specifies a billing number for charges incurred on the line. If you do not enter a billing number, the telephone company bills charges to the telephone number assigned to the line.

Your carrier determines the billing number, and uses it to sort your bill. If you have several departments, and each department has its own Ascend-Billing-Number, your carrier can separate and tally each department's usage.

Usage: Specify a telephone number. You can indicate up to ten characters, and you must limit those characters to the following:

```
1234567890()[]!z-*# |
```

Dependencies: The MAX uses the Ascend-Billing-Number attribute differently depending on the type of line you use:

- For a T1 line, the MAX appends the value specified in the Ascend-Billing-Number attribute to the end of each phone number it dials for the call.
- Ascend-Billing-Number for outgoing calls on an ISDN BRI line applies only to installations in Australia.
- For a T1 PRI line, the MAX uses the Ascend-Billing-Number rather than the phone number ID to identify itself to the answering party.

  The Clid Auth parameter enables you to require a device to authenticate incoming calls by checking the calling party's phone number. The device performs CLID (Calling Line ID) authentication before answering an incoming call. The calling party's phone number must match the Calling # parameter or the Calling-Station-ID attribute. If the device cannot authenticate the call when CLID authentication is required, the call is rejected.

  If the calling party uses the Ascend-Billing-Number attribute instead of its phone number as its ID, the CLID used by the answering side is not the true phone number of the caller. This situation presents a security breach if you use Clid Auth.

Further, be aware that if you specify a value for the Ascend-Billing-Number attribute, there is no guarantee that the phone company will send it to the answering device.

Ascend-Bridge (230)

Description: This attribute enables or disables protocol-independent bridging for the user
profile.

Usage: You can specify one of these values:

- Bridge-No (0)

  This setting disables bridging for the link. Bridge-No is the default.
- Bridge-Yes (1)

  This setting enables bridging for the link.

Example: This user profile specifies an IPX bridging link:

```
MAX1 Password="m2dan", Service-Type=Framed
     Framed-Protocol=PPP,
     Ascend-Route-IPX=Route-IPX-No,
     Ascend-Bridge=Bridge-Yes,
     Ascend-Handle-IPX=Handle-IPX-Client,
     Ascend-Netware-timeout=30
```

Ascend-Bridge-Address (168)

Description: This attribute specifies the IP address and associated MAC address of a device on a remote LAN to which the MAX can form a bridging connection.

Usage: The Ascend-Bridge-Address attribute has this format:

```
Ascend-Bridge-Address="<MAC_address> <IP_address>"
```

Table B-1 describes Ascend-Bridge-Address arguments.

Table B-1. Ascend-Bridge-Address arguments

Argument	Description
<MAC_address>	Specifies a MAC address in standard 12-digit hexadecimal format (yyyyyyyyyyyy) or in colon-separated format (yy:yy:yy:yy:yy:yy). If the leading digit of a colon-separated pair is 0 (zero), you do not need to enter it; that is, ":y" is the same as ":0y". The default value is 000000000000.
<IP_address>	Specifies an IP address in dotted decimal format. The default value is 0.0.0.0.

When your MAX receives an ARP request for one of the IP devices you specify, the MAX replies with the corresponding MAC address. Because the MAX replies to these ARP requests as if the IP devices were local, you must have user profiles that bridge IP packets to each device.

Dependencies: Each bridge entry must appear in a pseudo-user profile. You create a pseudo-user to store information that the MAX can query—in this case, in order to store bridging information. For a unit-specific bridge entry, specify the first line of a pseudo-user entry in this format:

```
bridge-<unit_name>-<num> Password="ascend", Service-Type=
Outbound
```

<unit_name> is the system name of the MAX—that is, the name specified by the Name parameter in the System Profile. <num> is a number in a sequential series, starting at 1.

In each pseudo-user profile, you specify one or more Ascend-Bridge-Address attributes. When you have properly configured the profile, RADIUS adds bridging entries to the bridge table whenever you power on or reset the MAX, or when you select the Upd Rem Cfg command from the Sys Diag menu. RADIUS adds the entries in this way:

1 RADIUS looks for entries having the format bridge-<unit_name>-<num>, where <unit_name> is the system name and <num> is a number in a sequential series, starting with 1.

2 RADIUS loads the data to create the bridging tables.

Example: This example creates two bridging table entries.

```
bridge-Ascend-1 Password="ascend", Service-Type=Outbound
        Ascend-Bridge-Address="2:2:3:10:11:12 1.2.3.4 1",
        Ascend-Bridge-Address="2:2:3:13:14:15 5.6.7.8 2"
```

Ascend-Callback (246)

Description: This attribute enables or disables callback. Callback occurs when the MAX answers a call and verifies a name and password against a user profile. If
Ascend-Callback=Yes, the MAX hangs up and dials back to the caller using these values:

- The phone number specified by Ascend-Dial-Number
- The password specified by Ascend-Send-Secret or Ascend-Send-Passwd
- Any other relevant attributes in the user profile that authenticated the call

Note: If you set up a RADIUS user profile for callback and CLID-only authentication, the MAX never answers the call; the caller can therefore avoid billing charges.

Usage: You can specify one of these values:

- Callback-No (0)

  This value indicates that the MAX answers in the normal manner after authentication.
- Callback-Yes (1)

  This value indicates that the MAX hangs up and calls back the caller after authentication.

Dependencies: The Ascend-Callback attribute applies only to incoming calls and should not appear in dial-out user profiles (when Service-Type=Outbound).

Ascend-Call-By-Call (250)

Description: This attribute specifies the T1 PRI service that the MAX uses when placing a PPP call.

Usage: Specify a number corresponding to the type of service the MAX uses. The default value is 6. Table B-2 lists the services available for each service provider.

Table B-2. Ascend-Call-By-Call settings

Number	AT&T	Sprint	MCI
0	Disable call-by-call service.	Reserved	N/A
1	SDN (including GSDN)	Private	VNET/Vision
2	Megacom 800	Inwatts	800
3	Megacom	Outwatts	PRISM1, PRISM II, WATS
4	N/A	FX	900
5	N/A	Tie Trunk	DAL
6	ACCUNET Switched Digital Services	N/A	N/A
7	Long Distance Service (including AT&T World Connect)	N/A	N/A
8	International 800 (I800)	N/A	N/A
16	AT&T MultiQuest	N/A	N/A

Ascend-Call-Filter (243)

Description: Unlike the Filter Profiles in the MAX configuration interface, RADIUS filters are part of the outgoing or incoming RADIUS user profile. In other words, within any RADIUS users file defining a user profile, you can

include values for Ascend-Call-Filter to define call filters for that profile. RADIUS filters are retrieved only when a call is placed using a RADIUS outgoing profile or answered using a RADIUS incoming profile.

Usage: Filter entries apply on a first-match basis. Therefore, the order in which filter entries are entered is significant.

If you make changes to a filter in a RADIUS user profile, the changes do not take effect until a call uses that profile.

IP call filter entries

Use this format for an IP call filter entry:

```
Ascend-Call-Filter="ip <dir> <action>
[dstip <dest ipaddr>\<subnet mask>][srcip <src ipaddr>\<sub-
net mask>]
[<proto> [dstport <cmp> <value>] [srcport <cmp> <value>]
[<est>]]"
```

Note: A filter definition cannot contain newlines. The syntax is shown on multiple lines here for printing purposes only.

Table B-3 describes each element of the syntax. None of the keywords are case

Table B-3. IP call filter syntax elements

Keyword or argument	Description
ip	The keyword “ip” indicates an IP filter.
<dir>	The <dir> argument indicates filter direction. You can specify “in” (to filter packets coming into the MAX) or “out” (to filter packets going out of the MAX).
<action>	<action> indicates what action the MAX should take with a packet that matches the filter. You can specify either “forward” or “drop”.

Table B-3. IP call filter syntax elements

Keyword or argument	Description
dstip <dest ipaddr>	"dstip" is a keyword indicating "destination IP address." The filter applies to packets whose destination address matches the value of <dest ipaddr>. If a subnet mask portion of the address is present, the MAX compares only the masked bits. If you set <dest ipaddr> to 0.0.0.0, or if this keyword and its IP address specification are not present, the filter matches all IP packets.
srcip <src ipaddr>	"srcip" is a keyword indicating "source IP address." The filter applies to packets whose source address matches the value of <src ipaddr>. If a subnet mask portion of the address is present, the MAX compares only the masked bits. If you set <src ipaddr> to 0.0.0.0, or if this keyword and its IP address specification are not present, the filter matches all IP packets.
<proto>	<proto> indicates a protocol that you can specify as a name or a number. The filter applies to packets whose protocol field matches this value.The supported names and numbers are icmp (1), tcp (6), udp (17), and ospf (89). If you set <proto> to 0 (zero), the filter matches any protocol.

Table B-3. IP call filter syntax elements

Keyword or argument	Description
dstport <cmp> <value>	"dstport" is a keyword indicating "destination port." This argument is valid only when the protocol is tcp (6) or udp (17). If you do not specify a destination port, the filter matches any port. <cmp> is an argument indicating how to compare the specified value to the actual destination port. It can have the value <, =, >, or !=. <value> can be a number or a name. Supported names and numbers are ftp-data (20), ftp (21), telnet (23), smtp (25), nameserver (42), domain (53), tftp (69), gopher (70), finger (79), www (80), kerberos (88), hostname (101), nntp (119), ntp (123), exec (512), login (513), cmd (514), and talk (517).
srcport <cmp> <value>	"srcport" is a keyword indicating "source port." It is valid only when the protocol is tcp (6) or udp (17). If you do not specify a source port, the filter matches any port. <cmp> is an argument indicating how to compare the specified value to the actual source port. It can have the value <, =, >, or !=. <value> can be a number or a name. Supported names and numbers are ftp-data (20), ftp (21), telnet (23), smtp (25), nameserver (42), domain (53), tftp (69), gopher (70), finger (79), www (80), kerberos (88), hostname (101), nntp (119), ntp (123), exec (512), login (513), cmd (514), and talk (517).
<est>	If you set this argument to 1, the filter matches a packet only if a TCP session is already established. It is valid only when the <proto> specification is tcp (6).

sensitive.

Generic call filter entries

Use this format for a generic call filter entry:

```
Ascend-Call-Filter="generic <dir> <action> <offset> <mask>
<value> <compare> [<more>]"
```

Note: A filter definition cannot contain newlines. The syntax is shown on multiple lines here for printing purposes only.

Table B-4 describes each element of the syntax. None of the keywords are case sensitive.

Table B-4. Generic call filter syntax elements

Keyword or argument	Description
generic	The keyword “generic” indicates a generic filter.
<dir>	The <dir> argument indicates filter direction. You can specify “in” (to filter packets coming into the MAX) or “out” (to filter packets going out of the MAX).
<action>	<action> indicates what action the MAX should take with a packet that matches the filter. You can specify either “forward” or “drop”.
<offset>	<offset> indicates the number of bytes masked from the start of the packet. The byte position specified by <offset> is called the byte-offset. Starting at the position specified by <offset>, the MAX applies the value of the <mask> argument. A mask hides the part of a number that appears behind the binary zeroes in the mask; for example, if you set <mask> to ffff0000 in hexadecimal format, the filter uses only the first 16 binary digits in the comparison, since f=1111 in binary format. The unit then compares the unmasked portion of the packet with the value specified by the <value> argument.

Table B-4. Generic call filter syntax elements

Keyword or argument	Description
<mask>	This argument indicates which bits to compare in a segment of the packet; the mask cannot exceed 6 bytes (12 hexadecimal digits). A one-bit in the mask indicates a bit to compare; a zero-bit indicates a bit to ignore. The length of the mask specifies the length of the comparison.
<value>	This argument indicates the value to compare to the packet contents at the specified offset in the packet. The length of the value must be the same as the length of the mask; otherwise, the MAX ignores the filter.
<compare>	This argument indicates how the MAX compares a packet's contents to the value specified by <value>. You can specify == or !=, for Equal or NotEqual. The default value is Equal.
<more>	If present, this argument specifies whether the MAX applies the next filter definition in the profile to the current packet before making the Forward or Drop decision. The <dir> and <action> values of the next entry must be the same as the <dir> and <action> of the current entry; otherwise, the MAX ignores the <more> flag.

Example: These are examples of IP call filter entries:

```
Ascend-Call-Filter="ip in drop"
```

```
Ascend-Call-Filter="ip out forward tcp"
```

```
Ascend-Call-Filter="ip out forward tcp dstip 10.0.200.3/16
srcip 10.0.200.25/16 dstport!=telnet"
```

```
Ascend-Call-Filter="ip out forward tcp dstip 10.0.200.3/16
srcip 10.0.200.25/16 icmp"
```

Note: A filter definition cannot contain newlines. The syntax is shown on multiple lines here for printing purposes only.

These are examples of generic call filter entries:

```
Ascend-Call-Filter="generic in drop 0 ffff 0080"
Ascend-Call-Filter="generic in drop 0 ffff != 0080 more"
Ascend-Call-Filter="generic in drop 16 ff aa"
```

Ascend-Call-Type (177)

Description: This attribute specifies the type of nailed-up connection in use.

Usage: You can specify one of these values:

- Nailed (1)

  This setting indicates a link that consists entirely of nailed-up channels. Nailed (1) is the default.

- Nailed/Mpp (2)

  This setting indicates a link that consists of both nailed-up and switched channels. The MAX establishes this connection whenever any of its nailed-up or switched channels are connected end-to-end. If a Nailed/Mpp link is down and the nailed-up channels are down, the link cannot re-establish itself until the MAX brings up one or more of the nailed-up channels, or dials one or more switched channels.

  Typically, the switched channels are dialed when the MAX receives a packet whose destination is the unit at the remote end of the Nailed/Mpp connection. The packet initiating the switched call must come from the caller side of the connection.

  If a failed channel is in the group specified by the Ascend-Group attribute, that channel is replaced with a switched channel, even if the call is online with more than the minimum number of channels. Failed nailed-up channels are replaced by switched channels, regardless of the Min Ch Count setting.

- Perm/Switched (3)

  This setting indicates a permanent switched connection.

  A permanent switched connection is an outbound call that attempts to remain up at all times. If the unit or central switch resets, or if the link is terminated, the permanent switched connection attempts to restore the link at ten-second intervals.

  Use this setting if your telephone company charges for each incoming and outgoing connection attempt, but does not charge for connection time on local calls. Ascend's regular bandwidth-on-demand feature conserves con-

nection time but causes many connection attempts. A permanent switched connection performs the opposite function—it conserves connection attempts but causes a long connection time.

For the answering device at the remote end of the permanent switched connection, we recommend that the Connection Profile be configured to answer calls but not originate them. If the remote device initiates a call, the MAX simply does not answer it. This situation could result in repeated charges for calls that have no purpose. To keep the remote device from originating calls, set AnsOrig=Ans Only for that device.

Dependencies: Keep this additional information in mind:

- The MAX adds or subtracts switched channels on a Nailed/Mpp connection as required by the settings on either side of the connection.

  Each side makes its calculations based on the traffic received at that side. If the two sides of the connection disagree on the number of channels needed, the side requesting the greater number prevails.
- The DO Hangup command works only from the caller side of the connection when you choose Nailed/Mpp.

Ascend-Connect-Progress (196)

Description: This attribute specifies the state of the connection before it is disconnected.

Ascend-Connect-Progress is included in an Accounting-Request packet when both of these conditions are true:

- The session has ended or has failed to authenticate (Acct-Status-Type=Stop).
- The Auth parameter is not set to RADIUS/LOGOUT.

Usage: Ascend-Connect-Progress can have any one of values specified in Table B-5.

Table B-5. Ascend-Connect-Progress codes

Code	Explanation
0	No progress.

Table B-5. Ascend-Connect-Progress codes

Code	Explanation
1	Not applicable.
2	The progress of the call is unknown.
10	The call is up.
30	The modem is up.
31	The modem is waiting for DCD.
32	The modem is waiting for result codes.
40	The terminal server session has started up.
41	The TCP connection is being established.
42	The immediate Telnet connection is being established.
43	A raw TCP session has been established with the host. This code does not imply that the user has logged into the host.
44	An immediate Telnet connection has been established with the host. This code does not imply that the user has logged into the host.
45	The Rlogin session is being established.
46	An Rlogin session has been established with the host. This code does not imply that the user has logged into the host.
60	The LAN session is up.
61	LCP negotiations are allowed.
62	CCP negotiations are allowed.
63	IPNCP negotiations are allowed.
64	Bridging NCP negotiations are allowed.

Table B-5. Ascend-Connect-Progress codes

Code	Explanation
65	LCP is in the Open state.
66	CCP is in the Open state.
67	IPNCP is in the Open state.
68	Bridging NCP is in the Open state.
69	LCP is in the Initial state.
70	LCP is in the Starting state.
71	LCP is in the Closed state.
72	LCP is in the Stopped state.
73	LCP is in the Closing state.
74	LCP is in the Stopping state.
75	LCP is in the Request Sent state.
76	LCP is in the ACK Received state.
77	LCP is in the ACK Sent state.
80	IPXNCP is in the Open state.
90	V.110 is up.
91	V.110 is in the Open state.
92	V.110 is in the Carrier state.
93	V.110 is in the Reset state.
94	V.110 is in the Closed state.

Ascend-Data-Filter (242)

Description: Unlike the Filter Profiles in the MAX configuration interface, RADIUS filters are part of the outgoing or incoming RADIUS user profile. In other words, within any RADIUS users file defining a user profile, you can include values for Ascend-Data-Filter to define data filters for that profile. RADIUS filters are retrieved only when a call is placed using a RADIUS outgoing profile or answered using a RADIUS incoming profile.

Usage: Filter entries apply on a first-match basis. Therefore, the order in which filter entries are entered is significant.

If you make changes to a filter in a RADIUS user profile, the changes do not take effect until a call uses that profile.

IP data filter entries

Use this format for an IP data filter entry:

```
Ascend-Data-Filter="ip <dir> <action>
[dstip <dest ipaddr>\<subnet mask>][srcip <src ipaddr>\<sub-
net mask>]
[<proto> [dstport <cmp> <value>] [srcport <cmp> <value>]
[<est>]]"
```

Note: A filter definition cannot contain newlines. The syntax is shown on multiple lines here for printing purposes only.

Table B-6 describes each element of the syntax. None of the keywords are case

Table B-6. IP data filter syntax elements

Keyword or argument	Description
ip	The keyword “ip” indicates an IP filter.
<dir>	The <dir> argument indicates filter direction. You can specify “in” (to filter packets coming into the MAX) or “out” (to filter packets going out of the MAX).

Table B-6. IP data filter syntax elements

Keyword or argument	Description
<action>	<action> indicates what action the MAX should take with a packet that matches the filter. You can specify either "forward" or "drop".
dstip <dest ipaddr>	"dstip" is a keyword indicating "destination IP address." The filter applies to packets whose destination address matches the value of <dest ipaddr>. If a subnet mask portion of the address is present, the MAX compares only the masked bits. If you set <dest ipaddr> to 0.0.0.0, or if this keyword and its IP address specification are not present, the filter matches all IP packets.
srcip <src ipaddr>	"srcip" is a keyword indicating "source IP address." The filter applies to packets whose source address matches the value of <src ipaddr>. If a subnet mask portion of the address is present, the MAX compares only the masked bits. If you set <src ipaddr> to 0.0.0.0, or if this keyword and its IP address specification are not present, the filter matches all IP packets.
<proto>	<proto> indicates a protocol that you can specify as a name or a number. The filter applies to packets whose protocol field matches this value.The supported names and numbers are icmp (1), tcp (6), udp (17), and ospf (89). If you set <proto> to 0 (zero), the filter matches any protocol.

Table B-6. IP data filter syntax elements

Keyword or argument	Description
dstport <cmp> <value>	"dstport" is a keyword indicating "destination port." This argument is valid only when the protocol is tcp (6) or udp (17). If you do not specify a destination port, the filter matches any port. <cmp> is an argument indicating how to compare the specified value to the actual destination port. It can have the value <, =, >, or !=. <value> can be a number or a name. Supported names and numbers are ftp-data (20), ftp (21), telnet (23), smtp (25), nameserver (42), domain (53), tftp (69), gopher (70), finger (79), www (80), kerberos (88), hostname (101), nntp (119), ntp (123), exec (512), login (513), cmd (514), and talk (517).
srcport <cmp> <value>	"srcport" is a keyword indicating "source port." It is valid only when the protocol is tcp (6) or udp (17). If you do not specify a source port, the filter matches any port. <cmp> is an argument indicating how to compare the specified value to the actual source port. It can have the value <, =, >, or !=. <value> can be a number or a name. Supported names and numbers are ftp-data (20), ftp (21), telnet (23), smtp (25), nameserver (42), domain (53), tftp (69), gopher (70), finger (79), www (80), kerberos (88), hostname (101), nntp (119), ntp (123), exec (512), login (513), cmd (514), and talk (517).
<est>	If you set this argument to 1, the filter matches a packet only if a TCP session is already established. It is valid only when the <proto> specification is tcp (6).

sensitive.

Generic data filter entries

Use this format for a generic data filter entry:

```
Ascend-Data-Filter="generic <dir> <action> <offset> <mask>
<value> <compare> [<more>]"
```

Note: A filter definition cannot contain newlines. The syntax is shown on multiple lines here for printing purposes only.

Table B-7 describes each element of the syntax. None of the keywords are case sensitive.

Table B-7. Generic data filter syntax elements

Keyword or argument	Description
generic	The keyword “generic” indicates a generic filter.
<dir>	The <dir> argument indicates filter direction. You can specify “in” (to filter packets coming into the MAX) or “out” (to filter packets going out of the MAX).
<action>	<action> indicates what action the MAX should take with a packet that matches the filter. You can specify either “forward” or “drop”.
<offset>	<offset> indicates the number of bytes masked from the start of the packet. The byte position specified by <offset> is called the byte-offset. Starting at the position specified by <offset>, the MAX applies the value of the <mask> argument. A mask hides the part of a number that appears behind the binary zeroes in the mask; for example, if you set <mask> to ffff0000 in hexadecimal format, the filter uses only the first 16 binary digits in the comparison, since f=1111 in binary format. The unit then compares the unmasked portion of the packet with the value specified by the <value> argument.

Table B-7. Generic data filter syntax elements

Keyword or argument	Description
<mask>	This argument indicates which bits to compare in a segment of the packet; the mask cannot exceed 6 bytes (12 hexadecimal digits). A one-bit in the mask indicates a bit to compare; a zero-bit indicates a bit to ignore. The length of the mask specifies the length of the comparison.
<value>	This argument indicates the value to compare to the packet contents at the specified offset in the packet. The length of the value must be the same as the length of the mask; otherwise, the MAX ignores the filter.
<compare>	This argument indicates how the MAX compares a packet's contents to the value specified by <value>. You can specify == or !=, for Equal or NotEqual. The default value is Equal.
<more>	If present, this argument specifies whether the MAX applies the next filter definition in the profile to the current packet before making the Forward or Drop decision. The <dir> and <action> values of the next entry must be the same as the <dir> and <action> of the current entry; otherwise, the MAX ignores the <more> flag.

Example: These are examples of IP data filter entries:

```
Ascend-Data-Filter="ip in drop"

Ascend-Data-Filter="ip out forward tcp"

Ascend-Data-Filter="ip out forward tcp dstip 10.0.200.3/16
srcip 10.0.200.25/16 dstport!=telnet"

Ascend-Data-Filter="ip out forward tcp dstip 10.0.200.3/16
srcip 10.0.200.25/16 icmp"
```

Note: A filter definition cannot contain newlines. The syntax is shown on multiple lines here for printing purposes only.

These are examples of generic data filter entries:

```
Ascend-Data-Filter="generic in drop 0 ffff 0080"
Ascend-Data-Filter="generic in drop 0 ffff != 0080 more"
Ascend-Data-Filter="generic in drop 16 ff aa"
```

Ascend-Data-Rate (Attribute197)

Description: This attribute specifies the data rate of the connection in bits per second.

Ascend-Data-Rate is included in an Accounting-Request packet when both of these conditions are true:

- The session has ended or has failed to authenticate (Acct-Status-Type=Stop).
- The Auth parameter is not set to RADIUS/LOGOUT.

Usage: Ascend-Data-Rate does not appear in a user profile. Its default value is 0 (zero).

Ascend-Data-Svc (247)

Description: This attribute specifies the type of data service the link uses for outgoing calls.

Usage: The data service you specify must be available end-to-end. You can set the Ascend-Data-Svc attribute to one of the values listed in Table B-8

Table B-8. Ascend-Data-Svc settings

Setting	Description
Switched-Voice-Bearer (0)	This value applies only to calls made over an ISDN BRI or T1 PRI line. When you specify this setting, the MAX enables the network to place an end-to-end digital voice call for transporting data when a switched data service is not available.

Table B-8. Ascend-Data-Svc settings

Setting	Description
Switched-56KR (1)	The call contains restricted data, guaranteeing that the data the MAX transmits meets the density restrictions of D4-framed TI lines. D4 specifies the D4 format, also known as the Superframe format, for framing data at the physical layer. This format consists of 12 consecutive frames, separated by framing bits. The call connects to the Switched-56 data service. The only services available to lines using inband signaling (T1 access lines containing one or more switched channels, and Switched-56 lines) are Switched-56K and Switched-56KR.
Switched-64K (2)	The call contains any type of data and connects to the Switched-64 data service.
Switched-64KR (3)	The call contains restricted data and connects to the Switched-64 data service.
Switched-56K (4)	The call contains any type of data and connects to the Switched-56 data service. The only services available to lines using inband signaling (T1 access lines containing one or more switched channels, and Switched-56 lines) are Switched-56K and Switched- 56KR. For most T1 PRI lines, select Switched-56K.
Nailed-56KR (1)	The call contains restricted data and connects to the Nailed-56 data service.
Nailed-64K (2)	The call contains any type of data and connects to the Nailed-64 data service.

Dependencies: Keep this additional information in mind:

- You can determine the base bandwidth of a call by multiplying the value of the Ascend-Base-Channel-Count attribute by the value of the Ascend-Data-Svc attribute.

- Either party can request a data service that is unavailable; in this case, the MAX cannot connect the call.

Ascend-DBA-Monitor (171)

Description: This attribute species how the Ascend calling unit monitors the traffic on an MP+ call. The Ascend unit can use this information to add or subtract bandwidth as needed.

Usage: You can specify one of these values:

- DBA-Transmit (0)

  This setting indicates that the MAX adds or subtracts bandwidth based on the amount of data it transmits.

  Transmit is the default.
- DBA-Transmit-Recv (1)

  This setting indicates that the MAX adds or subtracts bandwidth based on the amount of data it transmits *and* receives.
- DBA-None (2)

  This setting indicates that the MAX does not monitor traffic over the link.

Dependencies: Keep this additional information in mind:

- Ascend-DBA-Monitor is supported only on MP+ calls.
- If both sides of the link have Ascend-DBA-Monitor set to None, Dynamic Bandwidth Allocation is disabled.

Ascend-Dec-Channel-Count (237)

Description: This attribute specifies the number of channels the MAX removes when bandwidth changes either manually or automatically during a call.

Usage: Specify a number between 1 and 32. The default value is 1.

Dependencies: Keep this additional information in mind:

- Ascend-Dec-Channel-Count does not apply if all channels of a link are nailed up
  (Ascend-Call-Type=Nailed).

- Ascend-Dec-Channel-Count applies only when the link is using MP+ encapsulation (Framed-Protocol=MPP).
- You cannot clear a call by decrementing channels.

Ascend-Dial-Number (227)

Description: This attribute specifies the phone number the MAX dials to reach the bridge, router, or node at the remote end of the link.

Usage: Specify a telephone number. You can enter up to 20 characters, and you must limit those characters to the following:

```
1234567890()[]!z-*#|
```

The MAX sends only the numeric characters to place a call. The default value is null.

If Use Trunk Grps=Yes in the System Profile, the first digits in the Ascend-Dial-Number attribute have the meanings listed in Table B-9.

Table B-9. Ascend-Dial-Number digits

Digit	Explanation
First digit is between 4 and 9.	The MAX places the call over the corresponding trunk group listed in the Ch *n* Trnk Grp, B1 Trnk Grp, or B2 Trnk Grp parameters in the Line Profile. If Dial Plan=Trunk Grp, the digits following the first digit constitute an ordinary phone number. If Dial Plan=Extended, the next two digits specify the Dial Plan Profile containing the parameters the MAX uses when making the call. These parameters constitute the extended dial plan. An ordinary phone number follows these two digits.
First digit is 3.	The MAX places the call to a destination listed in a Destination Profile. In this case, the second and third digits indicate the number of the Destination Profile.

Table B-9. Ascend-Dial-Number digits

Digit	Explanation
First digit is 2.	The MAX places the call between host ports on the same MAX, or between TEs (Terminal Equipment) on a local ISDN BRI line on the same MAX. The first type of call is a port-to-port call; the latter type of call is a TE-to-TE call. In a port-to-port call, the second digit indicates the slot of a serial host port module. In a TE-to-TE call, the second digit indicates the slot of a Host/BRI module. If you enter 0 (zero) for the second digit, the call connects to any available serial host port and ignores the third digit. If you enter a nonzero value for the second digit, the third digit selects the serial host port (for a port-to-port call) or a local ISDN BRI port (for a TE-to-TE call). If you enter 0 (zero) for the third digit, the call connects to any available serial host port or local ISDN BRI line in the module selected by the second digit.

Ascend-Disconnect-Cause (195)

Description: This attribute specifies the reason a connection was taken offline.

Ascend-Disconnect-Cause is included in an Accounting-Request packet when both of these conditions are true:

- The session has ended or has failed to authenticate (Acct-Status-Type=Stop).
- The Auth parameter is not set to RADIUS/LOGOUT.

Usage: Ascend-Disconnect-Cause can return any of the values listed in Table B-10.

Table B-10. Ascend-Disconnect-Cause codes

Code	Description
0	No reason.

Table B-10. Ascend-Disconnect-Cause codes

Code	Description
1	The event was not a disconnect.
2	The reason for the disconnect is unknown. This code can appear when the remote connection goes down.
3	The call has been disconnected.
4	CLID authentication has failed.
These codes can appear if a disconnect occurs during the initial modem connection.	
10	The modem never detected DCD.
11	The modem detected DCD, but became inactive.
12	The result codes could not be parsed.
These codes are related to immediate Telnet and raw TCP disconnects during a terminal server session.	
20	The user exited normally from the terminal server.
21	The user exited from the terminal server because the idle timer expired.
22	The user exited normally from a Telnet session.
23	The user could not switch to SLIP or PPP because the remote host had no IP address or because the dynamic pool could not assign one.
24	The user exited normally from a raw TCP session.
25	The login process was terminated because the user failed to enter a correct password after three attempts.
26	The raw TCP option is not enabled.
27	The login process was terminated because the user typed Ctrl-C.

Table B-10. Ascend-Disconnect-Cause codes

Code	Description
28	The terminal server session was terminated.
29	The user closed the virtual connection
30	The virtual connection was terminated.
31	The user exited normally from an Rlogin session
32	The user selected an invalid Rlogin option.
33	The MAX has insufficient resources for the terminal server session.
These codes concern PPP connections.	
40	PPP LCP negotiation timed out while waiting for a response from a peer.
41	There was a failure to converge on PPP LCP negotiations.
42	PPP PAP authentication failed.
43	PPP CHAP authentication failed.
44	Authentication failed from the remote server.
45	The peer sent a PPP Terminate Request.
46	LCP got a close request from the upper layer while LCP was in an open state.
47	LCP closed because no NCPs were opened.
48	LCP closed because it could not determine to which MP bundle it should add the user.
49	LCP closed because no more channels could be added to an MP session.

Table B-10. Ascend-Disconnect-Cause codes

Code	Description
These codes are related to immediate Telnet and raw TCP disconnects, and contain more specific information that the Telnet and TCP codes listed earlier in this table.	
50	The Raw TCP or Telnet internal session tables are full.
51	Internal resources are full.
52	The IP address for the Telnet host is invalid.
53	The hostname could be resolved.
54	A bad or missing port number was detected.
These disconnect codes are returned by the TCP stack during an immediate Telnet or raw TCP session.	
60	The host reset the TCP connection.
61	The host refused the TCP connection.
62	The TCP connection timed out.
63	A foreign host closed the TCP connection.
64	The TCP network was unreachable.
65	The TCP host was unreachable.
66	The TCP network was administratively unreachable.
67	The TCP host was administratively unreachable.
68	The TCP port was unreachable.
These are additional disconnect codes.	
100	The session timed out because there was no activity on a PPP link.

Table B-10. Ascend-Disconnect-Cause codes

Code	Description
101	The session failed for security reasons.
102	The session was terminated for callback.
120	The call was refused because the protocol was disabled or unsupported.
150	RADIUS requested the disconnect.
160	The allowed retries for V.110 synchronization have been exceeded.
170	PPP authentication has timed out.

Ascend-First-Dest (189)

Description: This attribute records the destination IP address of the first packet received on a link after RADIUS authenticates the connection.

Ascend-First-Dest is included in an Accounting-Request packet when all of these conditions are met:

- The session has been authenticated.
- The session has ended (Acct-Status-Type=Stop).
- The Auth parameter is not set to RADIUS/LOGOUT.

Usage: Ascend-First-Dest does not appear in a user profile and has no default value.

Dependencies: This attribute only applies if the session has been configured to route IP.

Ascend-Force-56 (248)

Description: This attribute specifies whether the MAX uses only the 56-kbps portion of a channel, even when all 64 kbps appear to be available:

Usage: You can specify one of these values:

- Force-56-No

  This setting indicates that the MAX should use the entire 64 kbps (when available). Force-56-No is the default.

- Force-56-Yes

  This setting specifies that the MAX should use only the 56-kbps portion of a channel.

  Set Ascend-Force-56=Force=56-Yes when you place calls to European or Pacific Rim countries from within North America and the complete path cannot distinguish between the Switched-56 and Switched-64 data services. This feature is not required if you are placing calls only within North America.

Ascend-FR-Circuit-Name (156)

Description: This attribute specifies the PVC (Permanent Virtual Connection) for which the user profile is an endpoint. A circuit specification defines two DLCI endpoints of a PVC, with one endpoint specified in each RADIUS user profile (or Connection Profile).

Usage: Specify a text string containing up to 15 characters. The default value is null.

Dependencies: Keep this additional information in mind:

- You can specify Ascend-FR-Circuit-Name only when Framed-Protocol=FR-CIR.
- You can specify Ascend-FR-Circuit-Name only for a gateway connection (when Ascend-FR-Direct=FR-Direct-No).
- Two profiles are required for a single PVC.

  You can use two RADIUS user profiles, two Connection Profiles, or one RADIUS user profile and one Connection Profile. The two DLCIs can use the same Frame Relay Profile or different ones.

- Pairs of links with matching Ascend-FR-Circuit-Name attributes (or Circuit parameters) are switched to each other; therefore, make sure that you specify the exact same name for Ascend-FR-Circuit-Name or the Circuit parameter in each profile.

Ascend-FR-DCE-N392 (162)

Description: This attribute specifies the number of errors during Ascend-FR-DCE-N393-monitored events that cause the network side to declare the user side's procedures inactive.

Usage: Specify an integer between 1 and 10. The default value is 3.

Dependencies: Keep this additional information in mind:

- Set Ascend-FR-DCE-N392 to a value less than Ascend-FR-DCE-N393.
- Ascend-FR-DCE-N392 does not apply if Ascend-FR-Type=Ascend-FR-DTE.

Ascend-FR-DCE-N393 (164)

Description: This attribute indicates the DCE-monitored event count. A link is always considered active if the value of Ascend-FR-DCE-N393 is not reached.

Usage: Specify a number between 1 and 10. The default value is 4.

Dependencies: This attribute does not apply if Ascend-FR-Type=Ascend-FR-DTE.

Ascend-FR-Direct (219)

Description: This attribute specifies whether the MAX uses a gateway connection or a redirect connection for frame relay packets.

Usage: You can specify one of these values:

- FR-Direct-No (0) indicates that the MAX uses a gateway connection.

  A gateway connection is a bridging or routing link between the MAX and a remote site via a frame relay switch. When the MAX receives IP packets

destined for that site, it encapsulates the packets in frame relay (RFC 1490) and forwards the data stream out to the frame relay switch using the DLCI (Data Link Connection Indicator) specified by Ascend-FR-DLCI. The frame relay switch uses the DLCI to route the frames to the right destination.

FR-Direct-No is the default.

- FR-Direct-Yes (1) indicates that the MAX uses a redirect connection.

  A redirect connection is designed only for forwarding incoming switched calls that use IP routing, such as regular PPP or MP+ calls. When the MAX receives IP packets from a caller that has a redirect specified in its RADIUS user profile, it simply forwards the data stream out to the frame relay switch using the DLCI (Data Link Connection Indicator) specified by Ascend-FR-Direct-DLCI. In so doing, the MAX effectively passes on the responsibility of routing those packets to a later hop on the frame relay network. The MAX never examines the destination address of redirect packets.

Ascend-FR-Direct-DLCI (221)

Description: This attribute specifies the DLCI (Data Link Connection Indicator) for the user profile in a frame relay redirect connection. The DLCI identifies the user profile to the frame relay switch as a logical link on a physical circuit.

Usage: Specify an integer between 16 and 991. The default value is 16. Many redirect connections can use the same DLCI.

Dependencies: Ascend-FR-Direct-DLCI applies only if Ascend-FR-Direct=FR-Direct-Yes.

Example: This portion of a user profile shows a redirect connection configured using DLCI 21 and the Frame Relay Profile called “Montgomery”.

```
permconn-max-1 Password="ascend", Service-Type=Outbound
    User-Name="Phani-gw-1",
   Ascend-FR-Direct=FR-Direct-Yes,
   Ascend-FR-Direct-Profile="Montgomery",
   Ascend-FR-Direct-DLCI=21,
   Metric=2,
   ...
```

Ascend-FR-Direct-Profile (220)

Description: This attribute specifies the name of the Frame Relay Profile that carries the redirect connection.

Usage: Indicate the name of a Frame Relay Profile that connects to the frame relay switch handling the DLCI (Data Link Connection Indicator) specified by Ascend-FR-Direct-DLCI. You can specify up to 15 alphanumeric characters. The default value is null. Make sure that you enter the name exactly as it appears in the Name parameter of the Frame Relay Profile.

Dependencies: Ascend-FR-Direct-Profile applies only if Ascend-FR-Direct=FR-Direct-Yes.

Example: This portion of a user profile shows a redirect connection configured using DLCI 21 and the Frame Relay Profile called “Montgomery”.

```
permconn-max-1 Password="ascend", Service-Type=Outbound
    User-Name="Phani-gw-1",
   Ascend-FR-Direct=FR-Direct-Yes,
   Ascend-FR-Direct-Profile="Montgomery",
   Ascend-FR-Direct-DLCI=21,
   Metric=2,
   ...
```

Ascend-FR-DLCI (179)

Description: This attribute specifies the DLCI (Data Link Connection Indicator) for the user profile in a frame relay gateway connection. The DLCI identifies the user profile to the frame relay switch as a logical link on a physical circuit.

Usage: Specify an integer between 16 and 991. The default value is 16. You must assign each gateway connection its own DLCI.

Dependencies: Ascend-FR-DLCI applies only if Ascend-FR-Direct=FR-Direct-No.

Example: This portion of a user profile shows a gateway connection configured using DLCI 21 and the Frame Relay Profile called “Florence”.

```
permconn-max-1 Password="ascend", Service-Type=Outbound
    User-Name="Phani-gw-1",
```

```
Ascend-FR-Direct=FR-Direct-No,
Ascend-FR-Profile-Name="Florence",
Ascend-FR-DLCI=21,
Metric=2,
...
```

Ascend-FR-DTE-N392 (163)

Description: This attribute specifies the number of errors during Ascend-FR-DTE-N393-monitored events that cause the user side to declare the network side's procedures inactive.

Usage: Specify an integer between 1 and 10. The default value is 3.

Dependencies: Keep this additional information in mind:

- Set Ascend-FR-DTE-N392 to a value less than Ascend-FR-DTE-N393.
- Ascend-FR-DTE-N392 does not apply if Ascend-FR-Type=Ascend-FR-DCE.

Ascend-FR-DTE-N393 (165)

Description: This attribute indicates the DTE-monitored event count. A link is always considered active if the value of Ascend-FR-DTE-N393 is not reached.

Usage: Specify a number between 1 and 10. The default value is 4.

Dependencies: This attribute does not apply if Ascend-FR-Type=Ascend-FR-DCE.

Ascend-FR-Link-Mgt (160)

Description: In a Frame Relay Profile, this attribute specifies the link management protocol used between the MAX and the frame relay switch.

Usage: You can specify one of these values:

- Ascend-FR-No-Link-Mgt (0)

This setting indicates no link management, and is the default. A link is always considered active if no link management functions are performed.

- Ascend-FR-T1-617D (1)
  This setting indicates T1.617 Annex D link management.
- Ascend-FR-Q-933A (2)
  This setting indicates Q.933 Annex A link management.

Ascend-FR-LinkUp (157)

Description: In a Frame Relay Profile, this attribute specifies whether the frame relay link comes up automatically.

Usage: You can specify one of these values:

- Ascend-LinkUp-Default (0)
  This setting indicates that the datalink does not come up unless a DLCI brings it up, and shuts down after the last DLCI has been removed. This value is the default.
- Ascend-LinkUp-AlwaysUp (1)
  This setting indicates that the datalink comes up automatically and stays up even when the last DLCI has been removed.

Dependencies: You can start and drop frame relay connections by using the DO DIAL and DO HANGUP commands. DO DIAL brings up a connection. DO HANGUP closes the link and any DLCIs on it. If Ascend-FR-LinkUp=Ascend-LinkUp-AlwaysUp, DO HANGUP brings the link down, but the link automatically restarts. A restart also occurs if a DLCI brings up the datalink.

Ascend-FR-N391 (161)

Description: In a Frame Relay Profile, this attribute specifies the interval in seconds at which the MAX requests a Full Status Report.

If the frame relay link is configured for link management, it regularly request updates on the status of the link. The frame relay unit at the other end of the link must respond to these requests; otherwise, the MAX considers the link inactive. Furthermore, if the response to these requests indicates a DLCI failure, the MAX considers the link inactive.

Usage: Specify an integer between 1 and 255. The default value is 6.

Dependencies: This attribute does not apply if Ascend-FR-Type=Ascend-FR-DCE.

Ascend-FR-Nailed-Grp (158)

Description: This attribute associates a group of nailed-up channels with the Frame Relay Profile.

Usage: Specify a number between 1 and the maximum number of nailed-up channels that your MAX allows. The default value is 1.

Dependencies: Do not associated a group with more than one active Frame Relay Profile.

Ascend-FR-Profile-Name (180)

Description: This attribute specifies the name of the Frame Relay Profile that carries the gateway connection.

Usage: Indicate the name of a Frame Relay Profile that connects to the frame relay switch handling the DLCI (Data Link Connection Indicator) specified by Ascend-FR-DLCI. You can specify up to 15 alphanumeric characters. The default value is null. Make sure that you enter the name exactly as it appears in the Name parameter of the Frame Relay Profile.

Dependencies: Ascend-FR-Profile-Name applies only if Ascend-FR-Direct=FR-Direct-No.

Example: This portion of a user profile shows a gateway connection configured using DLCI 21 and the Frame Relay Profile called “Florence”.

```
permconn-max-1 Password="ascend", Service-Type=Outbound
    User-Name="Phani-gw-1",
   Ascend-FR-Direct=FR-Direct-No,
   Ascend-FR-Profile-Name="Florence",
   Ascend-FR-DLCI=21,
   Metric=2,
   ...
```

Ascend-FR-T391 (166)

Description: This attribute indicates the Link Integrity Verification polling timer.

Usage: You can specify a number of seconds between 5 and 30. The default value is 10.

Dependencies: This attribute does not apply if Ascend-FR-Type=Ascend-FR-DCE.

Ascend-FR-T392 (167)

Description: This attribute indicates the timer for the verification of the polling cycle— the length of time the unit should wait between Status Enquiry messages. An error is recorded if no Status Enquiry is received within the number seconds specified by this attribute.

Usage: Specify a number of seconds between 5 and 30. The default value is 10.

Dependencies: This attribute does not apply if Ascend-FR-Type=Ascend-FR-DTE.

Ascend-FR-Type (159)

Description: This attribute specifies the type of frame relay connection used by the Frame Relay Profile.

You can specify one of these values:

- Ascend-FR-DTE (0)
  This setting indicates a UNI-DTE interface. This value is the default. When you specify this value, the MAX performs DTE functions for link management, and can connect to a frame relay DCE unit—a frame relay switch.
  Choose this setting when Framed-Protocol=FR in a user profile for a gateway connection.
- Ascend-FR-DCE (1)

This setting indicates a UNI-DCE interface. When you specify this value, the MAX performs DCE functions for link management, and can connect to a frame relay DTE unit—the user's CPE (Customer Premises Equipment).

Choose this setting when Framed-Protocol=FR-CIR in a user profile for a gateway connection.

- Ascend-FR-NNI (2)

  This setting indicates an NNI interface. When you specify this value, the MAX performs both DTE and DCE functions for link management, and can connect to another NNI unit.

  Choose this setting when Framed-Protocol=FR-CIR in a user profile for a gateway connection.

Dependencies: Ascend-FR-Type is applicable only when a frame relay user profile specifies a gateway connection (Ascend-FR-Direct=FR-Direct-No) and Framed-Protocol=FR or FR-CIR.

Ascend-FT1-Caller (175)

Description: This attribute specifies whether the MAX initiates an FT1-AIM or an
FT1-B&O call, or whether it waits for the remote end to initiate these types of calls.

Usage: You can specify one of these values:

- FT1-No (0) specifies that the MAX waits for the remote end to initiate the call.

  FT1-No is the default.

- FT1-Yes (1) specifies that the MAX initiates the call.

  If you choose this setting, the MAX dials to bring online any switched circuits that are part of the call.

Dependencies: Keep this additional information in mind:

- If the remote end has set the Ascend-FT1-Caller attribute to FT1-No (or set the FT1 Caller parameter to No), set Ascend-FT1-Caller to FT1-Yes for the local MAX.

- If the remote end has set the Ascend-FT1-Caller attribute to FT1-Yes (or set the FT1 Caller parameter to Yes), set Ascend-FT1-Caller to FT1-No for the local MAX.

Ascend-Group (178)

Description: This attribute points to the nailed-up channels used by the profile's WAN link.

If you set the Ascend-Group attribute to a value that matches the settings of a Ch *n* Prt/Grp, B1 Prt/Grp, or B2 Prt/Grp parameter in a Line Profile, the MAX uses the specified channels for this profile's link across the WAN. Similarly, if Ascend-Group has the same value as Nailed Grp in the Serial WAN Profile, the MAX uses the serial WAN circuit for this profile's link.

Usage: Your usage depends upon the value you specify for the Ascend-Call-Type attribute:

- If you set Ascend-Call-Type to Nailed, you can specify a number between 1 and 60 for Ascend-Group.

  The default value is 1.

- If you set Ascend-Call-Type to Nailed/Mpp, you can use the Ascend-Group attribute to assign multiple nailed-up groups to the profile.

  Specify a single number, or specify a list of numbers between 1 and 60, separated by commas. Do not include spaces. The default value is 1.

Dependencies: Keep this additional information in mind:

- The Ascend-Group attribute does not apply if the link consists entirely of switched channels.
- If you add channels for the Ascend-Group attribute, the MAX adds the additional channels to any online connection that uses the group.
- Do not duplicate group numbers in active profiles—that is, choose a value for Ascend-Group that is not used by any other active Connection Profile, Call Profile, Frame Relay Profile, or RADIUS user profile.
- Although you can assign multiple groups to a user profile, do not mix the Serial WAN circuit with nailed-up BRI or T1/E1 channels.

Example: If Ascend-Call-Type=Nailed/Mpp, setting the Ascend-Group attribute to “1,3,5,7” assigns four nailed-up groups to the profile.

Ascend-Handle-IPX (222)

Description: This attribute specifies how the MAX handles NCP watchdog requests on behalf of IPX clients during IPX bridging.

Usage: You can specify one of these values:

- Handle-IPX-None (0)

  This setting indicates that special IPX behavior does not take place. Choose this setting when the LAN on each side of the bridge has one or more IPX servers.

  Handle-IPX-None is the default.

- Handle-IPX-Client (1)

  This setting indicates that the MAX discards RIP (Routing Information Protocol) and SAP
  (Service Advertising Protocol) periodic broadcasts at its WAN interface, but forwards RIP and SAP queries.

  The WAN interface is the port on the MAX that is connected to a WAN line. RIP and SAP queries enable a client workstation to locate a NetWare server across the network. Choose this setting when both these conditions are true:

  - The local LAN has IPX clients but no servers.
  - The MAX is acting as a bridge to another LAN containing only IPX servers or a combination of IPX servers and clients.

- Handle-IPX-Server (2)

  This setting indicates that the MAX discards all RIP (Routing Information Protocol) and SAP (Service Advertising Protocol) periodic broadcasts and queries at its WAN interface.

  This mode enables the MAX to bring down calls during idle periods without breaking
  client/server or peer-to-peer connections.

  Ordinarily, when a NetWare server does not receive a reply to the watchdog session
  keepalive packets it sends to a client, it closes the connection. When you specify Handle-IPX-Server, however, the MAX replies to NCP watchdog

requests on behalf of clients on the other side of the bridge; in other words, the MAX tricks the server watchdog process into believing that the link is still active. This process is called watchdog spoofing.

Choose this setting when both these conditions are true:

- The MAX is acting as a bridge to a remote LAN with IPX clients, but no servers.
- The local LAN contains only IPX servers, or a combination of IPX clients and
  servers.

Dependencies: Keep this additional information in mind:

- If you specify Ascend-Handle-IPX=Handle-IPX-Server, you must also specify a value for the Ascend-Netware-timeout attribute, indicating the maximum length of idle time during which the MAX performs watchdog spoofing for NetWare connections.
- If the connection does not bridge (Ascend-Bridge=Bridge-No), the Ascend-Handle-IPX attribute does not apply.
- If the MAX on one LAN sets Ascend-Handle-IPX=Handle-IPX-Server and the LAN on the other side of the connection has only NetWare clients, the MAX on the client-only LAN should set Ascend-Handle IPX=Handle-IPX-Client.

  If both LANs contain servers, both sides of the connection should set Ascend-Handle- IPX=Handle-IPX-None.
- Although Ascend-Handle-IPX does not apply if Ascend-Bridge=Bridge-No, the MAX automatically performs watchdog spoofing just as though you had set Ascend-Handle-IPX=Handle-IPX-Server; however, the MAX does not filter as though you had set Ascend-Handle-IPX=Handle-IPX-Server.

Example: This user profile specifies an IPX bridging link in which the local Ethernet supports NetWare clients, and the remote network supports both NetWare servers and clients:

```
MAX1 Password="m2dan", Service-Type=Framed
     Framed-Protocol=PPP,
     Ascend-Route-IPX=Route-IPX-No,
     Ascend-Bridge=Bridge-Yes,
     Ascend-Handle-IPX=Handle-IPX-Client,
     Ascend-Netware-timeout=30
```

Ascend-History-Weigh-Type (239)

Description: This attribute specifies which Dynamic Bandwidth Allocation (DBA) algorithm to use for calculating average line utilization (ALU) of transmitted data. DBA enables you to specify that the MAX uses ALU as the basis for automatically adding or subtracting bandwidth from a switched connection without terminating the link.

Usage: Figure B-1 illustrates the differences between the algorithms you can choose.

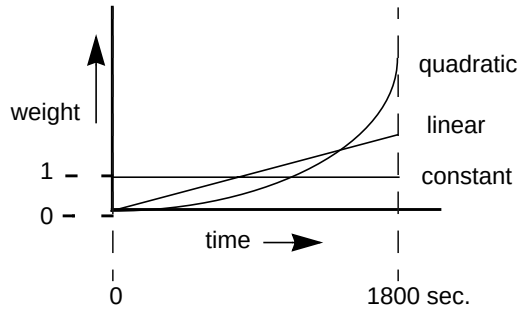


Figure B-1. Bandwidth algorithms for MP+ calls

- History-Constant (0) gives equal weight to all samples taken during the historical time period specified by the Ascend-Seconds-Of History attribute.

  When you select this option, older historical samples have as much impact on the decision to change bandwidth allocation as do more recent samples.
- History-Linear (1) gives more weight to recent samples of bandwidth usage than to older samples taken during the historical period specified by Ascend-Seconds-Of-History.

  The weighting grows at a linear rate.
- History-Quadratic (2) gives more weight to recent samples of bandwidth usage than to older samples taken during the historical period specified by the Ascend-Seconds-Of-History attribute.

  The weighting grows at a quadratic rate. History-Quadratic is the default.

Ascend-Home-Agent-IP-Addr (183)

Description: In a mobile node's RADIUS user profile, this attribute indicates the IP address of the home agent under ATMP (Ascend Tunnel Management Protocol) operation.

The RADIUS server passes the attributes contained in the mobile node's RADIUS user profile to the foreign agent; the foreign agent sends these attributes when connecting with the home agent.

A mobile node can also connect directly to the home agent. An ATMP-based RADIUS entry that is local to the home agent enables the mobile node to bypass a foreign agent connection, but does not preclude a foreign agent. If both the home agent and the foreign agent have local RADIUS entries for the mobile node, the node can choose between a direct connection or a tunneled connection through the foreign agent.

Usage: Specify an IP address in dotted decimal notation. An IP address consists of four numbers between 0 and 255, separated by periods. The default value is 0.0.0.0.

Example: The following RADIUS entry authenticates a mobile NetWare client that connects directly to the home agent. In this example, the home agent is configured in gateway mode; it forwards packets from the mobile node across a nailed WAN link to the home IPX network.

```
mobile-ipx Password="unit"
        Service-Type=Framed,
        Ascend-Route-IPX=Route-IPX-Yes,
        Framed-Protocol=PPP,
        Ascend-IPX-Peer-Mode=IPX-Peer-Dialin,
        Framed-IPX-Network=40000000,
        Ascend-IPX-Node-Addr=12345678,
        Ascend-Home-Agent-IP-Addr=200.168.6.18,
        Ascend-Home-Network-Name="dave's max",
        Ascend-Home-Agent-Password="pipeline"
```

Ascend-Home-Agent-Password (184)

Description: In a mobile node's RADIUS user profile, this attribute specifies the password that the foreign agent sends to the home agent in order to authenticate itself during ATMP (Ascend Tunnel Management Protocol) operation. This password must match the value of the Password parameter in the ATMP configuration in the Ethernet Profile for the home agent. All mobile nodes accessing a single home agent must specify the same password.

The RADIUS server passes the attributes contained in the mobile node's RADIUS user profile to the foreign agent; the foreign agent sends these attributes when connecting with the home agent.

A mobile node can also connect directly to the home agent. An ATMP-based RADIUS entry that is local to the home agent enables the mobile node to bypass a foreign agent connection, but does not preclude a foreign agent. If both the home agent and the foreign agent have local RADIUS entries for the mobile node, the node can choose between a direct connection or a tunneled connection through the foreign agent.

Usage: Specify a text string containing up to 20 characters. The default value is null.

Example: The following RADIUS entry authenticates a mobile NetWare client that connects directly to the home agent. In this example, the home agent is configured in gateway mode; it forwards packets from the mobile node across a nailed WAN link to the home IPX network.

```
mobile-ipx Password="unit"
        Service-Type=Framed,
        Ascend-Route-IPX=Route-IPX-Yes,
        Framed-Protocol=PPP,
        Ascend-IPX-Peer-Mode=IPX-Peer-Dialin,
        Framed-IPX-Network=40000000,
        Ascend-IPX-Node-Addr=12345678,
        Ascend-Home-Agent-IP-Addr=200.168.6.18,
        Ascend-Home-Network-Name="dave's max",
        Ascend-Home-Agent-Password="pipeline"
```

Ascend-Home-Agent-UDP-Port (186)

Description: In a mobile node's RADIUS user profile, this attribute specifies the UDP port number on the home agent to which the foreign agent directs ATMP (Ascend Tunnel Management Protocol) messages.

Usage: Specify a UDP port number between 0 and 65535. The default value is 5150.

Ascend-Home-Network-Name (185)

Description: In a mobile node's RADIUS user profile, this attribute specifies the name of the Connection Profile on which the home agent sends all packets it receives from the mobile node during ATMP (Ascend Tunnel Management Protocol) operation.

The RADIUS server passes the attributes contained in the mobile node's RADIUS user profile to the foreign agent; the foreign agent sends these attributes when connecting with the home agent.

A mobile node can also connect directly to the home agent. An ATMP-based RADIUS entry that is local to the home agent enables the mobile node to bypass a foreign agent connection, but does not preclude a foreign agent. If both the home agent and the foreign agent have local RADIUS entries for the mobile node, the node can choose between a direct connection or a tunneled connection through the foreign agent.

Usage: Specify the name of the home agent's Connection Profile. The default value is null.

Dependencies: You must specify a value for this attribute only if the home agent is a gateway (that is, only if Type=Gateway in the ATMP configuration for the Ethernet Profile).

Example: The following RADIUS entry authenticates a mobile NetWare client that connects directly to the home agent. In this example, the home agent is configured in gateway mode; it forwards packets from the mobile node across a nailed WAN link to the home IPX network.

```
mobile-ipx Password="unit"
       Service-Type=Framed,
```

```
Ascend-Route-IPX=Route-IPX-Yes,
Framed-Protocol=PPP,
Ascend-IPX-Peer-Mode=IPX-Peer-Dialin,
Framed-IPX-Network=40000000,
Ascend-IPX-Node-Addr=12345678,
 Ascend-Home-Agent-IP-Addr=200.168.6.18,
 Ascend-Home-Network-Name="dave's max",
 Ascend-Home-Agent-Password="pipeline"
```

Ascend-Host-Info (252)

Description: This attribute specifies a list of hosts to which a user can establish a Telnet session.

Usage: You can specify up to 10 Ascend-Host-Info entries in a user profile. Enter your attribute settings in this format:

Ascend-Host-Info="<IP_address> <text>**"**

- <IP_address> specifies the IP address of each host.

  Specify an IP address in dotted decimal notation. An IP address consists of four numbers between 0 and 255, separated by periods. The default value is 0.0.0.0.

- <text> describes each host.

  You can enter up to 31 characters for <text>. The default value is null. The RADIUS server assigns the text a number; when the user selects the number, the terminal server initiates a Telnet session with the host at the specified IP address.

Dependencies: If you specify a value for the Ascend-Host-Info attribute, you must also make these settings in the TServ Options menu of the Ethernet Profile:

- Set Initial Scrn=Menu or Toggle Scrn=Yes.
- Set Remote Conf=Yes.

Example: Here is an example for a MAX named Cal:

```
initial-banner-Cal Password="ascend", Service-Type=Outbound
     Reply-Message="Up to 16 lines of up to 80 characters
each",
     Reply-Message="will be accepted. Long lines will be
truncated",
```

```
Reply-Message="Additional lines will be ignored.",
Reply-Message="",
Ascend-Host-Info="1.2.3.4 Berkeley",
Ascend-Host-Info="1.2.3.5 Alameda",
Ascend-Host-Info="1.2.36 San Francisco",
...
```

Ascend-Idle-Limit (244)

Description: This attribute specifies the number of seconds the MAX waits before clearing a call when a session is inactive.

Usage: Specify a number between 0 and 65535. If you specify 0 (zero), the MAX always clears a call when a session is inactive. The default value is 120 seconds. If you accept the default and an existing Answer Profile specifies a value for the analogous Idle parameter, the Idle value is ignored and the MAX uses the Ascend-Idle-Limit default.

Dependencies: Keep this additional information in mind:

- If the time set by the Ascend-Idle-Limit expires, the call disconnects whether or not bandwidth utilization falls below the Ascend-MPP-Idle-Percent setting.
- When bandwidth utilization falls below the Ascend-MPP-Idle-Percent setting, the call disconnects regardless of whether the time specified by the Ascend-Idle-Limit attribute has expired.
- Because the Ascend-MPP-Idle-Percent attribute is dependent on traffic levels on both sides of the connection, we recommend that you use the Ascend-Idle-Limit attribute in preference to it.
- The Ascend-Idle-Limit attribute does not apply to nailed-up links.

Ascend-IF-Netmask (154)

Description: This attribute specifies the subnet mask in use for the local numbered interface.

Usage: Specify a subnet mask consisting of four numbers between 0 and 255, separated by periods. The default value is 0.0.0.0.

Ascend-Inc-Channel-Count (236)

Description: This attribute specifies the number of channels the MAX adds when bandwidth changes either manually or automatically during a call.

Usage: Specify a number between 1 and 32. The default value is 1.

Dependencies: Keep this additional information in mind:

- Ascend-Inc-Channel-Count does not apply if all channels of a link are nailed up (Ascend-Call-Type=Nailed).
- Ascend-Inc-Channel-Count applies only if the link is using MP+ encapsulation (Framed-Protocol=MPP).
- MP+ calls cannot exceed 32 channels.
- The sum of Ascend-Base-Channel-Count and Ascend-Inc-Channel-Count cannot exceed the maximum number of channels available.

Ascend-IP-Direct (209)

Description: This attribute specifies the IP address to which the MAX redirects packets from the user. When you include this attribute in a user profile, the MAX bypasses all internal routing and bridging tables, and simply sends all packets received on this connection's WAN interface to the specified IP address.

Ascend-IP-Direct does not affect packets sent to this connection. Traffic destined for the connection user is routed using the MAX unit's routing scheme.

Usage: Specify an IP address in dotted decimal notation. An IP address consists of four numbers between 0 and 255, separated by periods. The default value is 0.0.0.0. If you accept the default, the MAX does not redirect IP traffic.

Dependencies: Keep this additional information in mind:

- You can specify the Ascend-IP-Direct attribute only under these conditions:
  - IP routing is in use.
  - The user profile contains the specification Ascend-Bridge=Bridge-No.
  - Framed-Protocol is not set to COMB or FR.
- Do not set Ascend-IP-Direct and Ascend-FR-Direct in the same user profile; if you do, an error occurs.

- Ascend-IP-Direct connections typically turn off RIP.
  If the connection is configured to receive RIP, all RIP packets from the remote end are kept locally and forwarded to the IP address you specify. To turn off RIP, set Framed-Routing=None.

Example: This user profile specifies that the MAX redirects incoming packets to the host at IP address 10.2.3.11:

```
emma Password="m2dan", Service-Type=Framed
     Framed-Protocol=PPP,
     Framed-IP-Address=10.8.9.10,
     Framed-IP-Netmask=255.255.252.0,
     Ascend-Route-IP=Route-IP-Yes,
     Ascend-Bridge=Bridge-No,
     Ascend-IP-Direct=10.2.3.11,
     Ascend-Metric=2,
     Framed-Routing=None,
     ...
```

Ascend-IP-Pool-Definition (217)

Description: This attribute specifies the first IP address in an IP address pool, and indicates the number of addresses in the pool.

Usage: The Ascend-IP-Pool-Definition attribute has this format:

```
Ascend-IP-Pool-Definition="<num> <first_ipaddr>
<max_entries>"
```

Table B-11 describes each Ascend-IP-Pool-Definition argument.

Table B-11. Ascend-IP-Pool-Definition arguments

Argument	Description
<num>	Indicates the number of the pool. The default value is 1. Specify pool numbers starting with 1, unless you have defined pools in the MAX interface using the Pool #1 Start, Pool #1 Count, Pool #2 Start, and Pool #2 Count parameters and do not wish to override these settings. In this case, specify 3 for the first pool number in the RADIUS pseudo-user entry.
<first_ipaddr>	Specifies the first IP address in the address pool. The address you indicate should not accept a subnet mask, because it always becomes a host route. The default value is 0.0.0.0.
<max_entries>	Specifies the maximum number of IP addresses in the pool. Addresses are assigned sequentially, from <first_ipaddr> on, up to the limit of addresses specified by <max_entries>. The default value is 0.

Dependencies: You specify one or more Ascend-IP-Pool-Definition attributes in a pseudo-user profile. You create a pseudo-user to store information that the MAX can query—in this case, in order to store IP address pool information. Specify the first line of a pseudo-user entry in this format:

```
pools-<unit_name> Password="ascend", Service-Type=Outbound
```

<unit_name> is the system name of the MAX—that is, the name specified by the Name parameter in the System Profile. On the next lines of the profile, specify one or more Ascend-IP-Pool-Definition attributes.

Example: In this example, two IP address pools are created for the MAX to use. Address pool #1 contains a block of 7 IP addresses from 10.1.0.1 to 10.1.0.7. Address pool #2 contains a block of 48 IP addresses from 10.2.0.1 to 10.2.0.48.

```
pools-MAX Password="ascend", Service-Type=Outbound
    Ascend-IP-Pool-Definition="1 10.1.0.1 7",
    Ascend-IP-Pool-Definition="2 10.2.0.1 48"
```

Ascend-IPX-Alias (224)

Description: This attribute specifies an IPX network number to use when connecting to IPX routers that require numbered interfaces.

Usage: Specify an IPX network number. The default value is 0 (zero). RADIUS requires that this attribute have a decimal value (base 10), but IPX network numbers generally have hexadecimal values (base 16). In order to give this attribute a value, you must convert the hexadecimal IPX network number to a decimal value for use in the user profile.

Ascend-IPX-Node-Addr (182)

Description: This attribute specifies a unique IPX node address on the network specified by Framed-IPX-Network. This value completes the IPX address of a mobile node.

Usage: Specify a 12-digit ASCII string enclosed in double-quotes. The RADIUS server passes the attributes contained in the mobile node's profile to the foreign agent; the foreign agent sends these attributes when connecting with the home agent.

Ascend-IPX-Peer-Mode (216)

Description: This attribute specifies whether the caller associated with the user profile is an Ethernet client with its own IPX network address, or a dial-in PPP client.

Dial-in clients do not belong to an IPX network, so they must be assigned an IPX network number to establish a routing connection with the MAX. To provide an IPX network number for dial-in clients, you must define a "virtual" IPX network in the Ethernet Profile using the IPX Pool# parameter. The MAX advertises the route to this virtual network and assigns it as the network address for dial-in clients.

Usage: For the Ascend-IPX-Peer-Mode attribute, you can specify one of these values:

- IPX-Peer-Router (0) indicates that the caller is on the Ethernet network and has its own IPX address.

IPX-Peer-Router is the default.

- IPX-Peer-Dialin (1) indicates that the caller is a dial-in NetWare client that incorporates PPP software and dial-out hardware, but does not have an Ethernet interface.

  This setting causes the MAX to assign the caller an IPX address derived from the value of IPX Pool#. If the client does not supply its own unique node number, the MAX assigns a unique node number to the client as well. The MAX does not send IPX RIP and SAP advertisements across the connection and ignores IPX RIP and SAP advertisements received from the remote end. However, it does respond to IPX RIP and SAP queries received from dial-in clients.

Ascend-IPX-Route (174)

Description: This attribute enables you to configure a static IPX route in a user profile.

Usage: To configure a static IPX route, use this format:

```
Ascend-IPX-Route="<profile_name> <network#> [<node#>]
[<socket#>] [<server_type>] [<hop_count>] [<tick_count>]
[<server_name>]"
```

Limit each pseudo-user profile to about 25 routes—that is, you should specify up to 25 settings for the Ascend-IPX-Route attribute. The MAX fetches information from each pseudo-user profile in order to gather routing information.

Table B-12 describes each Ascend-IPX-Route argument.

Table B-12. Ascend-IPX-Route arguments

Argument	Description
<profile_name>	Specifies the RADIUS user profile used to reach the network. The default value is null.
<network#>	Indicates the unique internal network number assigned to the NetWare server. The default value is 00000000.

Table B-12. Ascend-IPX-Route arguments

Argument	Description
<node#>	Specifies the node number of the NetWare server reached through this route. The default value is 0000000000001—the typical node number for a NetWare file server.
<socket#>	Indicates the socket number of the NetWare server reached through this route. Typically, NetWare file servers use socket 0451. The default value is 0000. The number you specify must be a well-known socket number. Services that use dynamic socket numbers may use a different socket each time they load. To bring up a connection to a remote service that uses a dynamic socket number, specify a "master" server that uses a well-known socket number.
<server_type>	Specifies the SAP service type of the NetWare server. NetWare file servers have SAP service type 0004. The default value is 0000.
<hop_count>	Indicates the distance to the destination network in hops. The default value is 1.
<tick_count>	Specifies the distance to the destination network in IBM PC clock ticks (one-eighteenth of a second). This value is for round-trip timer calculation and for determining the nearest server of a given type.The default value is 12.
<server_name>	Indicates the name of an IPX server. The default value is null.

Dependencies: Each static route must appear in a pseudo-user profile. You create a pseudo-user to store information that the MAX can query—in this case, in order to store IPX routing information. You can configure pseudo-users for both global and MAX-specific configuration control of IPX dialout routes. The MAX loads the unit-specific dialout routes in addition to the global dialout routes.

For a unit-specific IPX dialout route, specify the first line of a pseudo-user entry in this format:

ipxroute-<unit_name>**-**<num> **Password="ascend", Service-Type=Outbound**

For a global IPX dialout route, specify the first line of a pseudo-user entry in this format:

ipxroute-<num> **Password="ascend", Service-Type=Outbound**

<unit_name> is the system name of the MAX—that is, the name specified by the Name parameter in the System Profile. <num> is a number in a sequential series, starting at 1.

In each pseudo-user entry, you can specify one or more routes using the Ascend-IPX-Route attribute. When you have properly configured the profile, RADIUS adds IPX dialout routes to the routing table whenever you power on or reset the MAX, or when you select the Upd Rem Cfg command from the Sys Diag menu. RADIUS adds the routes in this way:

1. RADIUS looks for entries having the format ipxroute-<unit_name>-1, where
   <unit_name> is the system name.
2. If at least one entry exists, RADIUS loads all existing entries having the format
   ipxroute-<unit_name>-<num> to initialize the IPX routing table.
   The variable <num> is a number in a sequential series, starting with 1.
3. The MAX queries ipxroute-<unit_name>-1, then ipxroute-<unit_name>-2, and so on, until it receives an authentication reject from RADIUS.
4. Once the host-specific routes are loaded, RADIUS loads the global configuration entries; these configurations have the form ipxroute-<num>.
5. The MAX queries ipxroute-1, then ipxroute-2, and so on, until it receives an authentication reject from RADIUS.

Example: This example defines a unit-specific IPX route:

```
ipxroute-CA-1 Password="ascend", Service-Type=Outbound
        Ascend-IPX-Route="def 6 7 8 9 10"
```

This example defines a global IPX route:

```
ipxroute-1 Password="ascend", Service-Type=Outbound
        Ascend-IPX-Route="abc 1 2 3 4 5 "
```

Ascend-Link-Compression (233)

Description: This attribute turns data compression on or off for a PPP link.

Usage: You can specify one of these values:

- Link-Comp-None (0) turns off data compression.
  Link-Comp-None in the default.
- Link-Comp-Stac (1) turns on data compression.
  The MAX applies the STACKER LZS compression/decompression algorithm.

Dependencies: Both sides of the link must set either the Ascend-Link-Compression attribute or the Link Comp parameter to turn on data compression.

Ascend-Maximum-Channels (235)

Description: This attribute specifies the maximum number of channels allowed on an MP+ call.

Usage: Specify an integer between 1 and the maximum number of channels your system supports. The default value is 1.

Dependencies: Keep this additional information in mind:

- This attribute applies only to MP+ calls.
- For optimum MP+ performance, both sides of a connection must set these parameters and attributes to the same values:
  - Base Ch Count (in the Connection Profile) or Ascend-Base-Channel-Count (in RADIUS)
  - Min Ch Count (in the Answer Profile and the Connection Profile) or Ascend-Minimum-Channels (in RADIUS)
  - Max Ch Count (in the Answer Profile and the Connection Profile) or Ascend-Maximum-Channels (in RADIUS)

Ascend-Maximum-Time (194)

Description: This attribute specifies the maximum length of time in seconds that any session is allowed. Once a session reaches the time limit, its connection is taken offline.

Usage: Specify an integer between 0 and 4,294,967,295. The default value is 0 (zero); when you accept the default, the MAX does not enforce a time limit.

Ascend-Menu-Item (206)

Description: This attribute defines a single menu item for a user profile. You can specify up to 20 Ascend-Menu-Item attributes per profile. The menu items display in the order in which they appear in the RADIUS profile.

Using this attribute, you can configure the terminal server user profile to give the user a custom menu of items from which to choose. The server uses the custom menu to present the user with a subset of terminal server commands. The user does not have access to the regular menu or to the terminal server command line.

Usage: Enter your specifications using this format:

Ascend-Menu Item=<command>;<text>;<match>

- <command> is the string sent to the terminal server when the user selects the menu item.
- <text> is the text displayed to the user.
- <match> is the pattern the user must type to select the item.
- The first semi-colon (;) that appears acts as the delimiter between <command> and <text>; the second semi-colon that appears acts as the delimiter between <text> and <match>.

By default, the MAX uses the standard terminal server menu.

Example: Suppose you set these attributes:

```
emma Password="m2dan", Service-Type=Login
   Ascend-Menu-Item="show ip stats;Display IP Stats",
   Ascend-Menu-Item="ping 1.2.3.4;Ping server",
   Ascend-Menu-Item="telnet 10.2.4.5;Telnet to Ken's
machine",
   Ascend-Menu-Item="show arp;Display ARP Table",
```

```
   Ascend-Menu-Selector="               Option:",
   ...
```

The terminal server displays this text:

```
1. Display IP Stats     3. Telnet to Ken's machine
2. Ping server          4. Display ARP Table.
               Option:
```

Now, suppose you also enter specifications for the <match> option, as in this entry:

```
emma Password="m2dan", Service-Type=Login
   Ascend-Menu-Item="show ip stats;ip=Display ip stats;ip",
   Ascend-Menu-Item="ping 1.2.3.4;p=Ping server. Ctrl-C
stops ping;p",
   Ascend-Menu-Item="telnet 10.2.4.5;t=Telnet to Ken's
machine;t",
   Ascend-Menu-Item="show arp;dsp=Display arp table;dsp ",
   Ascend-Menu-Selector="               Option:",
   ...
```

The terminal server displays this text:

```
ip=Display ip stats         p=Ping server. Ctrl-C stops ping
t=Telnet to Ken's machine    dsp=Display arp table
               Option:
```

Note that you cannot combine numeric menu selections with pattern matching. The first Ascend-Menu-Item attribute determines whether the screen displays numbered selections or patterns. This example shows what you should not do:

```
emma Password="m2dan", Service-Type=Login
   Ascend-Menu-Item="show ip stats;ip=Display ip stats",
   Ascend-Menu-Item="ping 1.2.3.4;p=Ping server. Ctrl-C
stops ping;p",
   Ascend-Menu-Item="telnet 10.2.4.5;t=Telnet to Ken's
machine;t",
   Ascend-Menu-Item="show arp;dsp=Display arp table;dsp ",
   Ascend-Menu-Selector="               Option:",
   ...
```

If you mix numbered selections and pattern matching as in this example, the terminal server screen displays the following text:

```
1. ip=Display ip stats              3. t=Telnet to Ken's
machine
2. p=Ping server. Ctrl-C stops ping  4. dsp=Display arp table
              Option:
```

Ascend-Menu-Selector (205)

Description: This attribute specifies a string as a prompt for user input in the terminal server menu interface.

By default, when you create a custom menu with the Ascend-Menu-Item attribute, the terminal server displays this string when prompting the user to make a selection:

```
Enter Selection (1-<num>, q)
```

The <num> argument represents the last number in the list. The terminal server code automatically determines the value of <num> by determining the number of items in the menu. The only valid user input is in the range 1 through <num>, and q to quit.

However, you can specify a different string for prompting the user to make a selection. The Ascend-Menu-Selector attribute enables you to specify a string that the terminal server displays when prompting a user for a menu selection. If you define this attribute, its value overrides the default of Enter Selection (1-<num>, q).

Usage: Specify a text string containing up to 31 characters. The terminal server displays this string when prompting the user for a menu selection.

Example: Suppose you set these attributes:

```
emma Password="m2dan", Service-Type=Login
   Ascend-Menu-Item="show ip stats;Display IP Stats",
   Ascend-Menu-Item="ping 1.2.3.4;Ping server",
   Ascend-Menu-Item="telnet 10.2.4.5; Telnet to Ken's
machine",
   Ascend-Menu-Item="show arp;Display ARP Table"
   Ascend-Menu-Selector="              Option:"
```

The terminal server displays this text:

```
1. Display IP Stats     3. Telnet to Ken's machine
2. Ping server          4. Display ARP Table.
```

```
                    Option:
```

Note that the valid user input in this example is still 1 through 4, or q to quit.

Ascend-Metric (225)

Description: Ascend-Metric enables you to specify the virtual hop count of an IP route.

If there are two routes available to a single destination network, you can ensure that the MAX uses any available nailed-up channel before using a switched channel by setting the Ascend-Metric attribute to a value higher than the metric of any nailed-up route. The higher the value entered, the less likely that the MAX will bring the link or route online. The MAX uses the lowest metric.

Usage: You can specify a number between 1 and 15. This value is the virtual hop count. The default value is 7.

Dependencies: Keep this additional information in mind:

- The Ascend-Metric attribute does not apply to bridged connections, such as Combinet links.
- The hop count includes the metric of each switched link in the route.

Example: If a route to a station takes three hops over nailed-up lines, and Ascend-Metric=4 in a user profile that reaches the same station, the MAX does not bring the user profile's link online. However, if the link is already online, the MAX does not use the nailed-up lines.

Ascend-Minimum-Channels (173)

Description: Ascend-Minimum-Channels specifies the minimum number of channels an MP+ call maintains.

Usage: You can specify a number between 1 and 32. The default value is 1.

Dependencies: Keep this additional information in mind:

- This attribute applies only to MP+ calls.

- For optimum MP+ performance, both sides of a connection must set these parameters and attributes to the same values:
  - Base Ch Count (in the Connection Profile) or Ascend-Base-Channel-Count (in RADIUS)
  - Min Ch Count (in the Answer Profile and the Connection Profile) or Ascend-Minimum-Channels (in RADIUS)
  - Max Ch Count (in the Answer Profile and the Connection Profile) or Ascend-Maximum-Channels (in RADIUS)

Ascend-MPP-Idle-Percent (254)

Description: This attribute specifies a percentage of bandwidth utilization below which the MAX clears a single-channel MP+ call.

Usage: Specify an integer between 0 and 99. The default value is 0 (zero); this setting causes the MAX to ignore bandwidth utilization when determining whether to clear a call.

Dependencies: Keep this additional information in mind:

- MP+ must be the selected encapsulation method for the profile (Framed-Protocol=MPP).
- If either end of a connection sets the Ascend-MPP-Idle-Percent attribute or Idle Pct parameter to 0 (zero), the MAX ignores bandwidth utilization when determining when to clear a call.
- Bandwidth utilization must fall below this percentage *on both sides of the connection* before the MAX clears the call.
- If the device at the remote end of the link enters an Ascend-MPP-Idle-Percent or Idle Pct setting lower than the value you specify, the MAX does not clear the call until bandwidth utilization falls below the lower percentage.
- If the time set by the Ascend-Idle-Limit expires, the call disconnects whether or not bandwidth utilization falls below the Ascend-MPP-Idle-Percent setting.
- When bandwidth utilization falls below the Ascend-MPP-Idle-Percent setting, the call disconnects regardless of whether the time specified by the Ascend-Idle-Limit attribute has expired.

- Because the Ascend-MPP-Idle-Percent attribute is dependent on traffic levels on both sides of the connection, we recommend that you use the Ascend-Idle-Limit attribute in preference to it.

Ascend-Multicast-Client (152)

Description: This attribute specifies when the user is a multicast client of the MAX.

To communicate with a multicast (MBONE) router, the MAX acts as a multicast client—it receives queries from the router and responds to them using IGMP (Internet Group Management Protocol). The multicast router may reside on its Ethernet interface or across a WAN link.

To communicate with multicast clients, the MAX sends the clients IGMP queries every 60 seconds, receives responses, and forwards multicast traffic. To the clients it looks like a multicast router, although in fact the MAX is forwarding multicast packets based on group memberships.

Usage: You can specify one of these values:

- Multicast-No (0)
  This setting indicates that the user is not a multicast client of the MAX.
- Multicast-Yes (1)
  This setting indicates that the user is a multicast client of the MAX.

Dependencies: This attribute applies solely to the IP-only release of the MAX 4000.

Ascend-Multicast-Rate-Limit (153)

Description: This attribute specifies how many seconds the MAX waits before accepting another packet from a multicast client. To prevent multicast clients from creating response storms to multicast transmissions, you configure the user profile to limit the rate at which the MAX accepts packets from clients.

Usage: Specify an integer. If you set the attribute to 0 (zero), the MAX does not apply rate limiting. The default value is 5. Any subsequent packets received in that 5-second window are discarded.

Dependencies: This attribute applies solely to the IP-only release of the MAX 4000.

Ascend-Multilink-ID (187)

Description: This attribute specifies the ID number of the Multilink bundle when the session closes. A Multilink bundle is a multichannel MP or MP+ call. Each online channel of the MP or MP+ call is a session.

Ascend-Multilink-ID is sent in an Accounting-Request packet when all of these conditions are true:

- The session was authenticated.
- The session has ended (Acct-Status-Type=Stop).
- The Auth parameter is not set to RADIUS/LOGOUT.

Usage: Ascend-Multilink-ID does not appear in a user profile and has no default value.

Ascend-Netware-timeout (223)

Description: This attribute specifies how long in minutes the MAX responds to NCP watchdog requests on behalf of IPX clients on the other side of an offline IPX bridging connection. Responding to watchdog requests on behalf of clients is commonly called watchdog spoofing.

Usage: Specify an integer between 0 and 65535. The default value is 0 (zero). This default allows the MAX to respond to watchdog requests without a time limit.

The timer begins counting down as soon as the WAN bridging link goes offline. At the end of the selected time, the client-server connections are released. If there is a reconnection of the WAN session, the timeout is cancelled.

Dependencies: Ascend-Netware-timeout applies to IPX bridging connections when the MAX is on the server LAN and not on the client LAN—that is, when Ascend-Handle-IPX=
Handle-IPX-Server.

Ascend-Number-Sessions (202)

Description: This attribute specifies the number of active user sessions of a given class (as specified by the Class attribute). In the case of multichannel calls, such as MP+ calls, each separate connection counts as a session.

Usage: The value of this attribute is the number of sessions that are active for the specified class. The Ascend-Number-Sessions attribute has a compound value. The first part specifies a user-session class; the second part reports the number of active sessions in that class.

In the MAX, you can set the Sess Timer parameter in the Auth submenu of the Ethernet Profile to send accounting requests at regular intervals. At the specified interval, the MAX reports the number of open sessions by sending an Ascend-Access-Event-Request packet (code 33). This packet contains two attributes—the NAS-Identifier attribute (4), followed by a list of Ascend-Number-Sessions attributes (202).

Dependencies: The Ascend-Number-Sessions attribute is sent in Ascend-Access-Event-Request packets. Only RADIUS daemons customized to recognize this packet code respond these request packets from the MAX. Other accounting daemons ignore it. Therefore, both the standard Livingston RADIUS daemon and the Ascend accounting daemon ignore this attribute.

When modifying the accounting daemon, make sure that it recognizes an Ascend-Access-Event-Request packet in this format:

```
Code (8-bit)=33
Identifier (8-bit) defined in the RADIUS Accounting Draft
Length (16-bit) defined in the RADIUS Accounting Draft
Authenticator (48-bit) defined in the RADIUS Accounting
Draft
List of Ascend-Number-Sessions attributes
```

Example: Suppose that the MAX has three classes of clients: Class-1, Class-2, and Class-3. At the time of the sessions report, there are eight active sessions: three Class-1 sessions, four Class-2 sessions, and one Class-3 session. The accounting packet sent back to the RADIUS accounting server has three Ascend-Number-Session attributes, one for each of these class/session pairs.

Ascend-Num-In-Multilink (188)

Description: This attribute specifies the number of sessions remaining in a Multilink bundle when the session closes. A Multilink bundle is a multichannel MP or MP+ call. Each online channel of the MP or MP+ call is a session.

Ascend-Num-In-Multilink is sent in an Accounting-Request packet when all of these conditions are true:

- The session was authenticated.
- The session has ended (Acct-Status-Type=Stop).
- The Auth parameter is not set to RADIUS/LOGOUT.

Usage: Ascend-Num-In-Multilink does not appear in a user profile and has no default value.

Ascend-PPP-Address (253)

Description: This attribute specifies the MAX unit's IP address reported to the calling unit during PPP IPCP negotiations.

Usage: Specify an IP address in dotted decimal notation. An IP address consists of four numbers between 0 and 255, separated by periods. The default value is 0.0.0.0. If you accept the default, IPCP negotiates with the value of the IP Adrs parameter in the Ethernet Profile.

If you specify a valid IP address, IPCP negotiates with that IP address. If you specify 255.255.255.255, IPCP negotiates with the address 0.0.0.0.

Dependencies: You can assign Ascend-PPP-Address a value different from the MAX unit's true IP address, as long as the user requesting access understands that limitation.

Ascend-PPP-Async-Map (212)

Description: This attribute gives the Ascend PPP code the async control character map for the PPP session. The control characters are passed through the PPP link as data and are used only by applications running over the link.

Usage: Specify a 4-byte bitmap to one or more control characters. The async control character map is defined in RFC 1548 and specifies that each bit position represents its ASCII equivalent. The bits are ordered with the lowest bit of the lowest byte being 0. For example, bit 19 corresponds to Control-S (DC3) or ASCII 19.

Example: Your specification might look like this one:

```
emma Password="m2dan", Service-Type=Login
     Ascend-PPP-Async-Map=19,
     ...
```

The number 19 translates to 13 hex or 10011 binary. Therefore, NUL (00), SOH (01), and EOT (04) are mapped.

Ascend-PPP-VJ-1172 (211)

Description: This attribute instructs the Ascend PPP code to use the 0x0037 value for the VJ compression type. The MAX uses this value only during IPNCP negotiation. Incoming 1172 type options are accepted without this option being set.

RFC 1172 section 5.2 contains an erroneous statement that the VJ compression type value is 0x0037; it should be 0x002d. However, many older PPP implementations use the 0x0037 value when negotiating VJ compression. If you do not specify a value for Ascend-PPP-VJ-1172, the VJ compression type is 0x002d.

Usage: Enter your specification using this format:

```
Ascend-PPP-VJ-1172=PPP-VJ-1172
```

Ascend-PPP-VJ-Slot-Comp (210)

Description: This attribute instructs the Ascend PPP code not to use slot compression when sending VJ-compressed packets.

When you turn on VJ compression, the MAX removes the TCP/IP header, and associates a TCP/IP packet with a connection by giving it a slot ID. The first packet coming into a connection must have a slot ID, but succeeding packets need not have one. If the packet does not have a slot ID, the MAX assumes that it should be associated with the last-used slot ID. This scenario uses slot ID compression, because the slot ID is not used in any packet but the first in a stream.

However, there may be times when you want each VJ-compressed packet to have a slot ID. The Ascend-PPP-VJ-Slot-Comp attribute exists for this purpose.

Usage: To specify that no slot compression occurs, set the Ascend-PPP-VJ-Slot-Comp attribute to VJ-Slot-Comp-No (1). If you do not specify a value for Ascend-PPP-VJ-Slot-Comp, and Framed-Compression=Van-Jacobson-TCP-IP, slot compression occurs.

Ascend-Preempt-Limit (245)

Description: This attribute specifies the number of idle seconds the MAX waits before using one of the channels of an idle link for a new call.

Usage: Specify an integer between 0 and 65535. The MAX never preempts a call if you enter 0 (zero). The default value is 60.

Dependencies: The Ascend-Preempt-Limit attribute does not apply to nailed-up links.

Ascend-Pre-Input-Octets (190)

Description: This attribute indicates the number of input octets before authentication.

Ascend-Pre-Input-Octets is included in an Accounting-Request packet when all of these conditions are true:

- The session was authenticated.
- The session has ended (Acct-Status-Type=Stop).
- The Auth parameter is not set to RADIUS/LOGOUT.

Usage: Ascend-Pre-Input-Octets does not appear in a user profile. Its default value is 0 (zero).

Ascend-Pre-Input-packets (192)

Description: This attribute indicates the number of input packets before authentication.

Ascend-Pre-Input-packets is included in an Accounting-Request packet when all of these conditions are true:

- The session was authenticated.
- The session has ended (Acct-Status-Type=Stop).
- The Auth parameter is not set to RADIUS/LOGOUT.

Usage: Ascend-Pre-Input-packets does not appear in a user profile. Its default value is 0 (zero).

Ascend-Pre-Output-Octets (191)

Description: This attribute indicates the number of output octets before authentication.

Ascend-Pre-Output-Octets is included in an Accounting-Request packet when all of these conditions are true:

- The session was authenticated.
- The session has ended (Acct-Status-Type=Stop).
- The Auth parameter is not set to RADIUS/LOGOUT.

Usage: Ascend-Pre-Output-Octets does not appear in a user profile. Its default value is 0 (zero).

Ascend-Pre-Output-packets (193)

Description: This attribute indicates the number of output packets before authentication.

Ascend-Pre-Output-packets is included in an Accounting-Request packet when all of these conditions are true:

- The session was authenticated.
- The session has ended (Acct-Status-Type=Stop).
- The Auth parameter is not set to RADIUS/LOGOUT.

Usage: Ascend-Pre-Output-packets does not appear in a user profile. Its default value is 0 (zero).

Ascend-PreSession-Time (198)

Description: This attribute reports the length of time in seconds from when a call connected to when it completes authentication.

Ascend-PreSession-Time is included in an Accounting-Request packet when both of these conditions are true:

- The session has ended or has failed to authenticate (Acct-Status-Type=Stop).
- The Auth parameter is not set to RADIUS/LOGOUT.

Usage: Ascend-PreSession-Time does not appear in a user profile. Its default value is 0 (zero).

Ascend-PRI-Number-Type (226)

Description: This attribute specifies the type of phone number the MAX dials.

Usage: You can specify one of these values:

- Unknown-Number (0)
  This setting indicates that the MAX can dial any type of number.
- Intl-Number (1)
  This setting indicates that the MAX dials a number outside the U.S.

- National-Number (2)
  This setting indicates that the MAX dials a number inside the U.S. National-Number is the default.
- Local-Number (4)
  This setting indicates that the MAX dials a number within your Centrex group.
- Abbrev-Number (5)
  This setting indicates that the MAX dials an abbreviated phone number.

Ascend-PW-Expiration

Note: Ascend-PW-Expiry is no longer supported. The attribute that replaced Ascend-PW-Expiry is Expiration.

Ascend-PW-Lifetime (208)

Description: This attribute specifies the number of days that a password is valid.

Usage: Specify an integer to indicate the number of days for which the user's password is valid. You can set the Ascend-PW-Lifetime attribute on any line other than the first line of the user profile.

Dependencies: Keep this additional information in mind:

- If a password expires and the user resets it, the RADIUS server adds the value of
  Ascend-PW-Lifetime to the date on which the user resets the password; the resulting date becomes the new value for Ascend-PW-Expiration.
  For example, suppose that Ascend-PW-Lifetime=30, Ascend-PW-Expiration=January 1, 1996, and today's date is March 1, 1996. If the user resets the password today, the value of Ascend-PW-Expiration becomes today's date + Ascend-PW-Lifetime, or March 31, 1996.
- If the password has not expired, the value of Ascend-PW-Expiration overrides the value of Ascend-PW-Lifetime.
  For example, if on January 1, 1996 you set Ascend-PW-Lifetime=30 and Ascend-PW-Expiration=January 15, 1996, the password expires on January

15, 1996.
In other words, if the password has not expired, the value of Ascend-PW-Lifetime is
irrelevant.

- If Ascend-PW-Lifetime is absent, the value of Lifetime-In-Days determines the password duration.

  The Lifetime-In-Days value in the RADIUS dictionary is the default value for
  Ascend-PW-Lifetime. By default, Lifetime-In-Days is 0 (zero); this value means that passwords do not expire.

Example: You might make this specification:

```
emma Password="m2dan", Service-Type=Login, Ascend-PW-
Expiration="Jan 1, 1996"
     Ascend-PW-Lifetime=30
```

Ascend-Receive-Secret (215)

Description: This attribute specifies a value that must match the password that the RADIUS server sends it to your MAX from the calling unit.

Usage: You can use the Ascend-Receive-Secret attribute for CACHE-TOKEN or PAP-TOKEN-CHAP authentication. In either case, you can specify up to 20 characters. The default value is null.

- CACHE-TOKEN authentication uses a shared secret, and simplifies the authentication process by caching the user's token for the fixed length of time specified by the Ascend-Token-Expiry attribute; during the lifetime of the token, subsequent calls by the user require only CHAP authentication without the use of a hand-held security card.

  For this type of authentication, set the Ascend-Receive-Secret attribute to the same password as the Send PW parameter in the Connection Profile that places the incoming call. The RADIUS server uses this value to authenticate incoming calls from a user while his or her token is cached and alive. The cached token is deposited on the MAX during the initial security-card authentication process.
- PAP-TOKEN-CHAP authentication uses an encrypted CHAP password with which the answering unit authenticates second and subsequent channels of an MP+ call.

For type of authentication, Set Ascend-Receive-Secret to the value of the Aux Send PW parameter in the Connection Profile used to dial the call.

In PAP-TOKEN-CHAP authentication, you need to verify only the initial connection using a hand-held security card. CHAP verifies any additional channels. That is, whenever the MAX adds channels to a PPP or MP+ call using PAP-TOKEN-CHAP, the calling unit sends the encrypted value of Aux Send PW, and the answering unit checks this password against Ascend-Receive-Secret. The answering unit receives Ascend-Receive-Secret from the RADIUS server when the first channel of the call connects.

Example: This example shows the settings necessary for a user called “John” to use an ACE server. The password received from the user is sent to the security server for authentication.

```
John  Authentication-Type=ACE, Ascend-Token-Expiry=90,
Ascend-Token-Idle=80, Ascend-Token-Immediate=Tok-Imm-Yes
      Ascend-Receive-Secret="shared-secret",
      Service-Type=Framed,
      Framed-Protocol=MPP,
      Framed-IP-Address=200.0.5.1,
      Framed-IP-Netmask=255.255.255.0
```

This example shows the settings necessary for a user called “Emma” to use an ACE server. Because this entry includes the attribute Ascend-Receive-Secret, the MAX can authenticate additional channels through CHAP without having to go to the ACE server for authentication.

```
Emma  Authentication-Type=ACE
      Service-Type=Framed,
      Framed-Protocol=MPP,
      Framed-IP-Address=200.0.5.1,
      Framed-IP-Netmask=255.255.255.0,
      Ascend-Receive-Secret="b5XSAM"
```

Ascend-Remote-Addr (155)

Description: This attribute specifies the IP address of the numbered interface at the remote end of a link.

Usage: Specify the IP address of the numbered interface. An IP address consists of four numbers between 0 and 255, separated by periods. The default value is 0.0.0.0.

Dependencies: For Ascend-Remote-Addr to apply, you must enable IP for the user profile (Ascend-Route-IP=Route-IP-Yes).

Ascend-Remove-Seconds (241)

Description: This attribute specifies the number of seconds that average line utilization (ALU) for transmitted data must fall below the threshold indicated by the Ascend-Target-Util attribute before the MAX begins removing bandwidth from a session. The MAX determines the ALU for a session by using the algorithm specified by the Ascend-History-Weigh-Type attribute.

When utilization falls below the threshold for a period of time greater than the value of the Ascend-Remove-Seconds attribute, the MAX attempts to remove the number of channels specified by the Ascend-Dec-Channel-Count attribute. Using the Ascend-Add-Seconds and Ascend-Remove-Seconds attributes prevents the system from continually adding and subtracting bandwidth, and can slow down the process of allocating or removing bandwidth.

Usage: Specify a number between 1 and 300. The default value is 10.

Dependencies: Keep this additional information in mind:

- One channel must be up at all times.
- Removing bandwidth cannot cause the ALU to exceed the threshold specified by the Ascend-Target-Util attribute.
- The number of channels remaining cannot fall below the amount specified by the Ascend-Minimum-Channels attribute.
- Ascend-Add-Seconds and Ascend-Remove-Seconds have little or no effect on a system with a high Ascend-Seconds-Of-History value.

  If the value of Ascend-Seconds-Of-History is low, the Ascend-Add-Seconds and Ascend-Remove-Seconds attributes provide an alternative way to ensure that spikes must persist for a certain period of time before the system responds.

Ascend-Require-Auth (201)

Description: This attribute specifies whether additional authentication is required after CLID (Calling Line ID) authentication.

Usage: You can specify one of these values:

- Not-Require-Auth (0) specifies that additional authentication is not required. Not-Require-Auth is the default.
- Require-Auth (1) specifies that additional authentication is required.

  If you require additional authentication, you must configure a two-tiered dial-in setup. The first-tier dial-in user profile has the following two-line format:

  ```
  <phonenum> Password="Ascend-CLID" Service-Type=Outbound
             Ascend-Require-Auth=Require-Auth
  ```

  - <phonenum> represents the calling party's phone number.
  - The Password setting specifies that RADIUS authenticates the caller by caller ID.
  - The Service-Type setting indicates that the entry does not allow dial-in users.
  - The Ascend-Require-Auth setting specifies that after CLID authentication, additional authentication is required.

  When you set Ascend-Require-Auth=Require-Auth, you should not include any other attributes in the user profile. You must specify the characteristics of the call in the second-tier user profile.

Example: This example shows a two-tiered approach. The first user profile specifies CLID authentication, and indicates that additional authentication will follow. Because Recv Auth=CHAP in the Answer Profile, CHAP authentication will follow CLID authentication. The second user profile sets up other attributes for the call.

```
5551212   Password="Ascend-CLID" Service-Type=Outbound
          Ascend-Require-Auth=Require-Auth

Emma    Password="pwd" Calling-Station-ID="5551212"
        Service-Type=Framed,
        Framed-Protocol=PPP,
        Framed-IP-Address=200.11.12.10,
```

```
Framed-IP-Netmask=255.255.255.248,
Ascend-Send-Secret="pwd",
...
```

Ascend-Route-IP (228)

Description: This attribute specifies whether IP routing is allowed for the user profile.

Usage: You can specify one of these values:

- Route-IP-No (0)
- Route-IP-Yes (1)
  Route-IP-Yes is the default.

Ascend-Route-IPX (229)

Description: This attribute indicates whether IPX routing is allowed for the user profile. For PPP and MP+ calls, both ends of the connection must have matching settings to route IPX.

Usage: You can specify one of these values:

- Route-IPX-No (0)
  Route-IPX-No is the default.
- Route-IPX-Yes (1)

Ascend-Seconds-Of-History (238)

Description: This attribute specifies the number of seconds the MAX uses as a sample for calculating average line utilization (ALU) of transmitted data; the MAX arrives at this average using the algorithm specified by the Ascend-History-Weigh-Type attribute.

The number of seconds you choose for the Ascend-Seconds-Of-History attribute depends on your device's traffic patterns. For example, if you want to average spikes with normal traffic flow, you may want the MAX to establish a longer historical time period. If, on the other hand, traffic patterns consist of many

spikes that are short in duration, you may want to specify a shorter period of time; doing so assigns less weight to the short spikes.

Usage: Specify a number between 1 and 300. The default value is 15 seconds.

Dependencies: Keep this additional information in mind:

- Ascend-Seconds-Of-History applies only to MP+ calls (Framed-Protocol=MPP).
- If you specify a small value for the Ascend-Seconds-Of-History attribute, and increase the values of the Ascend-Add-Seconds attribute and the Ascend-Remove-Seconds attribute relative to the value of Ascend-Seconds-Of-History, the system becomes less responsive to quick spikes.

  The easiest way to determine the proper values for all these attributes is to observe usage patterns; if the system is not responsive enough, the value of Ascend-Seconds-Of-History is too high.

Ascend-Send-Auth (231)

Description: This attribute specifies the authentication protocol that the MAX requests when initiating a connection using PPP or MP+ encapsulation. The answering side of the connection determines which authentication protocol, if any, the connection uses.

Usage: You can specify one of these values:

- Send-Auth-None (0) indicates that the MAX does not request an authentication protocol for outgoing calls.

  Send-Auth-None is the default.

- Send-Auth-PAP (1) indicates that the MAX requests PAP (Password Authentication Protocol).

  PAP is a PPP authentication protocol that provides a simple method for the MAX to establish its identity in a two-way handshake. Authentication takes place only upon initial link establishment, and does not use encryption. The remote device must support PAP.

  If you specify this setting, the MAX requests PAP authentication, but uses CHAP authentication if the called unit requires CHAP. Choose this setting for non-token card authentication if you want to send your password unencrypted.

- Send-Auth-CHAP (2) indicates that the MAX requests CHAP (Challenge Handshake Authentication Protocol).

  CHAP is a PPP authentication protocol that is more secure than PAP. CHAP provides a way for the remote device to periodically verify the identity of the MAX using a three-way handshake and encryption. Authentication takes place upon initial link establishment; a device can repeat the authentication process any time after the connection is made. The remote device must support CHAP.

  If you specify this setting, the MAX does not bring up the connection using PAP. Choose this setting for non-token card authentication if you do not wish to send your password unencrypted—that is, if you do not wish to use PAP authentication.

Dependencies: Keep this additional information in mind:

- Ascend-Send-Auth is applicable only to outgoing user profiles in RADIUS.
- The link must use PPP or MP+ encapsulation.
- If you request PAP or CHAP authentication, you must also specify a password using Ascend-Send-Secret or Ascend-Send-Passwd.

Ascend-Send-Passwd (232)

Description: This attribute specifies the password that the RADIUS server sends to the remote end of a connection on an outgoing call.

Usage: Specify a text string containing up to 20 characters. The default value is null.

Dependencies: In a user profile, you can specify either Ascend-Send-Passwd or Ascend-Send-Secret, but not both. Use Ascend-Send-Passwd only if your version of the MAX does not support Ascend-Send-Secret.

Ascend-Send-Secret (214)

Description: This attribute specifies the password that the RADIUS server sends to the remote end of a connection on an outgoing call. It is encrypted when passed between the RADIUS server and the MAX.

Usage: Specify a text string containing up to 20 characters. The default value is null.

Dependencies: In a user profile, you can specify either Ascend-Send-Passwd or Ascend-Send-Secret, but not both. Use Ascend-Send-Passwd only if your version of the MAX does not support Ascend-Send-Secret.

Ascend-Target-Util (234)

Description: This attribute specifies the percentage of bandwidth use at which the MAX adds or subtracts bandwidth.

Usage: Specify an integer between 0 and 100. The default value is 70.When the value is 70%, the device adds bandwidth when it exceeds a 70 percent utilization rate, and subtracts bandwidth when it falls below that number.

Dependencies: Keep this additional information in mind:

- When selecting a target utilization value, keep these guidelines in mind:
  - Monitor how the application behaves when using different bandwidths.

    For example, an application might be able to use 88% of a 64-kbps link, but only 70% of a 256-kbps link.
  - Monitor the application at different loads.
- Ascend-Target-Util applies only if the link is using MP+ encapsulation (Framed-Protocol=MPP).

Ascend-Third-Prompt (213)

Description: In the MAX configuration interface, the 3rd Prompt parameter enables you to specify an additional prompt for user input after the login and

password prompts in the terminal server interface. The MAX passes the information the user enters to the RADIUS server as the Ascend-Third-Prompt attribute.

Usage: The Ascend-Third-Prompt attribute can contain up to 80 characters and does not appear in a user profile. If the user enters more than 80 characters, the MAX truncates the input to 80. If the user does enter any characters, the MAX sets the attribute to null.

Ascend-Token-Expiry (204)

Description: This attribute specifies the lifetime in minutes of a cached token.

CACHE-TOKEN authentication uses a shared secret, and simplifies the authentication process by caching the user's token for the fixed length of time specified by the Ascend-Token-Expiry attribute.When the cached token is still alive, CHAP authenticates subsequent CACHE-TOKEN access requests from the same user without the use of a hand-held security card. When the cached token has expired, the ACE server authenticates CACHE-TOKEN access requests.

Usage: On the first line of the user profile, specify an integer representing the lifetime of the cached token in minutes. The default value is 0 (zero). If you accept the default, the MAX rejects subsequent CACHE-TOKEN requests from the same user.

Example: The following two-line example allows CACHE-TOKEN authentication with a 90-minute token cache. Notice that the Ascend-Token-Expiry attribute must appear on the first line of the entry, along with the username and Authentication-Type=ACE or = Defender:

```
Connor  Authentication-Type =ACE, Ascend-Token-Expiry=90
        Password="ACE",
        Ascend-Receive-Secret="shared-secret",
          ...
```

Ascend-Token-Idle (199)

Description: This attribute specifies the maximum length of time in minutes a cached token can remain alive between authentications.

Usage: On the first line of the user profile, specify an integer representing the maximum length of time in minutes that a cached token can remain alive. The default value is o (zero). If you accept this default, the cached token remains alive until the value of the Ascend-Token-Expiry attribute causes it to expire.

Dependencies: Typically, the value of Ascend-Token-Idle is lower than the value of Ascend-Token-Expiry.

Example: The following two-line example allows CACHE-TOKEN authentication with a 90-minute token cache and an 80-minute idle limit. Notice that the Ascend-Token-Idle attribute must appear on the first line of the entry:

```
Jim  Authentication-Type=ACE, Ascend-Token-Expiry=90,
Ascend-Token-Idle=80
        Password=bowie
        Ascend-Receive-Secret="shared secret"
```

Ascend-Token-Immediate (200)

Description: This attribute specifies how RADIUS treats the password received from a login user when the user profile specifies a hand-held security card server. Use this attribute in an ACE user profile that contains the setting Service-Type=Login.

Usage: You can specify one of these values:

- Tok-Imm-No (0) indicates that the password received from the user is ignored.

  Choose this value for a security server that requires that a user enter a challenge using a security card before the security server derives a password.

  Tok-Imm-No is the default.
- Tok-Imm-Yes (1) specifies that the password received from the user is sent to the security server for authentication.

Dependencies: The Ascend-Token-Immediate attribute does not work with CHAP authentication.

Example: This example shows a portion of a user profile that sends the password received from the login user to the ACE server. The login derives the password from a hand-held security card:

```
Connor  Authentication-Type=ACE, Ascend-Token-Immediate=Tok-
Imm-Yes
       Password=terminate
Ascend-Receive-Secret="shared-secret",
       Service-Type=Login,
         ...
```

Ascend-Transit-Number (251)

Description: This attribute specifies the U.S Interexchange Carrier (IEC) you use for long distance calls over a T1 PRI line.

Usage: Specify the same digits you use to prefix a phone number dialed over an ISDN BRI line, T1 access line, or voice interface:

- 288 selects AT&T.
- 222 selects MCI.
- 333 selects Sprint.

The default value is null. If you accept the default, the MAX uses any available IEC for long-distance calls.

Ascend-TS-Idle-Limit (169)

Description: This attribute specifies the number of seconds that a terminal server connection must be idle before the MAX disconnects the session.

Usage: You can specify a value between 0 and 65535.The default is 120. A setting of 0 (zero) means that the line can be idle indefinitely.

Dependencies: Ascend-TS-Idle-Limit does not apply if you are using a Frame Relay or raw TCP connection, or if Ascend-TS-Idle-Mode=TS-Idle-None.

Ascend-TS-Idle-Mode (170)

Description: This attribute specifies whether the MAX uses a terminal server idle timer and, if so, whether both the user and host must be idle before the MAX disconnects the session.

Usage: You can specify one of these settings:

- TS-Idle-None (0)

  This setting indicates that the MAX does not disconnect the session no matter how long the line is idle. This setting disables the idle timer.

- TS-Idle-Input (1)

  This setting indicates that the MAX disconnects the session if the user is idle for a length of time greater than the value of the Ascend-TS-Idle-Limit attribute.

  TS-Idle-Input is the default.

- TS-Idle-Input-Output (2)

  This setting indicates that the MAX disconnects the session if both the user and the host are idle for a length of time greater than the value of the Ascend-TS-Idle-Limit attribute.

Example: This entry specifies that the user must be idle for 90 seconds before the MAX disconnects the session.

```
DEFAULT Password="UNIX"
        Service-Type=Login,
        Ascend-TS-Idle-Limit=90,
        Ascend-TS-Idle-Mode=TS-Idle-Input
```

Dependencies: Ascend-TS-Idle-Mode does not apply if you are using a Frame Relay or raw TCP connection.

Calling-Station-ID (31)

Description: This attribute specifies the calling party number for CLID (Calling Line ID) authentication, indicating the phone number of the user that wants to connect to the MAX.

- If you set CLID Auth=Prefer in the Answer Profile, the MAX checks the calling party's phone number against the value of the Calling-Station-ID attribute whenever CLID authentication is available.

  If a match is found, and no further authentication is required, the MAX accepts the call.

- If you set CLID Auth=Required in the Answer Profile, the calling party's phone number must match the value of the Calling-Station-ID attribute before the MAX can answer the call.

  If CLID is not available, the MAX does not answer the call.

Usage: Specify a telephone number. You can indicate up to 37 characters, limited to the following:

```
1234567890()[]!z-*#|
```

The default value is null.

Example: This user profile is configured for CLID authentication using name, password, and caller ID:

```
Emma  Password="test", Calling-Station-ID="123456789"
      Service-Type=Framed,
      Framed-Protocol=PPP,
      Framed-IP-Address=255.255.255.254,
      Framed-IP-Netmask=255.255.255.255,
      Ascend-Assign-IP-Pool=1,
      Ascend-Route-IP=Route-IP-Yes,
      Ascend-Idle-Limit=30
```

CHAP-Password (3)

Description: This attribute specifies the response value provided by a CHAP (Challenge Handshake Authentication Protocol) user in response to the password challenge.

Usage: CHAP-Password is set by the MAX and sent in Access-Request packets. The default value is null.

Old-Password (17)

Description: The MAX and the RADIUS server use this attribute to change an expired password.

When a user specifies an expired password, RADIUS prompts the user for a new password. When the user enters the new password, the MAX sends an Access-Password-Request packet that contains both the old password (as the value of the Change-Password attribute), and the new password (as the value of the Password attribute).

If the RADIUS server accepts the new password, it tries to edit the users file and replace the expired password with the new one. Note that the RADIUS server can make this change in the user profile only in the flat file. It cannot make this change in the database version of the users file.

Usage: Old-Password does not appear in a user profile and has no default value.

Class (25)

Description: This attribute enables access providers to classify user sessions, such as for the purpose of billing users depending on the service option they choose.

If you include the Class attribute in the RADIUS user profile, the RADIUS server sends it to the MAX in the Access-Accept packet when the session begins. Class is then included in Accounting-Request packets sent to the RADIUS accounting server under these conditions:

- Whenever a session starts

- Whenever a session stops (as long as the Auth parameter is not set to RADIUS/LOGOUT)

Keep in mind that the accounting entries give the class on a per-user and per-session basis. The Ascend-Number-Sessions attribute reports information on all user sessions—that is, on the number of current sessions of each class.

In addition, suppose the MAX starts CLID authentication by sending an Access-Request packet and receives the Class attribute in an Access-Accept packet. If the MAX requires further authentication, it includes Class in the Access-Request packet.

Usage: Specify an alphanumeric text string containing up to 253 characters. The default value is null.

Called-Station-ID (30)

Description: Called-Station-ID specifies the called-party number, indicating the phone number dialed by the user to connect to the MAX. Called-Station-ID is set only if the called-party number is known.

Usage: Called-Station-ID is set by the MAX and sent in Access-Request, Access-Accept, and Accounting-Request packets. This attribute does not appear in a user profile and has no default value.

Expiration (21)

Description: This attribute specifies an expiration date for a user's password in a user profile.

When the MAX makes an authentication request, the RADIUS server checks the current date against the value of Expiration. If the date of the authentication request is the same date or a later date than the value of Expiration, the user receives a message saying that the password has expired.

You must specify Expiration when you first create a user.

Usage: Specify a month, day, and year.

- For the month specification, enter the first three letters of the month in which you want the password to expire; or, you can specify the entire name of the month.

  The month must begin with a capital letter.
- For the day specification, enter one or more digits indicating a valid day of the month; 2, 02, 002, and 0021 are all valid, but 32 is not.
- For the year specification, enter a four-digit year.

  The year must start with the number 19.
- Separate each part of the date specification using one or more spaces, tabs, or commas.

The default value is 00/00/00.

Dependencies: Keep this additional information in mind:

- If a password expires and the user resets it, the RADIUS server adds the value of
  Ascend-PW-Lifetime to the date on which the user resets the password; the resulting date becomes the new value for Expiration.

  For example, suppose that Ascend-PW-Lifetime=30, Expiration=January 1, 1996, and today's date is March 1, 1996. If the user resets the password today, the value of Expiration becomes today's date + Ascend-PW-Lifetime, or March 31, 1996.
- If the password has not expired, the value of Expiration overrides the value of Ascend-PW-Lifetime.

  For example, if on January 1, 1996 you set Ascend-PW-Lifetime=30 and Expiration=January 15, 1996, the password expires on January 15, 1996. In other words, if the password has not expired, the value of Ascend-PW-Lifetime is irrelevant.

Example: Your specification might look like this one:

```
emma Password="m2dan"
       Service-Type=Login, Expiration="November 1, 1995"
```

Framed-IP-Address (8)

Description: This attribute specifies the IP address of the caller in a user profile.

RADIUS can authenticate an incoming call by matching its IP address to one specified in the RADIUS user profile. In addition, if the remote end requires an IP address on an outgoing call, and does not assign one dynamically, you must specify it in the user profile.

Usage: Specify an IP address in dotted decimal notation *n.n.n.n*, where *n* is an integer between 0 and 255. The default value is 0.0.0.0. An answering user profile with this setting matches all IP addresses.

Dependencies: Every Connection Profile and RADIUS user profile that specifies an explicit IP address is a static route.

Framed-Compression (13)

Description: This attribute turns TCP/IP header compression on or off.

Usage: To turn on TCP/IP header compression, specify Van-Jacobson-TCP-IP. This setting applies only to packets in TCP applications, such as Telnet, and turns on header compression for both sides of the link. By default, this attribute does not turn on header compression.

Dependencies: Turning on header compression is most effective in reducing overhead when the data portion of the packet is small.

Framed-IPX-Network (23)

Description: This attribute specifies a virtual IPX network required for the ATMP (Ascend Tunnel Management Protocol) home agent to route IPX packets to the mobile node. When specified in a user profile, the Framed-IPX-Network attribute instructs the answering unit to advertise an additional IPX route.

Usage: Specify the IPX network number of the IPX router at the remote end of the connection. The default value is null.

RADIUS requires that Framed-IPX-Network have a decimal value (base 10), but IPX network numbers generally appear as hexadecimal values (base 16). In order

to give this attribute a value, you must convert the hexadecimal IPX network number to decimal format for use in the user profile. For example, if the IPX network number is 13870000, you must convert it to the decimal 49990000. This requirement does not apply for the IPX node address, which is represented as a 12-digit string enclosed in double-quotes.

Framed-MTU (12)

Description: This attribute specifies the maximum number of bytes the MAX can receive in a single packet on a PPP, Frame Relay, EU-UI, or EU-RAW link.

Usage: The default value is 1524; you should accept this default unless the device at the remote end of the link cannot support it. If the administrator of the remote network specifies that you must change this value, specify a number between 1 and 1524 (for a PPP, EU-UI, or EU-RAW link) or between 128 and 1600 (for a Frame Relay link).

Framed-IP-Netmask (9)

Description: This attribute specifies a subnet mask for the caller at Framed-IP-Address in a user profile.

Usage: Specify an IP address in dotted decimal notation *n.n.n.n*, where *n* is an integer between 0 and 255. The default value is 0.0.0.0. If you accept this default, the MAX assumes a default netmask based on the "class" of the address, as

Table B-13. IP address classes and default netmasks

Class	Address range	Network bits
Class A	0.0.0.0 → 127.255.255.255	8
Class B	128.0.0.0 → 191.255.255.255	16
Class C	192.0.0.0 → 223.255.255.255	24
Class D	224.0.0.0 → 239.255.255.255	N/A
Class E (reserved)	240.0.0.0 → 247.255.255.255	N/A

shown in Table B-13.

Framed-Protocol (7)

Description: This attribute specifies the type of framed protocol the link can use. When you set this attribute, the link cannot use any other type of framed protocol.

Usage: Table B-14 lists the values you can specify for Framed-Protocol.

Table B-14. Framed-Protocol settings

Setting	Incoming call	Outgoing call
PPP (1)	A user requesting access can dial in using MP+ (Multilink Protocol Plus), MP (Multilink Protocol), or PPP (Point-to-Point Protocol) framing. A user requesting access can also dial in unframed, and then change to PPP framing. If the user dials in using any other type of framing, the MAX rejects the call.	Outgoing calls use PPP framing.
SLIP (2)	A user requesting access can dial in unframed and change to SLIP framing. SLIP requires that a user dial in without using a framed protocol before changing to SLIP.	This value does not apply to outgoing calls.
MPP (256)	This value does not apply to incoming calls.	Outgoing calls request MP+ framing.

Table B-14. Framed-Protocol settings

Setting	Incoming call	Outgoing call
EURAW (257)	A user requesting access can dial in using EURAW framing. EURAW is a type of X.75 encapsulation in which IP packets are HDLC encapsulated with a CRC field. If the user dials in using any other type of framing, the MAX rejects the call.	Outgoing calls use EURAW framing.
EUUI (258)	A user requesting access can dial in using EUUI framing. EUUI is a type of X.75 encapsulation in which IP packets are HDLC encapsulated with a CRC field and a small header. If the user dials in using any other type of framing, the MAX rejects the call.	Outgoing calls use EUUI framing.
COMB (260)	A user requesting access can dial in using Combinet framing. If the user dials in using any other type of framing, the MAX rejects the call.	Outgoing calls use Combinet framing.
FR (261)	This value does not apply to incoming calls.	Outgoing calls use frame relay (RFC 1490) framing.
Ascend-ARA (262)	A dial-in user can establish an ARA (AppleTalk Remote Access) connection to the Ethernet network.	This value does not apply to outgoing calls.
FR-CIR (263)	This value specifies a frame relay circuit.	This value specifies a frame relay circuit.

Note: By default, the MAX does not limit the protocols a link can access.

Dependencies: What Framed-Protocol does depends on how you set Service-Type:

- If Service-Type=Framed or is unspecified, a user requesting access can dial in using the framing specified by Framed-Protocol; the MAX rejects other types of framing.

  A user requesting access can also dial in without using a framed protocol, but can then change to the framing specified by the Framed-Protocol attribute.
- If Service-Type=Framed or is unspecified, and Framed-Protocol has no specified value, the operator can use any framed protocol.
- If Service-Type=Login, the user cannot use a framed protocol.
- If Service-Type=Outbound, Framed-Protocol specifies the type of framing allowed on the outgoing call.

Example: The dial-in user in this example cannot use the terminal server and is limited to PPP protocols (PPP, MP+, or MP).

```
ascend Password="pipeline"
       Service-Type=Framed,
       Framed-Protocol=PPP,
       Framed-IP-Address=10.0.200.225,
       Framed-IP-Netmask=255.255.255.0,
       Ascend-Metric=2,
       Framed-Routing=None,
       Framed-Route="10.0.220.0 10.0.200.225 1",
       Ascend-Idle-Limit=30
```

The dial-in user in this example establishes an ARA connection to the Ethernet network:

```
ascend Password="pipeline"
       Service-Type=Framed,
       Framed-Protocol=Ascend-ARA
       Ascend-Idle-Limit=30,
...
```

Framed-Route (22)

Description: This attribute enables you to add static IP routes to the MAX unit's routing table.

Usage: The Framed-Route attribute has this format:

```
Framed-Route="<host_ipaddr>[/<subnet mask>] <gateway_ipaddr>
<metric> [<private>] [<name>]"
```

You should limit each pseudo-user profile to about 25 routes—that is, you should specify up to 25 settings for the Framed-Route attribute in a pseudo-user profile. The MAX fetches information from each entry in order to initialize its routing table.

Table B-15 describes each Framed-Route argument.

Table B-15. Framed-Route arguments

Syntax element	Description
<host_ipaddr>/<subnet_mask>	Indicates the IP address of the destination host or subnet reached by this route. If the address includes a subnet mask, the remote router specified by <router_ipaddr> is a router to that subnet, rather than to a whole remote network. To specify the entire remote network, do not specify a subnet mask.

Table B-15. Framed-Route arguments

Syntax element	Description
<router_ipaddr>	Specifies the IP address of the router at the remote end of the connection. The 0.0.0.0 address is a wildcard entry replaced by the caller's IP address.When RADIUS authenticates a caller and sends the MAX an Access-Accept message with a Framed-Route 0.0.0.0 router, the MAX updates its routing tables with the Framed-Route value, but substitutes the caller's IP address for the router. This setting is especially useful when RADIUS cannot know the IP address of the caller because the IP address is assigned from an address pool.
<metric>	Indicates the metric for this route. If the MAX has more than one possible route to a destination network, it chooses the one with the lower metric.
<private>	Specifies "y" if this route is private, or "n" if it is not private. If you specify that the route is private, the MAX does not disclose the existence of the route when queried by RIP or another routing protocol.
<name>	Indicates the name outgoing user profile that uses the route.

Dependencies: Each static route must appear in a pseudo-user profile. You create a pseudo-user to store information that the MAX can query—in this case, in order to store IP routing information. You can configure pseudo-users for both global and MAX-specific configuration control of IP dialout routes. The MAX loads the unit-specific dialout routes in addition to the global dialout routes.

For a unit-specific IP dialout route, specify the first line of a pseudo-user entry in this format:

route-<unit_name>**-**<num> **Password="ascend", Service-Type=Outbound**

For a global IP dialout route, specify the first line of a pseudo-user entry in this format:

```
route-<num> Password="ascend", Service-Type=Outbound
```

<unit_name> is the system name of the MAX—that is, the name specified by the Name parameter in the System Profile. <num> is a number in a sequential series, starting at 1.

In each pseudo-user entry, you can specify one or more routes using the Framed-Route attribute. When you have properly configured the profile, RADIUS adds IP dialout routes to the routing table whenever you power on or reset the MAX, or when you select the Upd Rem Cfg command from the Sys Diag menu. RADIUS adds the routes in this way:

1. RADIUS looks for entries having the format route-<unit_name>-1, where <unit_name> is the system name.
2. If at least one entry exists, RADIUS loads all existing entries having the format
   route-<unit_name>-<num> to initialize the IP routing table.
   The variable <num> is a number in a sequential series, starting with 1.
3. The MAX queries route-<unit_name>-1, then route-<unit_name>-2, and so on, until it receives an authentication reject from RADIUS.
4. Once the host-specific routes are loaded, RADIUS loads the global configuration entries; these configurations have the form route-<num>.
5. The MAX queries route-1, then route-2, and so on, until it receives an authentication reject from RADIUS.

The routes remain in effect until the next restart or until overwritten by dynamic updates or routes specified in Connection Profiles.

Note: In some cases, you might wish to update the MAX unit's routing tables when connecting to a user whose profile specified Service-Type=Framed. In this case, you can set the Framed-Route attribute in an incoming user profile to specify the user's IP address and subnet mask in the <host_ipaddr> and <subnet_mask> arguments; the route you specify in this manner exists only during the time the call is online. When you enter a nonzero router address for <router_ipaddr> that is different from the caller's address, the static route of a dial-in framed persists even after the connection goes offline.

Example: This example shows two RADIUS pseudo-user profiles defining global static IP routes:

```
route-1   Password="ascend" Service-Type=Outbound
   Framed-Route="10.0.200.33/29 10.0.200.37 1 n lala-gw-out
"
   Framed-Route="10.0.200.50/29 10.0.200.37 1 n lala-gw-out
"
   Framed-Route="10.0.200.47/29 10.0.200.49 1 n nana-gw-out
"

route-2   Password="ascend" Service-Type=Outbound
   Framed-Route="11.0.200.33/29 11.0.200.37 1 n zzz-gw-out "
   Framed-Route="12.0.200.47/29 11.0.200.49 1 n kk-gw-out "
```

Framed-Routing (10)

Description: This attribute specifies whether the MAX sends RIP (Routing Information Protocol) packets, receives RIP packets, or both.

Usage: You can specify one of these values:

- None (0) indicates that the MAX does not send or receive RIP updates.

  None is the default. Many sites turn off RIP on the WAN interface in order to avoid storing very large local routing tables. If you turn off RIP, the MAX does not listen to RIP updates across the connection. To route to other networks through that connection, the MAX must rely on static routes specified in a pseudo-user profile.
- Broadcast (1) indicates that the MAX sends RIP version 1 updates, but does not receive them.
- Listen (2) indicates that the MAX receives RIP version 1 updates, but does not send them.
- Broadcast-Listen (3) indicates that the MAX both sends and receives RIP version 1 updates.
- Broadcast-v2 (4) indicates that the MAX sends RIP version 2 updates, but does not receive them.
- Listen-v2 (5) indicates that the MAX receives RIP version 2 updates, but does not send them.
- Broadcast-Listen-v2 (6) indicates that the MAX both sends and receives RIP version 2 updates.

Dependencies: If RIP is enabled to both send and receive RIP updates on the WAN interface, the MAX broadcasts its routing table to the remote network and listens for RIP updates from that network. Gradually, all routers on both networks have consistent routing tables (all of which may become quite large).

Login-IP-Host (14)

Description: This attribute specifies the IP host to which the user automatically connects when you set Service-Type=Login and specify a value for the Login-Service attribute. Access begins immediately after login.

Usage: Specify an IP address in dotted decimal notation *n.n.n.n*, where *n* is an integer between 0 and 255. The default value is 0.0. 0.0.This setting specifies that the Login does not automatically connect to a particular host.

If you do not specify a value for the Login-IP-Host attribute, the user can access any remote host through the Telnet or raw TCP commands of the terminal server command-line interface. When the operator uses the menu-driven terminal server interface, access to remote hosts is limited to the hosts listed by the Ascend-Host-Info attribute.

Dependencies: Keep this additional information in mind:

- Login-IP-Host has the same functionality as the <hostname> field in the terminal server command-line interface.

  Closing the remote terminal server session also automatically closes the session with the Login-IP-Host.
- When Service-Type=Framed, RADIUS ignores the Login-IP-Host attribute.

Login-Service (15)

Description: This attribute specifies the type of terminal service connection to an IP host that occurs immediately after authentication.

Usage: Specify one of these values:

- Telnet (0)

  The user immediately establishes a Telnet session with the host specified by the Login-IP-Host attribute.

- Rlogin (1)

  The user immediately establishes an Rlogin session with the host specified by the Login-IP-Host attribute.

- TCP-Clear (2)

  This setting specifies a TCP/IP connection with no Telnet protocol. TCP-Clear establishes a TCP session between the MAX and the host specified by Login-IP-Host over which the user can run an application specified by Login-TCP-Port.

  If you specify this setting, the Answer Profile must specify TCP-Clear=Yes.

When you set the Login-Service attribute, a dial-in terminal server user makes an immediate connection to an IP host on your local network and never sees the terminal server interface.

By default, the MAX does not grant immediate access to an IP host.

Dependencies: Keep this additional information in mind:

- If you specify both Login-Service and Login-IP-Host, the MAX automatically connects the Login to the host specified by Login-IP-Host.
- If you do not specify Login-Service or Login-IP-Host, the Login sees either the MAX unit's terminal server command-line interface or the terminal server menu interface, depending upon how the MAX is configured.

Example: In this example, an Rlogin session starts automatically for anyone using the "userx" username and "xyzzy" password. When the session terminates, the connection also terminates.

```
# This profile causes an auto-rlogin to 10.0.200.4 upon
login.
userx  Password="xyzzy"
       Service-Type=Login,
       Login-Service=Rlogin,
       Login-IP-Host=10.0.200.4
```

Further, when you specify the following settings, a raw TCP session starts automatically for anyone using the "user1" username and "test1" password:

```
# This profile causes an auto-TCP to 4.2.3.1 port 9 upon
login.
user1  Password="test1"
       Service-Type=Login,
       Login-Service=TCP-Clear,
```

```
Login-IP-Host=4.2.3.1,
Login-TCP-Port=9
```

Login-TCP-Port (16)

Description: This attribute specifies the port number to which a TCP session connects when Login-Service=TCP-Clear in a user profile.

Usage: Specify an integer between 1 and 65535. The default value is 23.

Dependencies: Login-TCP-Port has the same functionality as the <port-number> field in the MAX unit's terminal server command-line interface. For information on the terminal server command-line interface, see the *MAX ISP and Telecommuting Configuration Guide*.

NAS-IP-Address (4)

Description: This attribute indicates the IP address of the MAX. When the MAX sends an Access-Request packet, it indicates its IP address to the RADIUS server using this attribute.

Usage: In most cases, you never need to specify the NAS-IP-Address attribute in a user profile.

However, you might want to specify it if multiple MAX units use a single RADIUS server, and you want to specify the MAX to which a particular user can connect. In this case, the NAS-Identifier value in the Access-Request packet and the NAS-IP-Address value in the user profile must match for the RADIUS server to authenticate the connection.

Specify an IP address in dotted decimal notation *n.n.n.n/nn*, where *n* is an integer between 0 and 255. Suppose that the user "Emma" is allowed to dial into the MAX at IP address 200.65.212.46. The first line of the user profile might look like this one:

```
Emma Password="pwd", NAS-IP-Address=200.65.212.46
```

NAS-Port (5)

Description: This attribute specifies the port on the MAX handling the user session. Specifically, NAS-Port identifies the interface and service the session is using. The MAX sends this attribute to the RADIUS server in an Access-Request packet and an Accounting Request packet.

Usage: You can set the NAS-Port attribute to restrict the line and channel a user can access. On the first line of the user profile, specify NAX-Port using this format:

`<type> <line> <channel>`

- <type> can have the value 1 for a digital call, or 2 for an analog call.
- <line> uses two digits to specify the line number the call is using.
- <channel> uses two digits to represent the channel on the line the call is using.

The incoming authentication request must the NAS-Port setting. The default value is 0 (zero).

Example: To restrict a dial-in user to analog service on line 1, channel 0, set up a user profile like this one:

```
name  Password="password", NAS-Port=20100
      User-Name="robin",
      Service-Type=Framed,
      Framed-Protocol=PPP,
      Ascend-Assign-IP-Pool=1,
      Ascend-Route-IP=1,
      Ascend-Idle-Limit=300,
      Framed-Routing=None
```

Password (2)

Description: This attribute specifies the password of the calling device or dial-in user in a user profile.

Usage: Specify an alphanumeric string containing up to 252 characters. The default value is null. The Password attribute may be used as a check-item, appearing on the first line, or as a reply-item in the following lines.

For example, consider this first line in a user profile:

```
Emma Password="pwd"
```

The user called “Emma” must specify the password “pwd” in order to gain access to the MAX.

Reply-Message (18)

Description: This attribute carries message text from the RADIUS server to RADIUS clients such as the MAX.

- In a pseudo-user profile that configures message text and a list of IP hosts, the Reply-Message attribute specifies text that appears to the terminal server operator who is using the menu-driven interface.
- If the RADIUS server determines that the MAX should terminate the session, it sends an Access-Terminate-Session packet containing the Reply-Message attribute.

Usage: Specify a text string containing up to 80 characters. The default value is null. You can specify up to 16 Reply-Message attributes in a pseudo-user profile.

Dependencies: Keep this additional information in mind:

- An Access-Terminate-Session packet is a RADIUS packet identified by the code number 31; only RADIUS daemons customized to support this packet code can send an Access-Terminate-Session packet.

  Neither the Ascend RADIUS daemon nor the Livingston RADIUS daemon supports this packet type. This packet can include only one attribute—the Reply-Message attribute—and this attribute can specify up to 80 characters of text.

  When the MAX receives an Access-Terminate-Session packet, it starts a timer, displays any Reply-Message included in the packet, and terminates the session. For example, if a user’s bill is past due, the Access-Terminate-Session packet could include the message “Emma, you have not paid your connect charges.”
- If you do not specify a Reply-Message attribute in a user profile that authenticates callers, and the RADIUS server sends an Access-Accept packet, no message appears.

- If the RADIUS server sends an Access-Reject packet and you do not specify a Reply-Message attribute in a customized RADIUS daemon, this message appears:

  ```
  ** Bad Password
  ```

  The MAX then allows the user two additional attempts to enter the correct password; if the user does not supply the correct password in three attempts, the MAX terminates the session.
- If the RADIUS server sends an Access-Terminate-Session packet and you do not specify a Reply-Message attribute in a customized RADIUS daemon, the MAX displays this message to the terminal server user:

  ```
  ** Session Terminated
  ```

  The MAX then uses a timer to terminate the login session. The RADIUS server discards all input it received before it terminated the session.

Example: Here is an example of a pseudo-user profile setting up message text for a MAX named Cal:

```
initial-banner-Cal Password="ascend", Service-Type=Outbound
     Reply-Message="Up to 16 lines of up to 80 characters
each",
     Reply-Message="will be accepted. Long lines will be
truncated",
     Reply-Message="Additional lines will be ignored.",
     Reply-Message="",
     Ascend-Host-Info="1.2.3.4 Berkeley",
     Ascend-Host-Info="1.2.3.5 Alameda",
     Ascend-Host-Info="1.2.36 San Francisco",
     ...
```

Service-Type (6)

Description: This attribute specifies the type of services the link can use.

If RADIUS authenticates an incoming call using the User-Name and Password attributes, and the type of call matches the value of the Service-Type attribute, the MAX applies the attributes specified in the user profile to the call. If the type of call does not match the Service-Type attribute, the MAX rejects the call.

Usage: You can specify one of these values:

- Login (1)

The operator can use an asynchronous Telnet connection to log into the terminal server. The MAX rejects incoming framed calls. The operator cannot use any framed protocol, but can start Telnet or raw TCP sessions.

- Framed (2)

  Incoming calls must use a framed protocol; otherwise, the MAX rejects them. Asynchronous Telnet sessions are unframed and therefore not allowed when you specify this value.

- Outbound (5)

  The user profile can be used for outgoing calls only. The MAX sends this value to the RADIUS server during an authentication request.

By default, the MAX does not limit the services the link can access.

Dependencies: Keep this additional information in mind:

- Login must have an asynchronous means for reaching the MAX; that is, the MAX must have digital modems or V.110 modules, or the call must be V.120 encapsulated.

  Asynchronous Telnet sessions are unframed and therefore not allowed when you set Service-Type=Framed.

User-Name (1)

Description: This attribute can specify one of the following in a user profile:

- The name of the calling device or dial-in user
- The keyword DEFAULT

  If you create a profile with the username DEFAULT and make that profile the *last profile* of the users file, the RADIUS server will use that profile to determine what to do with users who are not contained in the users file. You can configure only one DEFAULT profile in the users file.

- The incoming phone number (for CLID authentication)
- The name of a pseudo-user profile

  You can set up a pseudo-user profile to configure outgoing calls, a pool of dynamic IP addresses, static IP and IPX routes, bridge entries, and the message text and host list for the terminal server interface.

Usage: Specify an alphanumeric string containing up to 252 characters. The default value is null. The username must be the first word in a user profile; you need not specify the name of the attribute.

Example: For example, consider this first line in a user profile:

```
Emma Password="pwd"
       Expiration="Sep 30 1995"
```

The username is “Emma”. The RADIUS server tests the user’s name and password against the values the user provides when making a request for access. If the RADIUS server does not find a match, it denies the request for access.

Here is an example user profile for CLID authentication using the incoming phone number as the User-Name:

```
5551212  Password="Ascend-CLID" Service-Type=Outbound
         Ascend-Require-Auth=Not-Require-Auth,
         Service-Type=Framed,
         Framed-Protocol=PPP,
         Framed-IP-Address=255.255.255.254,
         Framed-IP-Netmask=255.255.255.255,
         Ascend-Assign-IP-Pool=1,
         Ascend-Route-IP=Route-IP-Yes,
         Ascend-Idle-Limit=30
```

This example shows User-Name in a pseudo-user profile for a static route:

```
route-1 Password="ascend", Service-Type=Outbound
        Framed-Route="10.4.5.0/22 10.9.8.10 1 n inu-out"
```

Configuring INTERSOLV drivers

C

Introduction

This section of the appendix includes a simple 11 step procedure for installing and setting up INTERSOLV drivers.

Although the Intrusive drivers that can be called by the Ascend Access Control Driver Manager are supported by the vendor's thorough documentation, this procedure has been used to install and set up an Access Control/Sybase ODBC configuration. It is only included here as a reference. You should consult the INTERSOLV documentation for complete instructions from the vendor.

The Ascend Access Control program and the Sybase DBMS were installed on the same machine, running the Solaris 2.5 operating system. The Sybase DBMS was a system 11.

The procedure

1. Log into the Solaris machine as root
2. Create a directory called odbc in the path /opt
3. Insert INTERSOLV diskette number 1 into the floppy drive (1 of 3 diskettes)
4. Mount the drive using this command:

   ```
   tar -xvf /dev/floppy
   ```

5. Run the setup program called ./setup

6 Input the path /opt/odbc when the setup program prompts you for the default driver location

7 Set the environment with this command:

```
setenv ODBCHOME /opt/odbc
```

8 Set the environment for the database with this command:

```
setenv SYBASE/sybase
```

9 Set the environment for the library files with this command:

```
setenv LD_LIBRARY_PATH $ODBCHOME/dlls:$SYBASE/lib
```

10 Add these lines to the .odbc.ini file's [qesyb] template. They allow the ODBC driver to talk to the Sybase database:

```
Dayabase=Master

ServerName=Sybase

LogonID=sa
```

11 Start the database server and create the necessary tables.

SQL script for authentication table

D

Following is an SQL script for creating a DBMS table called *Authentication*. The table's fields are derived from frequently used RADIUS authentication attributes. The fields are the table's column headings. You can edit the script to add or remove fields.

Caution: Your DBMS may limit the number of fields you can include in a table. Table's fields are column headings that appear in the table's top row. Ascend has tested some DBMSs that only permit you to create rows that are less than 1962 bytes long. The row created by this SQL script is 550 bytes long.

```
create table Authentication(
     Ascend_Assign_IP_Pool int NULL,
     Ascend_Bridge varchar(10) NULL,
     Ascend_Call_Type int NULL,
     Ascend_Callback  int NULL,
     Ascend_Data_Svc  int NULL,
     Ascend_Dial_Number varchar(20) NULL,
     Ascend_Idle_Limit varchar(20) NULL,
     Ascend_IPX_Peer_Mode int NULL,
     Ascend_IPX_Route  varchar(20) NULL,
     Ascend_Menu_Item varchar(80) NULL,
     Ascend_Menu_Selector varchar(80) NULL,
     Ascend_Metric varchar(20) NULL,
```

```
        Ascend_Require_Auth varchar(20) NULL,
        Ascend_Route_IP varchar(20) NULL,
        Ascend_Route_IPX varchar(80) NULL,
        Ascend_Send_Auth int NULL,
        Ascend_Send_Passwd varchar(20) NULL,
        Ascend_Send_Secret varchar(20) NULL,
        Ascend_TS_Idle_Limit int NULL,
        Ascend_TS_Idle_Mode int NULL,
        Authentication_Type int NULL,
        Calling_Station_Id varchar(20) NULL,
        Expiration varchar(25) NULL,
        Framed_IP_Address  varchar(20) NULL,
        Framed_IP_Netmask varchar(20) NULL,
        Framed_IPX_Network varchar(20) NULL,
        Framed_Protocol int NULL,
        Framed_Route varchar(80) NULL,
        Framed_Routing varchar(80) NULL,
        Login_IP_Host varchar(20) NULL,
        Login_Service int NULL,
        Login_TCP_Port int NULL,
        Password varchar(20) NULL,
        Reply_Message varchar(20) NULL,
        Service_Type varchar(20) NULL,
        User_Name varchar(20) NULL
)
```

MAX Accounting codes

E

This chapter contains tables of Ascend Access Control Accounting codes:

MAX Accounting Disconnect Codes

Table E-1. RADIUS Accounting disconnect codes

Code	Disconnect descriptions
1	DIS_NOT_APPLICABLE (Disconnect reason is unknown)
2	DIS_UNKNOWN (Disconnect reason is unknown)
10	DIS_MODEM_NEVER_CARRIER (Modem never detected DCD)
11	DIS_MODEM_LOSS_CARRIER (Modem detected DCD, but went inactive)
12	DIS_MODEM_RESULT_CODES_FAIL (Couldn't parse result codes)
20	DIS_TERMSRV_NORMAL (User quit)
21	DIS_TERMSRV_IDLE_TIMEOUT (Timeout waiting for input)
22	DIS_TERMSRV_EXIT_TELNET (Exiting telnet forces disconnect)
23	DIS_TERMSRV_NO_IP_ADDR (No IP address for switching to a framed protocol, e.g. SLIP,PPP)
24	DIS_TERMSRV_EXIT_TCP (Exiting raw TCP forces disconnect)
25	DIS_TERMSRV_PASSWD_FAIL (Exceeded login attempts)
26	DIS_TERMSRV_RAW_TCP_DISABLE (Attempt to raw TCP when its disabled)
27	DIS_TERMSRV_CTRL_C (Saw <Ctrl-C. during logins)
29	DIS_TERMSRV_DESTROYED (User closed a virtual connect)
30	DIS_TERMSRV_VC_DESTROYED (Active call for a modem outdial session closed. Originating end terminated, i.e. controlling terminal server session went down).
31	DIS_TERMSRV_EXIT_RLOGIN (rlogin exiting)

Table E-1. RADIUS Accounting disconnect codes

32	DIS_TERMSRV_RLOGIN_BAD_OPTION (Bad rlogin command line option specified)
40	DIS_PPP_LCP_TIMEOUT (LCP timed out waiting for rsp)
41	DIS_PPP_LCP_LCP_NEGOTIATION_FAIL (Fail to converge on LCP negotiations)
42	DIS_PPP_PAP (PAP authentication failed)
43	DIS_PPP_CHAP_AUTH_FAIL (CHAP Authentication failed)
44	DIS_PPP_REMOTE_AUTH_FAIL (Authentication failed from remote server)
45	DIS_PPP_RCV_TERMINATE (LCP got Terminate request from far-end while LCP was in Open state)
46	DIS_PPP_RCV_CLOSE_EVENT (LCP got Close state from upper-layer as in Open state, i.e. normal/graceful LCP closure)
47	DIS_PPP_CLOSE_LCP_NO_NCPS_OPEN (Closing LCP because no NCP's were opened)
48	DIS_PPP_CLOSE_LCP_BUNDLE_UNKN (For MP sessions, closing LCP; can't determine which MP bundle to add user to)
49	DIS_PPP_CLOSE_LCP_MP_ADD_FAIL (For Mp sessions, closing LCP; can't add more channels)
50	DIS_TS_ERR_TOO_MANY (Session tables full)
51	DIS_TS_ERR_RESOURCE (No more resources)
52	DIS_TS_ERR_INVALID_IP (IP address is invalid)
53	DIS_TS_ERR_HOSTNAME (Cannot resolve hostname)
54	DIS_TS_ERR_BAD_PORT (Bad or missing port number)
60	DIS_TS_ERR_HOST_RESET (Host reset)

Table E-1. RADIUS Accounting disconnect codes

61	DIS_TS_ERR_ CONNECTION_REFUSED (Connection was refused)
62	DIS_TS_ERR_CONNECTION_TIMEDOUT (Connection timed out)
63	DIS_TS_ERR_CONNECTION_CLOSED (Connection closed by foreign host out)
64	DIS_TS_ERR_NETWORK_UNREACHABLE (Network unreachable)
65	DIS_TS_ERR_HOST_UNREACHABLE (Host unreachable)
66	DIS_TS_ERR_NET_ADMIN_UNREACH (Network admin unreachable)
67	DIS_TS_ERR_HOST_ADMIN_UNREACHABLE (Host admin unreachable)
68	DIS_TS_ERR_PORT_UNREACHABLE (Port unreachable)
100	DIS_SESS_TIMEOUT (Session timeout)
101	DIS_SESS_INVALID_INCOMING (Invalid incoming user)
102	DIS_SESS_CALLBACK (Disconnect due to callback enable)
120	DIS_SESS_INVALID_PROTOCOL (Protocol disabled/unsupported)
150	DIS_SESS_BY_RADIUS (Disconnect requested by RADIUS)
160	DIS_V110_TIMEOUT (Timeout, resync retries exceed maximum V110 retries (MAX_V110_RETRIES))
170	DIS_PPP_AUTH_TIMEOUT (Timeout waiting trying to authenticate)

MAX Accounting Progress codes

Table E-2. RADIUS Accounting Progress codes

Code	Progress description
N/A	PR_NO_PROGRESS
N/A	PR_NOT_APPLICABLE
N/A	PR_UNKNOWN
10	PR_CALL_UP
30	PR_MODEM_UP
31	PR_MODEM_AWAITING_DCD
32	PR_MODEM_AWAITING_CODES
40	PR_TERMSRV_STARTED (Terminal server sess started; needn't be logged in yet)
41	PR_RAW_TCP_STARTED (Started raw tcp)
42	PR_TELNET_STARTED (Started immediate telnet)
43	PR_RAW_TCP_CONNECT (Raw connected to host)
44	PR_TELNET_CONNECT (Telnet connected to host)
45	PR_RLOGIN_STARTED (rlogin started)
46	PR_RLOGIN_CONNECT (rlogin connect)
50	PR_MODEM_OUTDIAL_CALL_UP (Call is active on a modem outdial session)
60	PR_LAN_SESSION_UP (Routing/bridging session up)
61	PR_OPENING_LCP (Opening Link Control Protocol negotiations)
62	PR_OPENING_CCP (Opening Compression Control Protocol negotiations)

Table E-2. RADIUS Accounting Progress codes

63	PR_OPENING_IPNCP (Opening Internet Protocol Network Control Protocol)
64	PR_OPENING_BNCP (Opening Bridging Network Control Protocol)
65	PR_LCP_OPENED (Link Control Protocol in Open state)
66	PR_CCP_OPENED (Compression Control Protocol in Open state)
67	PR_IPNCP_OPENED (IP NCP in Open state)
68	PR_BNPC_OPENED (Bridging NCP in Open state)
69	PR_LCP_STATE_INITIAL (LCP in Initial state; progress of LCP negotiations; see RFC1331 state transition table)
70	PR_LCP_STATE_STARTING (LCP in Starting state)
71	PR_LCP_STATE_CLOSED (LCP in Closed state)
72	PR_LCP_STATE_STOPPED (LCP in Stopped state)
73	PR_LCP_STATE_CLOSING (LCP in Closing state)
74	PR_LCP_STATE_STOPPING (LCP in Stopping state)
75	PR_LCP_STATE_REQSENT (LCP in Req-Sent state)
76	PR_LCP_STATE_ACKRECD (LCP in Ack-Rcvd state)
77	PR_LCP_STATE_ACKSENT (LCP in Ack-Sent state)
80	PR_IPXNCP_OPENED (IXP NCP in Open State)
90	PR_V110_UP (V110 is connected)
91	PR_V110_STATE_OPENED (V110 in opened state)
92	PR_V110_STATE_CARRIER (V110 in carrier state)
93	PR_V110_STATE_RESET (V110 in reset state)

Table E-2. RADIUS Accounting Progress codes

94	PR_V110_STATE_CLOSED (V110 in closed state)

Index

A

B

C

D

E

F

G

H

I

J

K

L

M

N

O

P

Q

R

S

T

U

V

W

X

Z