MAX T1/PRI
RADIUS Supplement

Ascend Communications

Part Number 7820-0405-002 January 24, 1996

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 SPIDs (Service Profile Identifiers) associated with your product
- The type of telco switch and mode, such as AT&T 5ESS Custom or Northern Telecom DMS-100 National ISDN 1
- Whether you are routing or bridging with your Ascend product
- 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`

Table of Contents

About This Supplement

What is in this supplement? vii
What you should know. vii
Documentation conventions vii
Related publications viii

1 Getting Started with RADIUS

Introduction to RADIUS 1-2
What you need before you start 1-2
Installing and integrating RADIUS 1-3
Starting the RADIUS daemon 1-4
Running the daemon with an ASCII users file 1-4
Running RADIUS in DBM mode. 1-6
Creating the users file database 1-6
Starting the RADIUS daemon in DBM mode 1-7
Setting up the RADIUS clients file 1-7
Setting up the RADIUS users file 1-7
List of session attributes 1-7
Users file syntax 1-11
User name in a profile. 1-11
Incoming phone number for CLID authentication 1-11
Pseudo-user profiles. 1-12
The default profile 1-14
Passwords in a profile 1-14
A keyword for CLID authentication 1-14
Keywords for external authentication 1-15
Password and Ascend-Receive-Secret. 1-16
Password expiration. 1-16
User service. 1-17
Login service for terminal server sessions 1-18
Additional terminal server options 1-19
PPP and TCP/IP configurations 1-20
Dynamic address assignment. 1-20
IP direct 1-20
Static IP routes. 1-21
IPX routing configuration. 1-22
Bridging configuration 1-22
Filters 1-22
IP filters 1-22
Generic filters 1-24
RADIUS accounting 1-25
When to use RADIUS accounting 1-26
How to set up RADIUS accounting 1-26
List of accounting attributes 1-27
Extensions for custom RADIUS daemons. 1-28

2 RADIUS Attributes

Numerical listing of attributes 2-2
Cross reference of attributes and parameters 2-34

About This Supplement

This Supplement describes how to use RADIUS (Remote Authentication Dial In User Service) with the MAX. Use this Supplement in conjunction with other manuals in the documentation set,

What is in this supplement?

This Supplement contains these chapters:

- Chapter 1, “Getting Started with RADIUS,” describes how RADIUS works and provides information about how to set up RADIUS to operate with the MAX.
- Chapter 2, “RADIUS Attributes,” documents each RADIUS attribute.

What you should know

This Supplement is intended for the person who will configure and maintain RADIUS and the MAX. You need to understand RADIUS and MAX security.

Documentation conventions

This section shows the documentation conventions used in this guide.

Convention	**Meaning**
Monospace text	Monospace text represents information that you enter exactly as shown, and it identifies onscreen text, such as, statistical information.
[]	Square brackets indicate an optional attribute that you append to a command. To include an attribute, type only the information inside the brackets. Do not type the brackets unless they appear in bold type.
italics	Italics represent variable information. Do not enter the words themselves in the command; enter the information they represent.
|	The | symbol separates command choices that are mutually exclusive.
Note:	A note signifies important additional information.
⚠ **Caution:**	A caution means that a failure to follow the recommended procedure could result in a loss of data or damage to equipment.

Convention	Meaning
⚠ **Warning:**	A warning means that a failure to take appropriate safety precautions could result in physical injury.

Related publications

This supplement does not provide a detailed explanation of RADIUS. For more information about RADIUS, see the RADIUS Internet-Draft draft-ietf-nas-radius-02.txt, which is available from Livingston on the Internet.

To learn about MAX security, refer to the *MAX Security Supplement*.

Getting Started with RADIUS

1

This chapter covers these topics:

Introduction to RADIUS 1-2

What you need before you start 1-2

Installing and integrating RADIUS 1-3

Starting the RADIUS daemon 1-4

Setting up the RADIUS clients file 1-7

Setting up the RADIUS users file 1-7

RADIUS accounting 1-25

Extensions for custom RADIUS daemons. 1-28

Introduction to RADIUS

RADIUS (Remote Authentication Dial In User Server) is a database server developed by Livingston Enterprises, Inc. When used with the MAX, it provides two important services:

- Session authentication

  RADIUS supports the same authentication modes as the MAX, including PAP and CHAP, Combinet name and password validation, CLID, callback, and terminal server validation. If the MAX cannot find a local Connection Profile matching an incoming PPP-encapsulated, Combinet, or terminal server call, the MAX queries the RADIUS server on the IP network and passes it the user ID and password. The RADIUS server then sends back a partial or complete profile that can specify routing, packet filtering, destination-specific static routes, and usage restrictions specific to the user.

  When used for authenticating sessions, RADIUS vastly increase the number of authentication entries that can be supported within the MAX. Without RADIUS, the number of authentication entries is limited by the number of Connection Profiles supported in the MAX.

- Accounting

  When the RADIUS daemon is invoked with the –A option, the server stores session information that can be used for billing or troubleshooting purposes.

The RADIUS server communicates information to the MAX in two different ways. Dynamic data updates are provided on demand when the server passes the MAX parameters needed to establish a session. Static data updates, such as configured static routes or Telnet hosts, are uploaded to the MAX when it starts up or when you use the Upd Rem Cfg command in the MAX Sys Diag menu.

Note: Most RADIUS authentication attributes have counterparts in the MAX configuration menus. For background information on how features work, we recommend that you read the appropriate chapters in the *MAX ISP and Telecommuting Configuration Guide* and the relevant parameter descriptions in the *MAX Reference Guide*. See also the section on cross-referencing attributes and parameters in Chapter 2, "RADIUS Attributes."

For details about how RADIUS works, see draft-ietf-nas-radius-02.txt, which is available from Livingston on the Internet.

Frequently, this document refers to the MAX as the NAS, or Network Access Server. The NAS is the device that requests a RADIUS service (authenticating a user or logging an accounting packet). In this context, a user attempting to open a connection to your MAX is a client of your MAX, while your MAX is a client of the RADIUS server.

What you need before you start

To use RADIUS with the MAX, you need the following items:

- You need a UNIX workstation or PC to run RADIUS.
- You need a TCP/IP connection between the system running the RADIUS daemon (the RADIUS server) to an Ascend MAX, or rack of MAX units.
- If you require RADIUS accounting or any of the Ascend attributes (see Table 1-3 on page 1-9) you must use the Ascend RADIUS daemon, version 1.16 (dated 7/25/95) or later.
- The Ascend RADIUS dictionary must be installed on your RADIUS server and it must have the same date as the Ascend RADIUS daemon you install.

The Ascend RADIUS dictionary includes the Ascend-specific attributes you need to make RADIUS work with the MAX. The only requirement for setting up the dictionary file is to make sure that it is located in the same directory as the daemon and that both files have the same date. If you find a discrepancy in the dates, download the latest dictionary file from ftp.ascend.com, and copy it into the same directory as the daemon.

Note: The RADIUS daemon reads the dictionary when it starts up. So, if you update the dictionary file while the daemon is running, you must kill the daemon process and then restart it to make the new attributes available.

Installing and integrating RADIUS

The latest information on installing RADIUS is always contained in the installation instructions on the Ascend FTP server. This section provides an overview.

To install RADIUS, follow these steps:

1. Use anonymous FTP to download the RADIUS files from the ftp.ascend.com.
2. Decompress (gunzip) and separate (tar) the files.
3. Read the README file, installation instructions, and Makefiles.
4. Use the appropriate Makefile to compile the Ascend RADIUS daemon on your system.

   The keywords ACE, SAFEWORD, and UNIX are reserved words built into the Ascend RADIUS daemon for use with external authentication servers. You can replace these reserved words with other strings by editing the daemon’s source file before compiling it.

   See “Running RADIUS in DBM mode” on page 1-6 for other considerations.
5. Move the Ascend RADIUS dictionary to /etc/raddb.
6. Create the RADIUS clients file and users file in the /etc/raddb directory.

   A client is the MAX or another machine that sends requests to the RADIUS server.

   A user is a caller (a login user or a device) that connects to the MAX. Each user has its own profile in the RADIUS database.

   RADIUS writes error messages to /etc/raddb/logfile. (The Syslog daemon does not create the RADIUS log file.)
7. Use a text editor to open the /etc/services file and add a line identifying the RADIUS daemon’s authentication port. For example:

   ```
   radius<tab>1645/udp   #radiusd
   ```

   The port number you specify must match the port number specified in the Auth Port parameter in the Auth submenu of the MAX Ethernet Profile. You can use a value other than 1645 as long as the Auth Port setting is matches the value. See the *MAX Security Supplement* for more information.

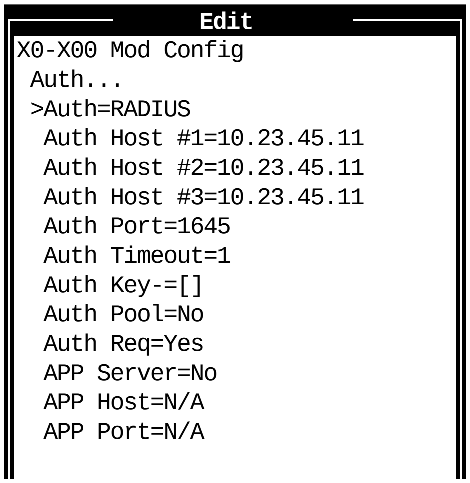
Note: If you intend to run RADIUS accounting, see “How to set up RADIUS accounting” on page 1-26.

The next steps show how to configure the MAX to communicate with the RADIUS daemon.

8. In the MAX configuration interface, open the Ethernet Profile, and then open the Auth submenu.
9. Set the Auth parameter to RADIUS or RADIUS/LOGOUT.

   If you configure the MAX for RADIUS/LOGOUT, RADIUS keeps track of session logouts.

10. Enter the IP address of the RADIUS host in the Auth Host #1 parameter.



```
Edit
X0-X00 Mod Config
 Auth...
 >Auth=RADIUS
  Auth Host #1=10.23.45.11
  Auth Host #2=10.23.45.11
  Auth Host #3=10.23.45.11
  Auth Port=1645
  Auth Timeout=1
  Auth Key-=[]
  Auth Pool=No
  Auth Req=Yes
  APP Server=No
  APP Host=N/A
  APP Port=N/A
```

    See the section on RADIUS servers in the *MAX Security Supplement* for details about the Auth Host #2, Auth Host #3, and Auth Timeout parameters.

11. Enter the UDP port number you specified for the daemon in /etc/services in the Auth Port parameter.

    The MAX and the daemon must agree about which UDP port to use for communication, so make sure that these values match.

12. Enter the RADIUS client password in the Auth Key parameter, exactly as it appears in the RADIUS clients file.

13. If you want to enforce CLID authentication for connections that have Clid Auth=Required, set the Auth Req parameter to Yes.

    See the section on RADIUS servers in the *MAX Security Supplement* for more details about the Auth Req parameter, as well as the Auth Pool and APP parameters.

14. Close the Auth submenu, and then close the Ethernet Profile, saving your changes.

Note: The MAX name and IP address must be in /etc/hosts file on the RADIUS host or in the Yellow Pages database to enable the RADIUS host and the MAX to communicate on the IP network.

Starting the RADIUS daemon

This section describes the Ascend RADIUS daemon options and explains how to run the daemon with either a flat ASCII users file or a users file that has been indexed to increase the efficiency of RADIUS searches.

Running the daemon with an ASCII users file

To start the RADIUS daemon in ASCII mode, type the following command:

```
radiusd
```

You can specify a number of options, in the following format:

```
radiusd options
```

where *options* includes one or more of the options listed immediately below, which can be specified in any order.

- –A *acct*

  This option controls the creation of the RADIUS accounting process, where *acct* can be one of the following strings: none, services, or incr.

  If *acct* is “none”, the daemon does not create the accounting process.

  If *acct* is “services”, the daemon creates the accounting process only if a line defining the UDP port to use for accounting is found in the /etc/services file (otherwise, the accounting process is not created.

  If *acct* is “incr”, the daemon creates the accounting process with the UDP port specified as the accounting port in the /etc/services file, or if that port is not defined, it increments the UDP port specified for radiusd and use that port number. (This is the default action if –A is not specified.)

- –a *acctdir*

  The default directory for RADIUS accounting information is /usr/adm/radacct. You can use this option to specify a different directory name (*acctdir* must already exist). For example:

  radiusd -a /home/radacct

  The accounting process in the daemon creates a file named “detail” in that directory, which will contain accounting records.

- –b *dbdir*

  The default directory for the RADIUS clients, users, dictionary, and log files is /etc/raddb. This option specifies another directory name (*dbdir* must already exist). For example:

  radiusd -b /radius/raddb

- –c

  This option enables cache-token authentication in the daemon. See the *MAX Security Supplement* for details about cache-token authentication, which is used with hand-held security cards. The profile for a security-card connection must have the appropriate attributes as well.

- –p

  This option enables users to change their own expired passwords. See the *MAX Security Supplement* for details about how this feature works in the Ascend RADIUS daemon.

- –s

  This option forces the daemon to run in single-process mode, which is much slower than the default multi-process mode and is normally not recommended.

- –u *usrfile*

  This option assigns the specified *usrfile* name to the RADIUS users file. (The default name is “users”.)

- –v

  This option prints the daemon’s version number, extension, date, and the options selected in the Makefile compilation.

- –w

  This option warns about syntax errors in the users file that are found when the daemon is running. A warning is generated only when the RADIUS daemon examines users file profiles during the authentication process. For a more complete scan of the file for syntax errors, use the builddbm command with the –e option.

- –x

  This option produces debug output.

Running RADIUS in DBM mode

When the MAX requests authentication from the RADIUS server, the daemon performs a linear search of the flat ASCII users file. If the number of profiles in the users file is large, you can increase the efficiency of that search by creating a users file database and running the daemon in DBM (database management) mode.

To create the DBM version of the daemon and the utility used to create the users file database, type:

```
make dbm
```

This command creates two executables, builddbm and radiusd.dbm.

Creating the users file database

Before running radiusd.dbm, you must create the users file database. To do so, type:

```
builddbm users
```

or

```
builddbm /etc/raddb/users
```

(The users file must already exist in ASCII format.) The resulting database files are named users.dir and users.pag.

Note: You must run builddbm each time the users file is modified. If remote users are able to change their own expired passwords, remember that you must run builddbm after each password change to enable the daemon to recognize the change.

The builddbm command supports several options, in the following format:

```
builddbm options
```

where *options* may be one or more of the following options, specified in any order:

- –d *dbdir*

  The default output directory for the database file is /etc/raddb. This option specifies another directory name (*dbdir* must already exist). For example:

  builddbm -d /radius/raddb

  This command results in two database files, /radius/raddb/users.dir and /radius/raddb/users.pag.

- -e

  This option forces the builddbm program to report syntax errors and duplicate entries found in the users file during the indexing process. The messages are written to standard output. If this option is not specified, they are written to standard error output instead.

- -h

  This option displays help.

- –u *usrfile*

  This option names the RADIUS users file for which a database is being built. (The default name is “users”.) If the daemon runs with the –u option, the name specified for the daemon must agree with the name specified for builddbm.

- –v

  This option runs builddbm in verbose mode.

Starting the RADIUS daemon in DBM mode

To start the RADIUS daemon in DBM mode, type the following command:

```
radiusd.dbm
```

The radiusd.dbm command supports the same set of options described for the radiusd command in “Running the daemon with an ASCII users file” on page 1-4, with one exception: the –p option is restricted when the daemon is running in DBM mode, because the users file database will not contain the user’s new password until you run builddbm again.

Setting up the RADIUS clients file

The RADIUS clients file defines the client machines that are allowed to make requests to the RADIUS server. For the RADIUS daemon to respond to client requests from the MAX, you must specify the MAX’s name and its password in the clients file.

The name of the MAX is specified in the Name parameter in the System Profile.

The password to include in the clients file is specified in the Auth Key parameter in the Auth submenu of the Ethernet Profile. If the accounting process of the daemon will be running in the same server (rather than on a separate host), the same password must also serve for the Acct Key parameter in the Accounting submenu of the Ethernet Profile.

For example, add a line similar to this to the clients file:

```
ascend3<tab>bXSAMpy
```

where “ascend3” is the Name and “bXSAMpy” is the password specified in the Auth Key parameter in the MAX Ethernet Profile and, if applicable, in the Acct Key parameter as well.

The name you specify must be resolvable on the IP network (via DNS, the Yellow Pages, etc.). If that is not the case, specify the IP address of the MAX instead.

Setting up the RADIUS users file

The RADIUS users file contains security and configuration information for each user. The full set of information for each user is called a user profile.

The MAX can authenticate an incoming call locally or through RADIUS. Local authentication occurs when the caller’s name and password match a Connection Profile stored in the MAX’s memory. RADIUS authentication occurs when the caller’s name and password match an entry in the RADIUS users file.

List of session attributes

When in incoming call is received, the MAX first checks its local Connection Profiles. If it doesn’t find a Connection Profile for the call and it is configured to communicate with RADIUS, it sends an Access-Request message to the RADIUS server.

The Access-Request packet includes the caller's name and password, and may also include the other attributes shown in Table 1-1. The value of these attributes is then compared to the specified value in the RADIUS user profile. These attributes, if present, must be specified on the first line of the user profile.

Table 1-1. Access Request attributes

Attribute (Number)	**Value**
User-Name (1)	The user's name
User-Password (2)	The user's password
CHAP-Password (3)	The user's CHAP password if password challenge is presented
NAS-Identifier (4)	IP address of the MAX
NAS-Port (5)	UDP port on which the MAX communicates with the RADIUS server (Auth Port)

If the attribute values submitted to RADIUS match the user profile, the RADIUS server authenticates the call and returns an Access-Accept packet containing a list of attributes characterizing that user. Table 1-2 lists the RADIUS attributes defined in the Livingston RADIUS draft. See Table 1-3 on page 1-9 for additional parameters defined by Ascend.

Table 1-2. RADIUS access response attributes

Attribute (Number)	**Value**
Caller-Id (31)	The calling-party number, indicating the phone number of the user that has connected to this MAX
Class (25)	A value sent to the MAX from RADIUS as part of an authentication-acceptance message
Client-Port-DNIS (30)	The called-party number, indicating the phone number dialed by the user to connect to this MAX
Framed-Address (8)	IP address of the user
Framed-IPX-Network (23)	A unique, internal IPX network number for the MAX's Ethernet interface
Framed-Protocol (7)	Type of protocol used: PPP, SLIP, MPP, EURAW, EUUI, COMB, or FR
Framed-Route (22)	A static route when User-Service=Dialout-Framed User
Login-Host (14)	The host to which the Login-User connects upon login
Login-Service (15)	The type of terminal server session: Telnet or TCP-Clear
Login-TCP-Port (16)	The port number to which a TCP session connects (default is 23)
NAS-IP-Address (32)	The IP address of the MAX

Table 1-2. RADIUS access response attributes (continued)

Attribute (Number)	Value
Reply-Message (18)	Message text sent from the RADIUS server to the MAX
User-Service (6)	Framed or unframed call: Framed-User, Login-User, or Dialout-Framed-User

Table 1-3 lists Ascend extensions to the RADIUS attributes. These are defined only in the Ascend RADIUS dictionary file and require the Ascend RADIUS daemon.

Table 1-3. Ascend RADIUS access response attributes

Attribute (Number)	Value
Ascend-Authen-Alias (203)	Sets this MAX’s login name during PPP authentication
Ascend-Callback (245)	Enables or disables callback
Ascend-Call-Filter (243)	Defines a call filter
Ascend-Data-Filter (242)	Defines a data filter
Ascend-FR-Direct (219)	Specifies whether the Connection Profile operates in frame relay redirect mode
Ascend-FR-Direct-DLCI (221)	Specifies the DLCI that carries this connection to the frame relay switch
Ascend-FR-Direct-Profile (220)	Specifies the name of the Frame Relay Profile that carries this connection to the frame relay switch
Ascend-Handle-IPX (222)	Specifies how the MAX handles NCP watchdog requests on behalf of IPX clients during IPX bridging
Ascend-Home-Agent-IP-Addr (183)	The IP address of the home agent under ATMP (Ascend Tunnel Management Protocol) operation
Ascend-Home-Agent-Password (184)	The password that the foreign agent sends to the home agent during ATMP operation
Ascend-Home-Agent-UDP-Port (186)	The UDP port number to use when the foreign agent sends ATMP messages to the home agent
Ascend-Home-Network-Name (185)	The name of the Connection Profile via which the home agent sends all packets it receives from the mobile node during ATMP operation
Ascend-IP-Direct (209)	The IP address to which the MAX redirects packets from the user
Ascend-IPX-Alias (224)	An IPX network number to use when connecting to IPX routers that require numbered interfaces
Ascend-Menu-Item (206)	Defines a single menu item for a user profile
Ascend-Menu-Selector (205)	Specifies a string as a prompt for user input in the terminal server menu interface

Table 1-3. Ascend RADIUS access response attributes (continued)

Attribute (Number)	Value
Ascend-Netware-timeout (223)	The number of minutes the MAX responds to NCP watchdog requests on behalf of IPX clients on the other side of an offline IPX bridging or routing connection
Ascend-PPP-Address (253)	The IP address reported to the calling unit during PPP IPCP negotiations
Ascend-PPP-Async-Map (212)	Gives the Ascend PPP code the async control character map for the PPP session
Ascend-PPP-VJ-1172 (211)	Instructs the Ascend PPP code to use the 0x0037 value for the VJ compression type
Ascend-PPP-VJ-Slot-Comp (210)	Instructs the Ascend PPP code not to use slot compression when sending VJ-compressed packets
Ascend-PW-Expiration (21)	An expiration date for the user’s password
Ascend-PW-Lifetime (208)	Specifies on a per-user basis the number of days that a password is valid
Ascend-Require-Auth (201)	Specifies whether additional authentication is required for CLID-authenticated calls
Ascend-Receive-Secret (215)	A value received from a dial-in user and used to verify an encrypted password
Ascend-Route-IPX (229)	Enables IPX routing
Ascend-Send-Auth (231)	Specifies the protocol to use (PAP or CHAP) for name-password authentication following CLID authentication
Ascend-Send-Secret (214)	When used in place of Ascend-Send-Passwd attribute, the password is encrypted when passed between the RADIUS server and the MAX
Ascend-Third-Prompt (213)	An additional prompt for user input after the login and password prompts
Ascend-Token-Expiry (204)	Sets the lifetime of a cached token—that is, the lifetime of hand-held security card authentication
Ascend-Token-Idle (199)	The maximum length of time in minutes a cached token can remain alive between authentications if a call is idle
Ascend-Token-Immediate (200)	Establishes how RADIUS treats the password received from a login-user when the users file entry specifies a hand-held security card server

Users file syntax

Note: The complete syntax for the users file is specified in EBNF format in the file named “users-file-syntax.1” in the “man” subdirectory.

User profiles consist of a first line that contains attributes such as the user’s name, password, and password expiration date. The first line cannot begin with a # character, a tab, or a space. The first word is the user name, followed by one or more spaces or tabs, followed by an attribute list (*without* a trailing comma), followed by a newline.

Subsequent lines may be a blank line or another configuration line that begins with a space or tab character, followed by an attribute list, followed by a comma, followed by a newline. The last line of the profile is identical to the other lines except that it has no trailing comma.

For example:

```
ascend1 Password = "pwd", Ascend-PW-Expiration = "Sep 30 1995"
<tab>User-Service = Framed-User,
<tab>Framed-Protocol = PPP,
<tab>Framed-Address = 10.0.1.1,
<tab>Framed-Netmask = 255.255.255.0,
<tab>Ascend-Metric = 2,
<tab>Framed-Routing = None,
<tab>Ascend-Idle-Limit = 30
```

The string to the left of the equal (=) sign is an attribute as defined in the dictionary file.The value to the right is the configuration data.

In the example profile, “ascend1” is the user name obtained from the remote caller and “pwd” is the password. These values correspond to the Station and Recv PW parameters in a MAX Connection Profile. The Framed-Address used for the incoming call is given the value 10.0.1.1. This value corresponds to the LAN Adrs parameter in a MAX Connection Profile.

User name in a profile

The first word in a profile is always the user name, followed by one or more spaces or tabs, followed by an attribute list (*without* a trailing comma), followed by a newline. The user name can be up to 252 characters.

For example:

```
ascend1 Password = "pwd", Ascend-PW-Expiration = "Sep 30 1995"
```

The user’s name and password are tested against the values provided by the user when an authentication request is made. If they don’t match the access request is denied.

The user name is the name of the calling device or dial-in user. It can also be one of the following values:

- The incoming phone number (for CLID authentication)
- A keyword representing a pseudo-user profile
- The keyword DEFAULT

Incoming phone number for CLID authentication

For CLID authentication, the user name is set to the incoming phone number and the password is set to Ascend-CLID. The user’s real name should be placed in the profile by using the User-Name attribute, as shown below:

```
#5551212 Password = "Ascend-CLID" User-Service = Dialout-Framed-User
<tab>User-Name = "real-user-name",
<tab>Framed-Protocol = PPP,
<tab>Framed-Address = 10.10.0.1,
<tab>Framed-Address = 255.255.255.0
```

See “A keyword for CLID authentication” on page 1-14for more details.

Pseudo-user profiles

A pseudo-user profile stores information that can be queried. All pseudo-user profiles have a password of “ascend” and User-Service=Dialout-Framed-User. To prevent users from logging in using this profile, the User-Service=Dialout-Framed-User assignment must appear in the first line of the profile, as shown in the examples throughout this section.

- banner

  The RADIUS server (Ascend daemon) can supply both the banner and a list of TELNET hosts to remote users logging into terminal server, provided that the users file has a profile with this user name and the Remote Conf parameter in the TServ Options submenu of the Ethernet Profile is set to Yes. When a user logs into the terminal server, the example profile shown below displays a banner and, if terminal server session is running under the menu driven interface, a list of TELNET hosts is also displayed.

```
banner Password = "ascend" User-Service = Dialout-Framed-User
<tab>Reply-Message = "Up to 16 lines of up to 80 characters each",
<tab>Reply-Message = "will be accepted. Long lines will be truncated",
<tab>Reply-Message = "Additional lines will be ignored",
<tab>Reply-Message = "",
<tab>Reply-Message = "There can be up to 10 Ascend-Host-Info entries",
<tab>Reply-Message = "in this profile. Each entry has an IP address",
<tab>Reply-Message = "to telnet to and up to 31 characters of text",
<tab>Reply-Message = "describing the host. The text will be assigned",
<tab>Reply-Message = "a number. When the number is selected a telnet",
<tab>Reply-Message = "session to the ip address will be initiated.",
<tab>Ascend-Host-Info "1.2.3.4 a host name or phrase",
<tab>Ascend-Host-Info "1.2.3.5 another host",
<tab>Ascend-Host-INfo "5.4.3.2 the last host"
```

When a user logs into the terminal server, they see a banner message like this:

```
Up to 16 lines of up to 80 characters each
will be accepted. Long lines will be truncated.
Additional lines will be ignored

There can be up to 10 Ascend-Host-Info entries
in this profile. Each entry contains an IP address
to telnet to and up to 31 characters of text
describing the host. The text will be assigned
a number. When the number is selected a telnet
session to the ip address will be initiated.

             1. host name or phrase
             2. another host
             3. the last host

                Enter Selection (1-3,q)
```

The banner profile can have no more than 16 Reply Message lines, with each line having no more than 80 characters of text. It can also have no more than 10 Ascend-Host-Info lines, with each line having no more than 31 characters of descriptive text following the IP address.

- pools-*name*

  A pools-name profile defines IP address pools to be used for dynamic assignment. A pool is a range of contiguous IP addresses.

  The *name* appended to “pools-” must match the name assigned to the MAX in the System Profile. The profile that defines address pools has the following format:

```
pools-name Password ="ascend" User-Service= Dialout-Framed-User,
<tab>Ascend-IP-Pool-Definition= "3 10.7.200.23 5",
<tab>Ascend-IP-Pool-Definition= "2 10.7.201.5 10"
```

  The Ascend-IP-Pool-Definition attributes defines a pool of addresses using this format:

  X a.b.c.d *Z*

  where *X* is the pool index number, a.b.c.d is the pool’s starting IP address, and *Z* is the number of IP addresses in the pool. For example, the definition “3 10.7.200.23 5” in the example shown above allocates 10.7.200.23—10.7.200.27 for dynamic assignment.

  See the chapter on Configuring the MAX as an IP Router in the *MAX ISP and Telecommuting Configuration Guide* for more details about dynamic address assignment.

  Note that if you assign the index number 1 or 2 to a pool definition, and address pool 1 or 2 (or both) is also defined in the Ethernet Profile of the MAX, the assignments in RADIUS take precedence over those in the MAX menus.

  For information on assigning IP addresses dynamically in a user profile, see “Dynamic address assignment” on page 1-20.

- route-*n*

  A route-n profile defines static routes used by the MAX to initialize its routing table. The MAX queries route-1, then route-2, then route-3, etc., until it receives an authentication reject from RADIUS. Each profile is limited to a maximum of 25 routes to enable it to fit into one Ethernet packet. See “Static IP routes” on page 1-21 for more details.

```
route-1 Password = "ascend", User-Service = Dialout-Framed-User
<tab>Framed-Route = "10.0.100.0/24 10.0.100.1 1 n homer-out"

route-2 Password = "ascend", User-Service = Dialout-Framed-User
<tab>Framed-Route = "10.0.200.0/24 10.0.200.1 1 n inu-out"
```

  The Framed-Route attribute takes two IP addresses: the first is the IP address of a host or subnet reached by this route, and the second is the address of the gateway at the remote end of the connection. The 0.0.0.0 gateway address is a wildcard entry replaced by the caller’s IP address.

  Following the two IP addresses is the metric for this route, followed by a “y” if this route is private, or “n” if it is not private.

  The last value specified in the Framed-Route attribute is the user name of the dialout RADIUS profile that the route uses (see the information on outdial users, next).

  If the MAX has a Connection Profile that reaches the gateway rather than an “outdial users” profile, do not specify the name as the last value for the Framed-Route attribute.

- outdial users

  An outdial users profile defines dialout profiles. At this time, separate profiles are required for dialin and dialout users. It is recommended (but not required) that dialin user X has a dialout profile named X-out.

This example user profile is associated with a route-n profile that specifies the user name “homer-out” (see the information on route-n profiles, immediately preceding). It may also be associated with a user profile whose user name is “homer”.

```
homer-out Password = "ascend", User-Service = Dialout-Framed-User
<tab>User-Name = "homer",
<tab>Ascend-Dial-Number = "31",
<tab>Framed-Protocol = PPP,
<tab>Framed-Address = 10.0.100.1,
<tab>Framed-Netmask = 255.255.255.0,
<tab>Ascend-Metric = 2,
<tab>Framed-Routing = None,
<tab>Framed-Route = "10.5.0.0/24 10.0.100.1 1",
<tab>Ascend-Idle-Limit = 30,
<tab>Ascend-Send-Auth = Send-Auth-PAP,
<tab>Ascend-Send-Secret = "passwrd1"
```

The Framed-Route attribute is required in a dialout-framed-user entry to establish a route between the caller and the called host (which might be a router).

The default profile

If you create a profile with the user name DEFAULT and place that profile as 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. For example, this DEFAULT profile allows terminal server users log in using their UNIX account name and password:

```
DEFAULT Password = "UNIX"
<tab>User-Service = Login-User,
<tab>Login-Service = Telnet
```

Make sure that the DEFAULT profile is last in the file—any profiles that follow the DEFAULT entry are ignored.

Passwords in a profile

The password is an encrypted password required to authenticate the caller, which may be up to 252 characters in length. Or, if you are running the Ascend RADIUS daemon and dictionary file, the password may be one of the following reserved words:

- The keyword Ascend-CLID (for CLID authentication)
- A keyword indicating external authentication

A keyword for CLID authentication

The keyword Ascend-CLID used as the profile password indicates CLID authentication.

There are a number of other conditions and attributes that affect how CLID authentication takes place and whether it will be sufficient authentication to establish the incoming session.

Note: CLID authentication does not apply to non-ISDN calls or to calls where CLID is not available.

The first condition is the setting of the Clid Auth parameter in the PPP Options submenu of the MAX Answer Profile. If that parameter is set to Required or Prefer, the authentication request is sent to RADIUS is sent with the calling party’s phone number as the login name and Ascend-CLID as the password. The users file must contain a profile with that phone number as the user name and Ascend-CLID as the password, for example:

```
5551212 Password = "Ascend-CLID" User-Service = Dialout-Framed-User
<tab>Ascend-Require-Auth = Require-Auth,
<tab>User-Name = "real-user-name"
<tab>Ascend-Send-Auth = Send-Auth-CHAP,
<tab>Framed-Protocol = PPP,
<tab>Framed-Address = 10.0.200.1,
<tab>Framed-Netmask = 255.255.255.0
```

The second condition that affects how CLID authentication is performed is the Ascend-Require-Auth attribute in the Ascend-CLID profile. If that attribute is set to Require-Auth, it means that the call must go through a second-tier name-password authentication, whether or not CLID authentication succeeds. If the parameter is set to Not-Require-Auth and CLID authentication passes, no further authentication is needed.

To perform the second-tier authentication required by the Ascend-Require-Auth attribute, another user profile is required. Both profiles are subject to a number of conditions that match that enable the RADIUS server to match them up for establishing the session.

- The Ascend-CLID profile must include the User-Name attribute, and the user name of the second profile must match that value.
- The Ascend-CLID profile must include the Ascend-Send-Auth parameter specifying the authentication protocol to be used for verifying the user’s password.
- All other session attributes specified in the Ascend-CLID profile must also be specified in the second user profile with the same values.

These two profiles implement a full CLID authentication scheme:

```
5551212 Password = "Ascend-CLID" User-Service = Dialout-Framed-User
<tab>Ascend-Require-Auth = Require-Auth,
<tab>User-Name = "Joel",
<tab>Ascend-Send-Auth = Send-Auth-CHAP,
<tab>Framed-Protocol = PPP,
<tab>Framed-Address = 10.0.4.1

Joel Password = "xyzzy"
<tab>User-Service = Login-User,
<tab>Login-Service = Telnet,
<tab>Login-Host = 10.0.4.1
```

Keywords for external authentication

This section describes the keyword passwords that indicate to the RADIUS server that authentication will use an external database or an external authentication server. External authentication using an ACE or SAFEWORD server is described in detail in the chapter on Security Cards in the *MAX Security Supplement*. These are the keyword passwords:

- UNIX

  You can request validation using the /etc/password file on the UNIX host by setting the Password field to UNIX, as shown in this example:

  ```
  ascend1 Password = "UNIX"
  <tab>User-Service = Framed-User,
  <tab>Framed-Protocol = PPP,
  <tab>Framed-Address = 10.0.2.1,
  <tab>Framed-Netmask = 255.255.255.0
  ```

  Setting the password to UNIX provides authentication through the normal UNIX authentication procedures, as for a user login.

- SAFEWORD

  You can request validation via the Enigma Logic SafeWord dynamic password library by setting Password to SAFEWORD, as shown below (see the *MAX Security Supplement* for more information).

  ```
  ascend3 Password = "SAFEWORD"
  <tab>User-Service = Framed-User,
  <tab>Framed-Protocol = PPP,
  <tab>Framed-Address = 10.0.3.1,
  <tab>Framed-Netmask = 255.255.255.0
  ```

- ACE

  You can request validation via the Security Dynamics ACE dynamic password library by setting Password to ACE, as shown below. This example uses token caching for 90 minutes (see the *MAX Security Supplement* for details).

  ```
  ascend4 Password = "SAFEWORD", Ascend-Token-Expiry = 90
  <tab>Ascend-Receive-Secret = "shared secret",
  <tab>User-Service = Framed-User,
  <tab>Framed-Protocol = PPP,
  <tab>Framed-Address = 10.0.3.1,
  <tab>Framed-Netmask = 255.255.255.0
  ```

Note: Any ACE entry may be used to authenticate multiple users behind a single remote router (such as an Ascend Pipeline unit) by having a profile in which the user name is set to the Pipeline’s system name and Password is set to ACE. When the user enters the dynamic password obtained from a security card, the user must enter it in this format:

```
password.realname
```

where *realname* is the user’s real name. The *realname* will be presented to the ACE server instead of the name of the Pipeline. Token caching will still function normally. All users will share the same profile, and all accounting will use the Pipeline name, not the real user name.

Password and Ascend-Receive-Secret

When you are passing authentication requests to an external server such as an ACE or SAFEWORD server, you can support PAP-TOKEN-CHAP or CACHE-TOKEN authentication modes by using the Ascend-Receive-Secret attribute to handle the secondary password. For example:

```
asc5 Password="ACE", Ascend-Token-Expiry=90, Ascend-Token-Idle=80
<tab>Ascend-Receive-Secret="shared secret", User-Service=Framed-User,
<tab>Framed-Protocol=PPP,
<tab>Framed-Address=10.0.3.1,
<tab>Framed-Netmask=255.255.255.0
```

See the chapter on Security Cards in the *MAX Security Supplement* for details.

Password expiration

The Ascend RADIUS daemon supports password aging and expiration as well as a method for enabling dial-in users to replace expired passwords under certain conditions. This profile will cause this password to expire on 96/02/15 and if the password is changed remotely, the new password will have a duration of 180 days.

```
user Password = "aging", Ascend-PW-Expiration = "Feb 15 1996"
<tab>User-Service = Login-User,
```

```
<tab>Login-Service = Telnet,
<tab>Ascend-PW-Lifetime = 180
```

Note: If the Ascend RADIUS daemon is running in DBM mode, it accepts a user's replacement for an expired password, but does not allow that user immediate access to the network. The daemon does not recognize the new password until you rebuild the users file database by running builddbm again.

See the section on RADIUS servers in the *MAX Security Supplement* for more information about how users modify their expired passwords with the Ascend daemon.

User service

The User-Service attribute defines the type of service to be enabled for the call. If this attribute is not specified, both framed and unframed services are available.The attribute can be set to one of these values:

- Framed-User

  The Framed-User service is used for PPP or SLIP framing. For example, this profile defines a PPP-encapsulated call that is assigned an IP address and subnet mask:

  ```
  ascend1 Password = "pwd", Ascend-PW-Expiration = "Sep 30 1995"
  <tab>User-Service = Framed-User,
  <tab>Framed-Protocol = PPP,
  <tab>Framed-Address = 10.0.4.1,
  <tab>Framed-Netmask = 255.255.255.0,
  <tab>Ascend-Metric = 2,
  <tab>Framed-Routing = None,
  <tab>Ascend-Idle-Limit = 30
  ```

  (This type of connection can access the MAX user interface if PPP encapsulates a Telnet session to the MAX.)

- Login-User

  The Login-User service indicates a terminal server, raw TCP, or Telnet session. For example, this profile causes an auto-telnet to 10.0.4.1 upon login:

  ```
  Dave Password = "xyzzy"
  <tab>User-Service = Login-User,
  <tab>Login-Service = Telnet,
  <tab>Login-Host = 10.0.8.1
  ```

  Telnet users can either connect to the MAX user interface, or be forwarded on to another IP host, as is the case in this example profile. Because User-Service=Login-User, the call cannot be PPP encapsulated, nor can the caller select PPP or SLIP from the MAX terminal server menu.

- Dialout-Framed-User

  Profiles with User-Service=Dialout-Framed-User *cannot* be used to authenticate incoming calls. This assignment denies dial-in RADIUS requests and must appear in the first line with the name of the user entry, for example:

  ```
  robin-out Password = "ascend" User-Service = Dialout-Framed-User
  ```

  This User-Service setting has two applications: to define tables that can be queried, such as static route tables and address pools, and to define profiles for users who can dial-out through the MAX. See the information on "route-*n*" and "outdial users" below "Pseudo-user profiles" on page 1-12.

- Unspecified

  Sometimes User-Service is unspecified, allowing both framed and unframed connections. For example, if a user wishes to run SLIP (a framed protocol) over a modem connection, the following users file entry allows both terminal server login through a modem and SLIP:

  ```
  thf Password = "MbsYXaaP2
  <tab>Framed-Protocol = SLIP,
  <tab>Framed-Address = 10.0.6.1,
  <tab>Framed-Netmask = 255.255.255.255
  ```

Login service for terminal server sessions

The Login-Service attribute specifies the type of login session to be established for a login-user. It can be set to Telnet or TCP-Clear.

Figure 1-1 shows how the raw TCP session is initiated for a terminal server login session.

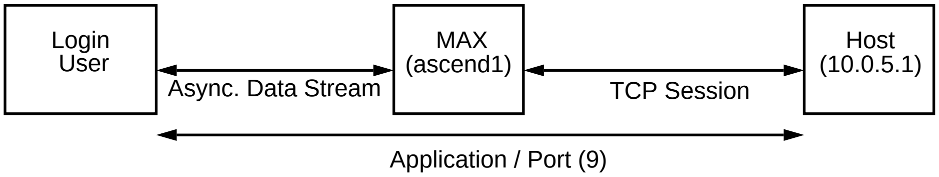


Figure 1-1 TCP-Clear implementation

Ascend’s implementation of Login-Service=TCP-Clear requires an asynchronous connection between the caller and the MAX. Therefore the MAX must be equipped with digital modems or V.110 modules, or the call must be V.120 encapsulated. Furthermore, Login-Service=TCP-Clear rejects PPP encapsulated calls whether synchronous or asynchronous.

This profile causes an auto-telnet to 10.0.4.1 upon login:

```
Joel Password = "xyzzy"
<tab>User-Service = Login-User,
<tab>Login-Service = Telnet,
<tab>Login-Host = 10.0.4.1
```

This profile will start a raw TCP connection to 10.0.5.1, port 23:

```
test1 Password = "test1"
<tab>Login-Service = TCP-Clear,
<tab>Login-Host = 10.0.5.1,
<tab>Login-TCP-Port = 23
```

This profile will start a raw TCP connection to 10.0.6.1, port 7:

```
test2 Password = "test2"
<tab>Login-Service = TCP-Clear,
<tab>Login-Host = 10.0.6.1,
<tab>Login-TCP-Port = 7
```

This profile starts a telnet connection to 10.0.7.1, port 25:

```
test3 Password = "test3"
```

```
<tab>Login-Service = Telnet,
<tab>Login-Host = 10.0.7.1,
<tab>Login-TCP-Port = 25
```

Note: You define a custom menu on a per-profile basis using the Ascend-Menu-Selector and Ascend-Menu-Item attributes.

Additional terminal server options

Several new attributes have been added to the Ascend RADIUS dictionary to support additional terminal server features. For details on these attributes, see Chapter 2, "RADIUS Attributes."

- Reply-Message

  A RADIUS attribute that can be sent with an Access-Accept, Access-Reject, or other packets sent as a reply to an Access-Request.

- Ascend-Menu-Item and Ascend-Menu-Selector

  You can configure a profile to present the user with a subset of terminal server commands and a selection prompt for choosing a command from that subset by using these attributes. The user will not have access to the regular menu or to the terminal server command line.

  For example, for this sample profile:

  ```
  emma Password = "m2dan", User-Service = Login-User
  <tab>Ascend-Menu-Item="show ip stats;Display IP Stats",
  <tab>Ascend-Menu-Item="ping 1.2.3.4;Ping server",
  <tab>Ascend-Menu-Item="telnet 10.2.4.5;Telnet to Ken’s machine",
  <tab>Ascend-Menu-Item="show arp;Display ARP Table"
  <tab>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:
  ```

  Valid user input in this example is 1 through 4, or q to quit.

- Ascend-PPP-VJ-Slot-Comp

  This is an attribute that instructs the MAX to not use slot compression when sending VJ compressed packets over a PPP link.

- Ascend-PPP-VJ-1172

  This is an Ascend-specific attribute that instructs the MAX to use the 0x0037 value for the VJ compression type.

- Ascend-PPP-Asynch-Map

  This is an Ascend-specific attribute which gives the MAX the async control character map for the PPP session. The specified control characters are passed through the PPP link as data and used only by applications run over the link. You can 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.

- Ascend-Third-Prompt

  An Ascend-specific attribute which returns the string entered by the terminal server user in response to the prompt set up by the 3rd Prompt parameter. The string used for the 3rd

Prompt can be up to 20 characters. For example, if you specify 3rd Prompt=Password2>>, the terminal server displays these prompts:

```
Login:
Password:
Password2>>
```

The user can enter up to 80 characters after this prompt. If the user enters more than 80, the input is truncated to 80 when it is stored in the Ascend-Third-Prompt attribute.

PPP and TCP/IP configurations

The Framed-Protocol attribute defines the type of protocol associated with a particular type of call. It can be set to PPP, SLIP, MPP, EURAW, EUUI, COMB, or FR. For example, this profile sets the Framed-Protocol to PPP and passes back the specified IP address and netmask to establish the session.

```
ascend1 Password = "pwd", Ascend-PW-Expiration = "Sep 30 1995"
<tab>User-Service = Framed-User,
<tab>Framed-Protocol = PPP,
<tab>Framed-Address = 10.0.1.1,
<tab>Framed-Netmask = 255.255.255.0,
<tab>Ascend-Metric = 2,
<tab>Framed-Routing = None,
<tab>Ascend-Idle-Limit = 30
```

Dynamic address assignment

Dynamic IP address assignment requires PPP encapsulation. To specify dynamic address assignment in a user profile, use the Ascend-Assign-IP-Pool attribute.

The value of Ascend-Assign-IP-Pool specifies the pool’s index number, as defined in the pools-name profile (see page 1-13) or the MAX Ethernet Profile. For example:

```
ascend1 Password = "pipeline"
<tab>User-Service = Framed-User,
<tab>Framed-Protocol = PPP,
<tab>Framed-Routing = None,
<tab>Ascend-Assign-IP-Pool = 1,
<tab>Ascend-Idle-Limit = 30,
<tab>Framed-Route = "10.0.0.1 0.0.0.0 1"
```

This profile assigns the user an address from Pool 1 and adds a route to 10.0.0.1 with the user’s address as the gateway to that route. Depending on the setting of the Pool Only parameter in the MAX Ethernet Profile, the MAX may or may not allow the caller to reject the dynamic assignment and use his own IP address.

For details on how the MAX handles dynamic address assignment, see the chapter on Configuring the MAX as an IP Router in the *MAX ISP and Telecommuting Configuration Guide*.

IP direct

The Ascend-IP-Direct attribute specifies an IP address to which the MAX redirects all IP packets received from the user. When you include this attribute in a profile, the MAX bypasses all internal routing and bridging tables and sends all packets received on this connection’s WAN interface to the specified IP address. Ascend-IP-Direct does not affect outbound packets.

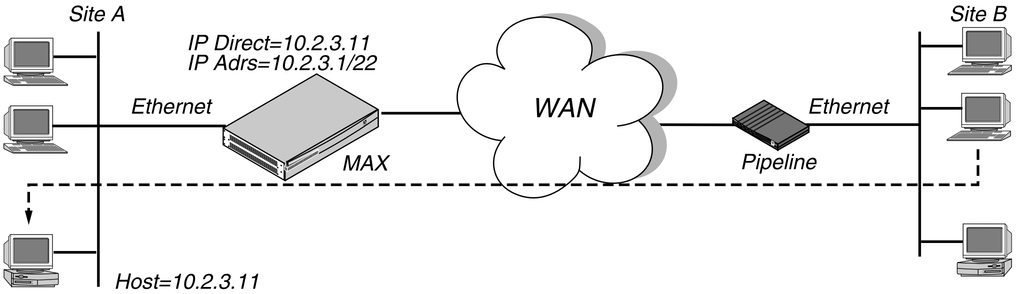


Figure 1-2 IP redirection

Static IP routes

Static IP routes are specified in the users file by using a route-n pseudo-user profile, as described in the “route-*n*” part of “User name in a profile” on page 1-11.

When an outgoing packet is transmitted over one of these static routes, it uses the calling, authentication, and encapsulation parameters set up in an outgoing RADIUS Connection Profile. The static routes are uploaded from RADIUS to the MAX at start up or whenever a user executes the Upd Rem Cfg command from the MAX user interface.

The following example shows two RADIUS users file entries defining the static routes associated with outgoing Connection Profiles also on the RADIUS server:

```
route-1 Password = "ascend" User-Service = Dialout-Framed-User
<tab>Framed-Route = "10.0.200.33/29 10.0.200.37 1 n robin-out"
<tab>Framed-Route = "10.0.200.50/29 10.0.200.37 1 n robin-out"
<tab>Framed-Route = "10.0.200.47/29 10.0.200.49 1 n thf-out"

route-2 Password = "ascend" User-Service = Dialout-Framed-User
<tab>Framed-Route = "11.0.200.33/29 11.0.200.37 1 n matt-out"
<tab>Framed-Route = "12.0.200.47/29 11.0.200.49 1 n dhersh-out"
```

When Framed-Route appears in a dialout users file entry, the routes are downloaded by the MAX during startup or reset. They remain in effect until the next restart or until overwritten by dynamic updates or Connection Profiles.

In some cases, you might wish to update the MAX’s routing tables when connecting to a framed-user. For dial-in framed-users, these routes only exist during the time the call is online.

⚠ **Caution: When you enter a gateway (nonzero) address different from the caller’s address, the static route of a dial-in framed-user persists even after the connection goes offline.**

Static routes can also be defined for dial-in framed users. The following users file entry defines a Connection Profile where a route to 10.0.0.1 is added with the users address as the gateway. Routes defined in this way exist only as long as the connection is online.

```
ascend4 Password = "pipeline"
<tab>User-Service = Framed-User,
<tab>Framed-Protocol = PPP,
<tab>Framed-Routing = None,
<tab>Ascend-Assign-IP-Pool = 1,
<tab>Ascend-Idle-Limit = 30,
<tab>Framed-Route = "10.0.0.1 0.0.0.0 1"
```

IPX routing configuration

This profile enables IPX routing, turns off IP routing, and specifies the mode of the IPX router module in the MAX:

```
ipxtest Password = "netware"
<tab>Ascend-Route-IPX = Route-IPX-Yes,
<tab>Ascend-Route-IP = Route-IP-No,
<tab>Ascend-IPX-Peer-Mode = Peer-Mode-Router
```

Bridging configuration

This profile turns off IPX and IP routing. The connection will use only protocol-independent bridging at the link level:

```
bridge Password = "bridge"
<tab>Ascend-Bridge = Bridge-Yes,
<tab>Ascend-Route-IP = Route-IP-No,
<tab>Ascend-Route-IPX = Route-IPX-No
```

Filters

Filters are an Ascend extension to RADIUS. Two string fields are defined in the RADIUS dictionary: Ascend-Data-Filter and Ascend-Call-Filter. The Ascend-Data-Filter defines a data/routing filter. An Ascend-Call-Filter defines a call filter (a filter that affects whether the MAX places a call or keeps a call active). When you define a filter in a user profile, it applies to filters sent or received by that user. None of the keywords associated with the Ascend-Data-Filter and Ascend-Call-Filter attributes are case-sensitive.

Data filters and call filters are always one of two types: IP (affecting TCP/IP/UDP packets only) or Generic (affecting all packet types).

Note: For information about how filters work, see the chapter on Using Filters in the *MAX ISP and Telecommuting Configuration Guide*.

IP filters

This profile shows an IP data filter that specifies that all TCP/IP/UDP outbound packets will be forwarded:

```
ascend1 Password = "ascend", User-Service = Dialout-Framed-User
<tab>User-Name = "inu",
<tab>Ascend-Dial-Number = 555-1234,
<tab>Framed-Address = 10.0.200.1,
<tab>Framed-Netmask = 255.255.255.0,
<tab>Ascend-Metric = 1,
<tab>Framed-Routing = None,
<tab>Ascend-Idle-Limit = 20,
<tab>Ascend-Send-Auth = Send-Auth-CHAP,
<tab>Ascend-Send-Secret = "kuro",
<tab>Ascend-Data-Filter = "ip out forward"
```

An IP filter uses the following syntax (where brackets indicate an optional item):

```
Ascend-Data-Filter = "ip dir action [ dstip n.n.n.n/nn]
[ srcip n.n.n.n/nn] # [ proto [ dstport cmp value] [ src port cmp value]
[ est]]"
```

```
Ascend-Call-Filter = "ip dir action [ dstip n.n.n.n/nn]
[ srcip n.n.n.n/nn] # [ proto [ dstport cmp value] [ src port cmp value]
[ est]]"
```

A filter definition cannot contain newlines. The syntax is shown on multiple lines here for printing purposes only.

- ip

  “ip” is the keyword indicating an IP filter.

- dir

  This parameter indicates filter direction. It must be either *in* (to filter packets coming in to the MAX) or *out* (to filter packets going out of the MAX).

- action

  This parameter specifies what to do with a packet that matches the filter. It must be either *forward* or *drop*.

- dstip n.n.n.n/nn

  “dstip” is a keyword indicating “Destination IP address.” If this parameter and its IP address are not present, the filter will match any IP addresses. If a netmask portion (/nn) of the address is present, the MAX only compares the masked bits.

- srcip n.n.n.n/nn

  “srcip” is a keyword indicating “Source IP address.” If this parameter and its IP address are not present, the filter will match any IP addresses. If a netmask portion (/nn) of the address is present, the MAX only compares the masked bits.

- proto

  “proto” is a keyword indicating “Protocol.” The protocol may be specified as either a name or a number. The supported names and numbers are least icmp(1), tcp(6), udp(17), ospf(89).

- dstport cmp *value*

  “dstport” is a keyword indicating “Destination Port.” This parameter is valid only when the protocol is tcp(6) or udp(17). If the destination port is not specified, the filter matches any port.

  “cmp” is a keyword indicating how to compare the specified value to the actual destination port. It can have the value<, =, >, or !=.

  The value can be entered as a number or a name. Supported names 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.” This parameter is valid only when the protocol is tcp(6) or udp(17). If the source port is not specified, the filter matches any port.

  “cmp” is a keyword indicating how to compare the specified value to the actual source port. It can have the value <, =, >, or !=.

The value can be entered as a number or a name. Supported names are ftp-data(20), ftp(21), telnet(23), smpt(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

  “est” is a keyword that, if present, indicates that the filter matches a packet only if a TCP session is already established.It is valid only when the protocol field is tcp(6).

Generic filters

This profile shows one IP data filter and two generic data filters. Together, these filters specify that IP and ARP packets will be sent out by the MAX but that all other packets will be dropped.

```
ascend1 Password = "ascend", User-Service = Dialout-Framed-User
<tab>User-Name = "inu",
<tab>Ascend-Dial-Number = 555-1234,
<tab>Framed-Address = 10.0.200.1,
<tab>Framed-Netmask = 255.255.255.0,
<tab>Ascend-Metric = 1,
<tab>Framed-Routing = None,
<tab>Ascend-Idle-Limit = 20,
<tab>Ascend-Send-Auth = Send-Auth-CHAP,
<tab>Ascend-Send-Secret = "kuro",
<tab>Ascend-Data-Filter = "ip out forward",
<tab>Ascend-Data-Filter = "generic out forward 12 ffff 0806",
<tab>Ascend-Data-Filter = "generic out drop 0 0 0"
```

A generic filter uses the following syntax (where brackets indicate an optional item):

```
Ascend-Data-Filter = "generic dir action offset mask value
[ comparison] [ more]"
```

```
Ascend-Call-Filter = "generic dir action offset mask value
[ comparison] [ more]"
```

A filter definition cannot contain newlines. The syntax is shown on multiple lines here for printing purposes only.

- generic

  “generic” is the keyword indicating a generic filter.

- dir

  This parameter indicates filter direction. It must be either *in* (to filter packets coming in to the MAX) or *out* (to filter packets going out of the MAX).

- action

  This parameter specifies what to do with a packet that matches the filter. It must be either *forward* or *drop*.

- offset *n*

  “offset” is a keyword indicating a byte offset into a frame. The filter will begin comparing the contents of the packets after ignoring the specified number bytes at the beginning of the packet.

- mask*nnnnnnnnnnnn*
- “mask” is a keyword indicating which bits to compare in a segment of the packet, which 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*nnnnnnnnnnnn*
- "value" specifies the value to compare to the packet contents at the specified offset in packet. *Note: The length of the value must be the same as the length of the mask or the filter will be ignored.*
- comparison *value*

  This keyword specifies how a packet's contents are compared to the value specified in this filter. Its value can be == or !=, for Equal or NotEqual. If it is not specified, its value is Equal.
- more

  This keyword, if present, specifies that the next filter definition in the profile is to be applied to the current packet before the Forward or Drop decision is made. *Note: The dir and action values of the next entry must be the same as the dir and action of the current entry or the more flag will be ignored.*

RADIUS accounting

RADIUS accounting is a way to log information about three types of events: start session, stop session, and failure-to-start session. Sessions can be either terminal server or bridging/routing sessions.

A group of attributes is sent with each of these three types of events, and the event record is time-stamped. For example, a start session event includes the user-name attribute, the IP address attribute, and so forth.

These example RADIUS accounting records show the start and stop of an IP routing session:

```
Tue Nov 28 12:00:41 1995
User-Name = "ronc1" NAS-Identifier = 206.65.212.46
NAS-Port = 20113
Acct-Status-Type = Start
Acct-Delay-Time = 0
Acct-Session-Id = "7"
Acct-Authentic = RADIUS
Framed-Protocol = PPP
Framed-Address = 11.0.0.1

Tue Nov 28 12:02:48 1995
User-Name = "ronc1" NAS-Identifier = 206.65.212.46
NAS-Port = 20113
Acct-Status-Type = Stop
Acct-Delay-Time = 0
Acct-Session-Id = "7"
Acct-Authentic = RADIUS
Acct-Session-Time = 128
Acct-Input-Octets = 2421
Acct-Output-Octets = 1517
Acct-Input-Packets = 79
Acct-Output-Packets = 47
Framed-Protocol = PPP
Framed-Address = 11.0.0.1
```

Note: Some attributes are optional, and their absence in an event record may have significant meaning. See the description of individual attributes in Chapter 2, "RADIUS Attributes," for details.

When to use RADIUS accounting

RADIUS accounting is typically used for billing purposes, using the information in an event record about who called and how long the session lasted. It is also used for troubleshooting RADIUS and MAX operations, using information about how many login failures occurred and the characteristics of the failed attempts.

The attribute descriptions in Chapter 2, "RADIUS Attributes," describe when an attribute is sent to the accounting process and included in an event record.

How to set up RADIUS accounting

To set up RADIUS accounting after installing the most recent Ascend RADIUS daemon, as described in “Installing and integrating RADIUS” on page 1-3, follow these steps:

1. Add a line to /etc/services file identifying the RADIUS daemon’s accounting port. For example:

   ```
   radacct<tab>1646/udp   #radius-accounting
   ```

   The port number you specify must match the port number specified in the Acct Port parameter in the Acct submenu of the MAX Ethernet Profile. You can use a value other than 1646 as long as the Acct Port setting is matches the value. See the*MAX Security Supplement* for more information.

2. If necessary, create the /usr/adm/radacct directory.

   Or, you can use the –a option when invoking the daemon to specify a different directory in which to store accounting information. The accounting process in the daemon creates a file named “detail” in /usr/adm/radacct or the specified directory. The “detail” file will contain accounting records.

3. Start the RADIUS daemon including the –A option, for example:

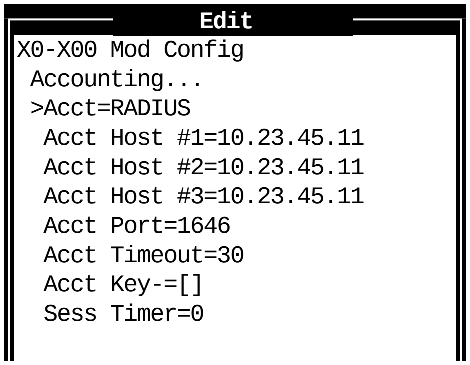
   ```
   radiusd -A services
   ```

   You can run the daemon in DBM mode if you wish, as long as you supply the –A option that tells the daemon which port to listen on for accounting information.

4. In the MAX configuration interface, open the Ethernet Profile, and then open the Accounting submenu.

5. Set the Acct parameter to RADIUS.

6. Enter the IP address of the RADIUS host in the Acct Host #1 parameter.



```
                Edit
X0-X00 Mod Config
 Accounting...
 >Acct=RADIUS
  Acct Host #1=10.23.45.11
  Acct Host #2=10.23.45.11
  Acct Host #3=10.23.45.11
  Acct Port=1646
  Acct Timeout=30
  Acct Key-=[]
  Sess Timer=0
```

7. Enter the UDP port number you specified for the accounting process of the daemon in /etc/services in the Acct Port parameter.

   Or, if you used the “incr” keyword to the –A option when invoking the daemon, specify the number of the UDP port used for authentication services +1.

8. Enter the RADIUS client password in the Acct Key parameter, exactly as it appears in the RADIUS clients file.

9. Unless you are using a customized RADIUS accounting process that can respond to session timer requests, leave the Sess Timer parameter set to 0.

   See “Extensions for custom RADIUS daemons” on page 1-28 for details.

10. Close the Auth submenu, and then close the Ethernet Profile, saving your changes.

List of accounting attributes

These attributes can be sent to or from the RADIUS accounting daemon. The RADIUS server sends an Accounting-Start packet (Acct-Status-Type=Start) when a session starts. It sends an Accounting-Stop packet (Acct-Status-Type=Stop) when a session terminates. Accounting packets contain attributes that report the cause of a session termination and its state prior to termination; the number of octets and packets sent/received prior to authentication, and so forth.

Table 1-4. RADIUS accounting attributes

Attribute (Number)	Value
Acct-Authentic (45)	A string indicating how the call was authenticated: RADIUS or Local
Acct-Delay-Time (41)	The number of seconds the MAX has been trying to send this Accounting packet
Acct-Input-Octets (42)	The number of octets received during the session
Acct-Input-Packets (47)	The number of packets received during the session
Acct-Output-Octets (43)	The number of octets sent during the session
Acct-Output-Packets (48)	The number of packets sent during the session

Table 1-4. RADIUS accounting attributes (continued)

Attribute (Number)	Value
Acct-Session-Id (44)	A unique numeric string identified with the bridging, routing, or terminal server session reported in this Accounting packet
Acct-Session-Time (46)	The number of seconds the session has been logged in
Acct-Status-Type (40)	Requests that have Acct-Status-Type=Start are accounting-start packets and requests that have Acct-Status-Type=Stop are accounting-stop packets.
Ascend-Connect-Progress (196)	The state of the connection before it is disconnected
Ascend-Data-Rate (197)	The data rate of the connection in bits per second
Ascend-Disconnect-Cause (195)	The reason a connection was taken offline
Ascend-First-Dest (189)	Records the destination IP address of the first packet received on a connection after the connection has been authenticated
Ascend-Maximum-Time (194)	The maximum length of time in seconds that any session is allowed before being taken offline
Ascend-Multilink-ID (187)	Applies to sessions that are part of a “Multilink bundle”
Ascend-Num-In-Multilink (188)	Applies to sessions that are part of a “Multilink bundle”
Ascend-Number-Sessions (202)	Used in conjunction with the Class attribute to specify the number of active sessions of each class reported to the RADIUS accounting server
Ascend-Pre-Input-Octets (190)	Records the number of input octets before authentication
Ascend-Pre-Input-Packets (192)	Records the number of input packets before authentication
Ascend-Pre-Output-Octets (191)	Records the number of output octets before authentication
Ascend-Pre-Output-Packets (193)	Records the number of output packets before authentication
Ascend-PreSession-Time (198)	The length of time in seconds from when a call connected to when it completes authentication

Extensions for custom RADIUS daemons

This section describes features that are supported in the MAX software, but are not implemented in the Ascend RADIUS daemon or the Livingston RADIUS daemon. This information is intended for programmers building a customized RADIUS daemon. For details on how to construct RADIUS packets, see draft-ietf-nas-radius-02.txt, which is available from Livingston on the Internet.

- Access-Terminate-Session packets (RADIUS code 31)

  Access-Terminate-Session packets are RADIUS Access-Response packets identified by the code number 31. Only RADIUS daemons that have been customized to support this packet code send Access-Terminate-Session packets. (Neither the Ascend RADIUS daemon nor the Livingston RADIUS daemon implement this packet type.)

  Access-Terminate-Session packets can include only one attribute, the Reply-Message attribute, which can contain 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" with the Access-Terminate-Session.

- Ascend-Session-Timer packets (RADIUS code 33)

  Ascend-Session-Timer packets are RADIUS response packets identified by the code number 33. Only RADIUS daemons that have been customized to recognize this packet code respond to Ascend-Session-Timer requests from the MAX. (Neither the Ascend RADIUS daemon nor the Livingston RADIUS daemon respond to these requests.)

  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 a code 33 packet.

  Ascend-Session-Timer packets contain two attributes, the NAS-Identifier attribute (4), followed by a list of Ascend-Number-Sessions attributes (202).

  The Ascend-Number-Sessions attribute has two parts: the first is the number of open sessions in a particular class, and the second is the actual class. If some open sessions have no known class, they are reported by this attribute also.

RADIUS Attributes

2

This chapter discusses RADIUS attributes found in users file entries, and contains these sections:

Numerical listing of attributes 2-2

Cross reference of attributes and parameters 2-34

Each listing provides information in this format:

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.

See Also: The See Also text points you to related information.

Numerical listing of attributes

This section describes many of the attributes found in users file entries on the RADIUS server. With the exception of attributes beginning with "Ascend", all attributes are defined in the Livingston RADIUS draft.

Note: The following descriptions specify the kind of packets in which an attribute is sent. Bear in mind that when an attribute is not sent in an Accounting packet, the session is unframed.

User-Name (Attribute 1)

Description: User-Name indicates the name of the user that the RADIUS server will authenticate.

Usage: You can specify up to 31 alphanumeric characters.

Dependencies: This attribute is sent in the following types of packets:

- Accounting-Request packets in which Acct-Status-Type=Stop.

  These packets are sent at the end of a session. If a session fails to be authenticated, the User-Name attribute is not sent with this type of packet.
- Authentication-Response packets.
- Authentication-Request packets in which Acct-Status-Type=Stop.

User-Password (Attribute 2)

Description: User-Password specifies the password of the user that the RADIUS server will authenticate.

Usage: You can specify up to 20 characters.

Dependencies: This attribute is sent in the following types of packets:

- Authentication-Request packets in which Acct-Status-Type=Stop
- Authentication-Response packets

CHAP-Password (Attribute 3)

Description: CHAP-Password specifies the response value provided by a CHAP (Challenge Handshake Authentication Protocol) user in response to the password challenge.

Dependencies: This attribute is sent in the following types of packets:

- Authentication-Request packets in which Acct-Status-Type=Stop
- Authentication-Response packets

NAS-Identifier (Attribute 4)

Description: NAS-Identifier indicates the IP address of the MAX authenticating the user or sending an Accounting packet. This attribute is analogous to the IP Adrs parameter.

Dependencies: The NAS-Identifier attribute is sent in the following type of packets:

- Accounting-Request packets when the Auth parameter is set to a value other than RADIUS/LOGOUT.

  The NAS-Identifier attribute is sent at the end of a session when Acct-Status-Type=Stop. If the session fails to be authenticated, the attribute is still sent with the packet.
- Authentication-Request packets in which Acct-Status-Type=Stop.
- Authentication-Response packets.

See Also: The Auth and IP Adrs parameters in the *MAX Reference Guide*.

NAS-Port (Attribute 5)

Description: NAS-Port specifies the port on the MAX handling the user session. Specifically, NAS-Port identifies the interface and service the session is using.

Usage: For Ascend products, NAS-Port numbers are 5-digit values in the format `tllcc`:

- `t` can have the value 1 for a digital call, or 2 for an analog call.
- `ll` represents the line number the call is using.
- cc represents the channel on the line the call is using.

A port of 0 (zero) is returned when a port number cannot be calculated.

Dependencies: This attribute is sent in the following types of packets:

- Authentication-Request packets in which Acct-Status-Type=Stop.
- Authentication-Response packets.
- Accounting-Request packets.

  The NAS-Port attribute is sent at the end of a session when Acct-Status-Type=Stop. If the session fails to be authenticated, the attribute is still sent with the packet.

User-Service (Attribute 6)

Description: User-Service specifies the type of services the user can access.

Usage: If an incoming call is authenticated by matching the name and password of a user entry, and the type of call matches the value of the User-Service attribute, the MAX applies the parameters of that entry to the call. If the type of call does not match the User-Service attribute, the MAX rejects the call. If you do not specify a value for this attribute, the MAX does not limit the services the user can access.

User-Service can have one of these values:

- Framed-User

  Incoming calls must use a framed protocol. Incoming unframed calls are rejected.
- Login-User

  The operator can use an asynchronous Telnet connection to log into the terminal server. Incoming framed calls are rejected and the user cannot use any framed protocol. Login-users can start Telnet or raw TCP sessions.
- Dialout-Framed-User

  This value is sent from the MAX during an authentication request. If an entry has User-Service set to this value and it appears on the first line with name and password, the entry does not allow dial-in users.

Dependencies: Keep this additional information in mind:

- Login-User 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 by Framed-User.
- The User-Service attribute is sent in Authentication-Response packets.

Framed-Protocol (Attribute 7)

Description: Framed-Protocol specifies the type of framed protocol allowed to the user. No other framing is allowed.

Usage: These are the values you can specify for Framed-Protocol:

- PPP (1)

  A user requesting access can dial in using MP+, MP, or PPP framing. If the user dials in using any other type of framing, the call is rejected. A user requesting access can also dial in unframed, and then change to PPP framing. 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)

  Outgoing calls request MP+ framing. This value does not apply to incoming calls.
- EURAW (257)

  A user requesting access can dial in using EURAW framing. If the user dials in using any other type of framing, the call is rejected. Outgoing calls use EURAW framing. EURAW is a type of X.75 encapsulation in which IP packets are HDLC encapsulated with a CRC field.
- EUUI (258)

  A user requesting access can dial in using EUUI framing. If the user dials in using any other type of framing, the call is rejected. Outgoing calls use 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.
- COMB (260)

  A user requesting access can dial in using Combinet framing. If the user dials in using any other type of framing, the call is rejected. Outgoing calls use Combinet framing.
- FR (261)

  Outgoing calls use frame relay (RFC 1490) framing. This value does not apply to incoming calls.

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"
       User-Service=Framed-User,
       Framed-Protocol=PPP,
       Framed-Address=10.0.200.225,
       Framed-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
```

Dependencies: Keep this additional information in mind:

- What Framed-Protocol does depends on how you set User-Service (attribute 6):
  - If User-Service=Framed-User or is unspecified, a user requesting access can dial in using the framing specified by Framed-Protocol; other types of framing are rejected.

    A user requesting access can also dial in without using a framed protocol, but can then change only to the framing specified by the Framed-Protocol attribute.
  - If User-Service=Framed-User or is unspecified, and Framed-Protocol has no specified value, the operator can use any framed protocol.
  - If User-Service=Login-User, the user cannot use a framed protocol.
  - If User-Service=Dialout-Framed-User, Framed-Protocol specifies the type of framing used on the outgoing call; incoming calls are rejected.
- The Framed-Protocol attribute is sent in an Accounting-Request packet only if a framed protocol is in use and you have not set Auth=RADIUS/LOGOUT.
- The Framed-Protocol attribute is sent in Authentication-Response packets.

See Also: “User-Service (Attribute 6)” on page 2-3 and the Auth parameter in the *MAX Reference Guide*.

Framed-Address (Attribute 8)

Description: Framed-Address specifies the IP address of the user.

Dependencies: This attribute is sent in an Accounting-Request packet only if a framed protocol is in use and you have not set Auth=RADIUS/LOGOUT.

See Also: “Framed- Protocol (Attribute 7)” on page 2-4, and the Auth and Auth Pool parameters in the *MAX Reference Guide*.

Login-Host (Attribute 14)

Description: Login-Host specifies the host to which the Login-User automatically connects. This access begins immediately after login.

Dependencies: Keep this information in mind:

- The Login-Host attribute is sent in an Accounting-Request packet only if these conditions are true:
  - The user dialed into a terminal server session through one of the MAX’s digital modems or by using V.120 encapsulation.
  - RADIUS authenticated the call.
  - RADIUS authentication specifies a login host.
  - The Auth parameter has a value other than RADIUS/LOGOUT.
- Login-Host has the same functionality as the *host-name* field in the terminal server command-line interface.

  Closing the remote terminal server session also automatically closes the login-host session.
- When User-Service=Login-User and Login-Service=Telnet, the login-host is connected by Telnet.
- When User-Service=Login-User and Login-Service=TCP-Clear, the login-host is connected by raw TCP.
- When User-Service=TCP-Clear, you must specify Login-TCP-Port (attribute 16).
- When User-Service=Framed-User, the Login-Host attribute is ignored.

- If you do not specify a value for the Login-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. See the Host #*n* Addr and Host #*n* Text parameters in the *MAX Reference Guide* for more information.
- The Login-Host attribute is sent in Authentication-Response packets.

See Also: “Login-Service (Attribute 15)” on page 2-6, “Login-TCP-Port (Attribute 16)” on page 2-7, and “User-Service (Attribute 6)” on page 2-3.

Login-Service (Attribute 15)

Description: Login-Service specifies the type of terminal service supported.

Usage: Login-Service can have one of these values:

- Telnet

  Telnet is the only remote terminal server protocol supported.
- TCP-Clear

  Incoming unframed asynchronous calls can start a raw TCP session. Raw TCP establishes a TCP session between the MAX and a host (Login-Host, attribute 14) over which the user can run an application specified by Login-TCP-Port (attribute 16). See the `tcp` terminal server command in the *MAX ISP and Telecommuting Configuration Guide* for further information.

Note: rlogin is currently not supported.

Example: In this example, a Telnet session starts automatically for anyone using the `userx` username and `xyzzy` password. When the Telnet session terminates, the connection also terminates.

```
# This profile causes an auto-telnet to 10.0.200.4 upon login.
userx  Password="xyzzy"
       User-Service=Login-User,
       Login-Service=Telnet,
       Login-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"
       User-Service=Login-User,
       Login-Service=TCP-Clear,
       Login-Host=4.2.3.1,
       Login-TCP-Port=9
```

The line specifying the TCP port using the Login-TCP-Port attribute is optional.

Dependencies: Keep this additional information in mind:

- If you specify both Login-Service and Login-Host (attribute 14), the MAX automatically connects the Login-User to the host specified by Login-Host.
- If you do not specify Login-Service or Login-Host, the Login-User sees either the MAX’s terminal server command-line interface or the terminal server menu interface, depending upon how the MAX is configured.

- The Login-Service attribute is sent in a RADIUS Accounting packet only if these conditions are true:
  - The user dialed into a terminal server session through one of the MAX’s digital modems or by using V.120 encapsulation.
  - RADIUS authenticated the call.
  - RADIUS authentication specifies a login host.
  - The Auth parameter has a value other than RADIUS/LOGOUT.
- The Login-Service attribute is sent in Authentication-Response packets.

See Also: “Login-Host (Attribute 14)” on page 2-5 and “Login-TCP-Port (Attribute 16)” on page 2-7.

Login-TCP-Port (Attribute 16)

Description: Login-TCP-Port specifies the port number to which a TCP session connects. The default is 23. See the Login-Service attribute on page 2-6 for the types of sessions supported.

Dependencies: Keep this additional information in mind:

- Login-TCP-Port has the same functionality as the *port-number* field in the MAX’s terminal server command-line interface.

  For information on the terminal server command-line interface, see the *MAX ISP and Telecommuting Configuration Guide*.
- The Login-TCP-Port attribute is sent in an Accounting-Request packet only if these conditions are true:
  - The user dialed into a terminal server session through one of the MAX’s digital modems or by using V.120 encapsulation.
  - RADIUS authenticated the call.
  - RADIUS authentication specifies a login host.
  - The Auth parameter has a value other than RADIUS/LOGOUT.
- The Login-TCP-Port attribute is sent in Authentication-Response packets.

See Also: “Login-Service (Attribute 15)” on page 2-6 and the Auth parameter in the *MAX Reference Guide.*

Reply-Message (Attribute 18)

Description: Reply-Message carries message text from the RADIUS server to RADIUS clients such as the MAX. Several types of packets, including Authentication-Response, Access-Accept, Access-Reject, and Access-Terminate-Session packets, can include this attribute. In addition, the Reply-Message attribute can set up the banner lines of the MAX’s terminal server.

Usage: You can include Reply-Message in RADIUS users file entries. The maximum number of Reply-Message attributes per profile is 16. Use this format:

```
Reply-Message=string
```

`string` contains the text of the reply message. Enter up to 80 characters.

Example: Suppose you set this users file entry:

```
emma Password=“m2dan”, User-Service=Login-User
Reply-Message=”\r\n\tRemember to pay your bill. \r\n”
```

When Emma logs in, the message “Remember to pay your bill” displays.

In addition to Access-Accept and Access-Reject packets, the MAX recognizes the Access-Terminate-Session packet. If 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 has not paid a bill, the RADIUS server can be customized to send that user the message “You have not paid your bill” with the Access-Terminate-Session packet.

Note: Neither the standard RADIUS daemon nor the Ascend RADIUS daemon send Access-Terminate-Session packets.

Dependencies: Keep this additional information in mind:

- If you do not specify a Reply-Message attribute in a users file entry 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, the message `** Bad Password` appears.

  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 the message `** Session Terminated` to the terminal server user and uses a timer to terminate the login session.

  The RADIUS server discards all input it received before it terminated the session.

Ascend-PW-Expiration (Attribute 21)

Description: Ascend-PW-Expiration specifies an expiration date for a user’s password in the users file entry.

Usage: When the MAX makes an authentication request, the RADIUS server checks the current date against the value of Ascend-PW-Expiration. If the date of the authentication request is the same date or a later date than the value of Ascend-PW-Expiration, the user receives a message saying that the password has expired.

You must specify Ascend-PW-Expiration when you first create a user. Enter the Ascend-PW-Expiration specification on the User/Password line in this format:

```
Ascend-PW-Expiration=”date”
```

`date` consists of a specification for 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.

Example: Your specification might look like this one:

```
emma Password=“m2dan”, User-Service=Login-User, Ascend-PW-Expi-
ration=”November 1, 1995”
```

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 (attribute 208) 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=June 1, 1995, and today's date is October 1, 1995. If the user resets the password today, the value of Ascend-PW-Expiration becomes today's date + Ascend-PW-Lifetime, or October 31, 1995.
- If the password has not expired, the value of Ascend-PW-Expiration overrides the value of Ascend-PW-Lifetime.

  For example, if on October 1, 1995 you set Ascend-PW-Lifetime=30 and Ascend-PW-Expiration=October 15, 1995, the password expires on October 15, 1995. In other words, if the password has not expired, the value of Ascend-PW-Lifetime is irrelevant.
- The Ascend-PW-Expiration attribute is sent in Authentication-Response packets.

See Also: "Ascend-PW-Lifetime (Attribute 208)" on page 2-24.

Framed-Route (Attribute 22)

Description: Framed-Route enables you to add static routes to the MAX's routing table.

When Framed-Route appears in a dialout users file entry, the routes are downloaded by the MAX during startup or reset. They remain in effect until the next restart or until overwritten by dynamic updates or Connection Profiles.

In some cases, you might wish to update the MAX's routing tables when connecting to a framed-user. For dial-in framed-users, these routes exist only during the time the call is online.

⚠ **Caution: When you enter a gateway (nonzero) address different from the caller's address, the static route of a dial-in framed-user persists even after the connection goes offline.**

Usage: Use this format for the Framed-Route attribute:

```
h.h.h.h[/nn] g.g.g.g m [p] [name]
```

- `h.h.h.h[/nn]` is the IP address of a host or subnet reached by this route.

  You must enter the IP address in dotted decimal format. You have the option of including the number of bits in the subnet mask as well.
- `g.g.g.g` is the address of the gateway at the remote end of the connection.

  The 0.0.0.0 gateway address is a wildcard entry replaced by the caller's IP address.When RADIUS authenticates a caller and RADIUS sends the MAX an Access-Accept message with a Framed-Route 0.0.0.0 gateway, the MAX updates its routing tables with the Framed-Route value, but substitutes the caller's IP address for the gateway. 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.
- `m` is the metric for this route.
- `p` has the value `y` if this route is private, or `n` if it is not private.
- `name` is the outgoing RADIUS Connection Profile that the route uses.

  Do not specify a value for `name` when the MAX has a Connection Profile in the standard user interface that reaches the gateway.

Example: The following example shows two RADIUS users file entries defining the static routes associated with outgoing Connection Profiles on the RADIUS server:

```
route-1   Password=“ascend” User-Service=Dialout-Framed-User
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” User-Service=Dialout-Framed-User
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 “
```

Dependencies: The Framed-Route attribute is sent in Authentication-Response packets.

Framed-IPX-Network (Attribute 23)

Description: Framed-IPX-Network specifies a unique, internal IPX network number for the MAX’s Ethernet interface. It also creates a static route to another Ethernet through this Connection Profile.

Framed-IPX-Network corresponds to the IPX Net# parameter in the Connection Profile. IPX Net# specifies the network number of the router at the remote end of the connection. It is optional and has a default value of 0 (zero).

Usage: Enter the network number of the router at the remote end of the connection only if that router requires that the MAX know the router’s network number before connecting. In most cases, you do not need to give this attribute a value. If you use the default value (0), the Connection Profile is still valid, but the MAX does not advertise this route until a connection is made to the given Ethernet.

RADIUS requires that Frame-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 users file. If you specify a value for this attribute, it must be unique within your wide-area IPX network and match the configuration of other routers on the network.

Dependencies: Keep this additional information in mind:

- Framed-IPX-Network is sent in a RADIUS Accounting packet only if a framed protocol is being used and is running under IPX routing.
- Framed-IPX-Network is not sent in an Accounting-Request packet if the parameter Auth=RADIUS/LOGOUT.
- Framed-IPX-Network is sent in Authentication-Response packets.

See Also: The Auth and IPX Net# parameters in the *MAX Reference Guide*.

Class (Attribute 25)

Description: Class can be received by the MAX as part of an authentication-acceptance message from the RADIUS authentication server.

Dependencies: Keep this additional information in mind:

- If the value of Class is known from an authentication-acceptance packet, Class is included in the Accounting-Request packet sent to the RADIUS accounting server, but only when these conditions are true:
  - The Auth parameter is not set to RADIUS/LOGOUT.
  - Acct-Status-Type=Stop in the Authentication-Request packet.
- Class is sent in Authentication-Response packets.
- Class is sent to the RADIUS authentication server when known from an authentication-acceptance packet received through CLID authentication.

See Also: The Auth parameter in the *MAX Reference Guide*.

Client-Port-DNIS (Attribute 30)

Description: Client-Port-DNIS specifies the called-party number, indicating the phone number dialed by the user to connect to this MAX.

DNIS stands for Dialed Number Information Service.

Dependencies: Keep this additional information in mind:

- Client-Port-DNIS is sent only if the called-party number is known.
- Client-Port-DNIS is sent to the RADIUS Accounting server in an Accounting-Request packet if the Auth parameter is set to a value other than RADIUS/LOGOUT.
- Client-Port-DNIS is sent in Authentication-Response packets.

See Also: The Auth parameter in the *MAX Reference Guide*.

Caller-Id (Attribute 31)

Description: Caller-Id specifies the calling-party number, indicating the phone number of the user that has connected to this MAX.

Dependencies: Keep this additional information in mind:

- Caller-Id is sent only if the calling-party number is known.
- Caller-Id is sent to the RADIUS Accounting server in an Accounting-Request packet if the Auth parameter is set to a value other than RADIUS/LOGOUT.
- Caller-Id is sent in Authentication-Response packets.

See Also: The Auth parameter in the *MAX Reference Guide*.

NAS-IP-Address (Attribute 32)

Description: NAS-IP-Address specifies the IP address of the MAX.

Dependencies: The NAS-IP-Address attribute is sent in Authentication-Response packets.

Accounting Attributes (40 through 48)

Description: When the MAX begins a terminal server, bridging, or routing session, it sends an Accounting Start packet to the RADIUS accounting server; this packet describes the type of session being opened and the name of the user opening the session. (The MAX does not send an Accounting Start packet if a call fails authentication or otherwise fails to log in.)

At the end of a session, including cases in which a user fails to authenticate, the MAX sends an Accounting Stop packet including attributes 1, 4, 5, 40, 41, 42, 43, 44, 45 46, 47, 48, 188, 189, 190, 191, 192, 193, 194, 195, 196, 197, and 198. If you are running an unmodified Ascend RADIUS daemon, the information in Accounting packets is saved in a RADIUS log file by the RADIUS accounting server.

Note: In some cases, a session begins with a user login and then authentication follows, such as when a terminal server user is allowed to choose PPP or SLIP after login.
If User-Service=Login-User (attribute 6), or if User-Service is unspecified, an Accounting Start packet is sent after login.

Each accounting attribute is described in the sections that follow.

Acct-Status-Type (Attribute 40)

This attribute marks whether the Accounting packet sent to the RADIUS server is the beginning (Start) or end (Stop) of a bridging, routing, or terminal server session.

The Acct-Status-Type attribute is sent in Accounting-Request packets when the Auth parameter is set to a value other than RADIUS/LOGOUT. The Acct-Status-Type attribute is set to Stop at the end of a session and is sent in the Accounting-Request packet. If the session fails to be authenticated, the attribute is still sent with the packet.

Acct-Delay-Time (Attribute 41)

This attribute specifies how many seconds the MAX has been trying to send this Accounting packet.

The Acct-Delay-Time attribute is sent in Accounting-Request packets at the end of a session when the Auth parameter is set to a value other than RADIUS/LOGOUT and Acct-Status-Type=Stop. If the session fails to be authenticated, the attribute is still sent with the packet.

Acct-Input-Octets (Attribute 42)

This attribute specifies how many octets have been received during the session.

The Acct-Input-Octets attribute is sent in Accounting-Request packets at the end of a session under these conditions:

- The Accounting-Request packet has Acct-Status-Type=Stop.
- The Auth parameter is set to a value other than RADIUS/LOGOUT.
- The session is authenticated.

Acct-Output-Octets (Attribute 43)

This attribute specifies how many octets have been sent during the session.

The Acct-Output-Octets attribute is sent in Accounting-Request packets at the end of a session under these conditions:

- The Accounting-Request packet has Acct-Status-Type=Stop.
- The Auth parameter is set to a value other than RADIUS/LOGOUT.
- The session is authenticated.

Acct-Session-Id (Attribute 44)

This attribute is a unique numeric string identified with the bridging, routing, or terminal server session reported in this Accounting packet. The Accounting Start packet and Accounting Stop packet can be correlated using Acct-Session-Id. Its value can range from 1 to 2137383647. Each time the MAX is switched on, its value begins again at 1.

The Acct-Session-Id attribute is sent in Accounting-Request packets at the end of a session under these conditions:

- The Accounting-Request packet has Acct-Status-Type=Stop.
- The Auth parameter is set to a value other than RADIUS/LOGOUT.
- The session is authenticated.

If the session fails to be authenticated, the attribute is still sent with the packet.

Note: 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.

Acct-Authentic (Attribute 45)

This attribute can have either of the following values:

- RADIUS (1) specifies that an incoming call was authenticated by RADIUS.
- Local (2) specifies that an incoming call was authenticated by a local Connection Profile or by TACACS, or that the call was accepted without authentication.

The Acct-Authentic attribute is sent in Accounting-Request packets at the end of a session under these conditions:

- The Accounting-Request packet has Acct-Status-Type=Stop.
- The Auth parameter is set to a value other than RADIUS/LOGOUT.
- The session is authenticated.

Acct-Session-Time (Attribute 46)

This attribute indicates how many seconds the session has been logged in. It is sent in Accounting-Request packets at the end of a session under these conditions:

- The Accounting-Request packet has Acct-Status-Type=Stop.
- The Auth parameter is set to a value other than RADIUS/LOGOUT.
- The session is authenticated.

Acct-Input-packets (Attribute 47)

This attribute specifies how many packets have been received during the session. It is sent in Accounting-Request packets at the end of a session under these conditions:

- The Accounting-Request packet has Acct-Status-Type=Stop.
- The Auth parameter is set to a value other than RADIUS/LOGOUT.
- The session is authenticated.

Packet counts are valid only if a framed protocol is in use.

Acct-Output-packets (Attribute 48)

This attribute specifies how many packets have been sent during the session. It is sent in Accounting-Request packets at the end of a session under these conditions:

- The Accounting-Request packet has Acct-Status-Type=Stop.
- The Auth parameter is set to a value other than RADIUS/LOGOUT.
- The session is authenticated.

Packet counts are valid only if a framed protocol is in use.

Dependencies: Keep this additional information in mind:

- If you are running an unmodified Ascend RADIUS daemon, the RADIUS log file name for the Ascend RADIUS accounting file and the Livingston RADIUS accounting file are the same:

  ```
  usr/adm/radacct/host/detail
  ```

  `host` is the RADIUS client and `detail` is the name of the log file. Because the client of the RADIUS accounting server is your MAX, `host` is your MAX's hostname or IP address in dotted decimal notation.
- The Accounting packet also includes the Class attribute (25) reported by the authentication server.
- In addition to Accounting packets sent when a session opens or closes, Accounting packets that report the number of open sessions are sent at regular time intervals, and Accounting Stop packets are sent when a connection fails to authenticate.

  See the Sess Timer parameter in the *MAX Reference Guide*, and "Ascend- Number- Sessions (Attribute 202)" on page 2-22.
- Additional accounting attributes are attributes 189 through 193 and 195 through 198.

See Also: The Auth and Sess Timer parameters in the *MAX Reference Guide*.

Ascend-Home-Agent-IP-Addr (Attribute 183)

Description: Ascend-Home-Agent-IP-Addr indicates the IP address of the home agent under ATMP (Ascend Tunnel Management Protocol) operation. You must specify an IP address in dotted decimal notation.

The RADIUS server passes the attributes contained in the mobile node's RADIUS Connection Profile to the foreign agent; the foreign agent sends these attributes when connecting with the home agent.

Dependencies: The Ascend-Home-Agent-IP-Addr attribute is sent in Authentication-Response packets.

See Also: For detailed information on ATMP operation, see the *MAX ISP and Telecommuting Configuration Guide*.

Ascend-Home-Agent-Password (Attribute 184)

Description: Ascend-Home-Agent-Password specifies the password that the foreign agent sends to the home agent in order to authenticate itself during ATMP (Ascend Tunnel Management Protocol) operation.

The RADIUS server passes the attributes contained in the mobile node's RADIUS Connection Profile to the foreign agent; the foreign agent sends these attributes when connecting with the home agent.

Dependencies: The Ascend-Home-Agent-Password attribute is sent in Authentication-Response packets.

See Also: For detailed information on ATMP operation, see the *MAX ISP and Telecommuting Configuration Guide*.

Ascend-Home-Network-Name (Attribute 185)

Description: Ascend-Home-Network-Name contains 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 Connection Profile to the foreign agent; the foreign agent sends these attributes when connecting with the home agent.

Dependencies: Keep this additional information in mind:

- You must specify a value for this attribute only if the home agent is a gateway (that is, only if Type=Gateway in the Ethernet/Mod Config/ATMP Options menu).
- The Ascend-Home-Network-Name attribute is sent in Authentication-Response packets.

See Also: For detailed information on ATMP operation, see the *MAX ISP and Telecommuting Configuration Guide*.

Ascend-Home-Agent-UDP-Port (Attribute 186)

Description: Ascend-Home-Agent-UDP-Port specifies the UDP port number to use when the foreign agent sends ATMP (Ascend Tunnel Management Protocol) messages to the home agent.

The RADIUS server passes the attributes contained in the mobile node's RADIUS Connection Profile to the foreign agent; the foreign agent sends these attributes when connecting with the home agent

Dependencies: The Ascend-Home-Agent-UDP-Port attribute is sent in Authentication-Response packets.

See Also: For detailed information on ATMP operation, see the *MAX ISP and Telecommuting Configuration Guide*.

Ascend-Multilink-ID (Attribute 187)

Description: Ascend-Multilink-ID applies to sessions that are part of a "Multilink bundle." 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 reports the ID number of the Multilink bundle when the session closes.

Dependencies: The Ascend-Multilink-ID attribute is sent in Authentication-Response packets.

Ascend-Num-In-Multilink (Attribute 188)

Description: Ascend-Num-In-Multilink applies to sessions that are part of a “Multilink bundle.” A Multilink bundle is a multichannel MP or MP+ call. Each online channel of the MP or MP+ call is a session. The Ascend-Num-In-Multilink attribute records the number of sessions remaining in a Multilink bundle when the session reported in an Accounting Stop packet closes.

Dependencies: The Ascend-Num-In-Multilink attribute is sent in the following types of packets:

- Authentication-Response packets.
- Accounting-Request packets in which Acct-Status-Type=Stop, and only when the Auth parameter is not set to RADIUS/LOGOUT.

  These packets are sent at the end of a session. If a session fails to be authenticated, the Ascend-Num-In-Multilink attribute is not sent with this type of packet.

Ascend-First-Dest (Attribute 189)

Description: Ascend-First-Dest records the destination IP address of the first packet received on a connection after the connection has been authenticated. This attribute only applies if the session has been configured to route IP.

Dependencies: The Ascend-First-Dest attribute is sent in Accounting-Request packets at the end of a session under these conditions:

- The Accounting-Request packet has Acct-Status-Type=Stop.
- The Auth parameter is set to a value other than RADIUS/LOGOUT.
- The session is authenticated.

Ascend-Pre-Input-Octets (Attribute 190)

Description: Ascend-Pre-Input-Octets records the number of input octets before authentication.

Dependencies: The Ascend-Pre-Input-Octets attribute is sent in Accounting-Request packets at the end of a session under these conditions:

- The Accounting-Request packet has Acct-Status-Type=Stop.
- The Auth parameter is set to a value other than RADIUS/LOGOUT.
- The session is authenticated.

Ascend-Pre-Output-Octets (Attribute 191)

Description: Ascend-Pre-Output-Octets records the number of output octets before authentication.

Dependencies: The Ascend-Pre-Output-Octets attribute is sent in Accounting-Request packets at the end of a session under these conditions:

- The Accounting-Request packet has Acct-Status-Type=Stop.
- The Auth parameter is set to a value other than RADIUS/LOGOUT.
- The session is authenticated.

Ascend-Pre-Input-packets (Attribute 192)

Description: Ascend-Pre-Input-packets records the number of input packets before authentication.

Dependencies: The Ascend-Pre-Input-packets attribute is sent in Accounting-Request packets at the end of a session under these conditions:

- The Accounting-Request packet has Acct-Status-Type=Stop.
- The Auth parameter is set to a value other than RADIUS/LOGOUT.
- The session is authenticated.

Ascend-Pre-Output-packets (Attribute 193)

Description: Ascend-Pre-Output-packets records the number of output packets before authentication.

Dependencies: The Ascend-Pre-Output-packets attribute is sent in Accounting-Request packets at the end of a session under these conditions:

- The Accounting-Request packet has Acct-Status-Type=Stop.
- The Auth parameter is set to a value other than RADIUS/LOGOUT.
- The session is authenticated.

Ascend-Maximum-Time (Attribute 194)

Description: Ascend-Maximum-Time 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.

Dependencies: The Ascend-Maximum-Time attribute is sent in Authentication-Response packets.

Ascend-Disconnect-Cause (Attribute 195)

Description: Ascend-Disconnect-Cause specifies the reason a connection was taken offline.

Usage: Ascend-Disconnect-Cause can return any of the values listed in Table 2-1.

Table 2-1. Ascend-Disconnect-Cause values

Value	Explanation
unknown(2)	Reason unknown.
clidAuthFail(4)	Failure to authenticate calling-party number.
The following values apply to modem connections:	
noModemNoCarrier(10)	No carrier detected.
noModemLossCarrier(11)	Loss of carrier.
noModemResultCodes(12)	Failure to detect modem result codes.
The following values apply to terminal server sessions:	
tsUserExit(20)	User exited terminal server.
tsIdleTimeout(21)	Timeout waiting for user input.
tsExitTelnet(22)	Disconnect due to exiting Telnet session.

Table 2-1. Ascend-Disconnect-Cause values

Value	Explanation
tsNoIPAddr(23)	Could not switch to SLIP/PPP; the remote end has no IP address.
tsExitTcp(24)	Disconnect due to exiting raw TCP.
tsPassWordFail(25)	Bad passwords.
tsRawTCPDisable(26)	Raw TCP disabled.
tsControlC(27)	Control-C detected.
tsDestroyed(28)	Terminal server destroyed.
The following values apply to PPP sessions:	
pppLcpTimeout(40)	PPP LCP negotiation timed out.
pppLcpNegotiateFail(41)	PPP LCP negotiation failed.
pppPAPAuthFail(42)	PPP PAP authentication failed.
pppCHAPAuthFail(43)	PPP CHAP authentication failed.
pppRemoteAuthFail(44)	PPP remote authentication failed.
pppRcvTerminate(45)	PPP received Terminate Request from remote end.
pppCloseEvent(46)	Upper layer requested that the session be closed.
The following values apply regardless of the type of session in use:	
sessTimeOut(100)	Session timed out.
sessFailSecurity(101)	Session failed for security reasons.
sessCallback(102)	Session terminated due to callback.
invalidProtocol(120)	Call refused because the detected protocol is disabled.

Dependencies: The Ascend-Disconnect-Cause attribute is sent in Accounting-Request packets in which Acct-Status-Type=Stop, and only when the Auth parameter is not set to RADIUS/LOGOUT. The attribute is sent at the end of a session. If the session fails to be authenticated, the attribute is still sent with the packet.

Ascend-Connect-Progress (Attribute 196)

Description: Ascend-Connect-Progress specifies the state of the connection before it is disconnected.

Usage: Ascend-Connect-Progress can have any one of values specified in Table 2-2.

Table 2-2. Ascend-Connect-Progress values

Value	Explanation
prUnknown(2)	Progress unknown
prCallUp(10)	Call up
prModemUp(30)	Modem up
prModemWaitDCD(31)	Waiting for DCD
prModemWaitCodes(32)	Waiting for result codes
prTermSrvStarted(40)	Terminal server session started up
prLanSessionUp(60)	LAN session up
prOpeningLCP(61)	LCP negotiations allowed
prOpeningCCP(62)	CCP negotiations allowed
prOpeningIPNCP(63)	IP NCP negotiations allowed
prOpeningBNCP(64)	Bridging NCP negotiations allowed
prLCPOpened(65)	LCP in Open state
prCCPOpened(66)	CCP in Open state
prIPNCPOpened(67)	IP NCP in Open state
prBNCPOpened(68)	Bridging NCP in Open state
prLCPStateInitial(69)	LCP in Initial state
prLCPStateStarting(70)	LCP in Starting state
prLCPStateClosed(71)	LCP in Closed state
prLCPStateStopped(72)	LCP in Stopped state
prLCPStateClosing(73)	LCP in Closing state
prLCPStateStopping(74)	LCP in Stopping state
prLCPStateReqSent(75)	LCP in Request Sent state
prLCPStateAckRecd(76)	LCP in ACK Received state
prLCPStateAckSent(77)	LCP in ACK Sent state

Dependencies: The Ascend-Connect-Progress attribute is sent in Accounting-Request packets at the end of a session under these conditions:

- The Accounting-Request packet has Acct-Status-Type=Stop.
- The Auth parameter is set to a value other than RADIUS/LOGOUT.
- The session is authenticated.

If the session fails to be authenticated, the attribute is still sent with the packet.

Ascend-Data-Rate (Attribute197)

Description: Ascend-Data-Rate specifies the data rate of the connection in bits per second.

Dependencies: The Ascend-Data-Rate attribute is sent in Accounting-Request packets at the end of a session under these conditions:

- The Accounting-Request packet has Acct-Status-Type=Stop.
- The Auth parameter is set to a value other than RADIUS/LOGOUT.
- The session is authenticated.

If the session fails to be authenticated, the attribute is still sent with the packet.

Ascend-PreSession-Time (Attribute 198)

Description: Ascend-PreSession-Time reports the length of time in seconds from when a call connected to when it completes authentication.

Dependencies: The Ascend-PreSession-Time attribute is sent in Accounting-Request packets at the end of a session under these conditions:

- The Accounting-Request packet has Acct-Status-Type=Stop.
- The Auth parameter is set to a value other than RADIUS/LOGOUT.
- The session is authenticated.

If the session fails to be authenticated, the attribute is still sent with the packet.

Ascend-Token-Idle (Attribute 199)

Description: Ascend-Token-Idle sets the maximum length of time in minutes a cached token can remain alive between authentications. If this attribute is not specified, the cached token remains alive until Ascend-Token-Expiry (attribute 204) causes it to expire. Typically, the value of Ascend-Token-Idle is lower than the value of Ascend-Token-Expiry.

Dependencies: The Ascend-Token-Idle attribute is sent in Authentication-Response packets.

Ascend-Token-Immediate (Attribute 200)

Description: Ascend-Token-Immediate establishes how RADIUS treats the password received from a login-user when the users file entry specifies a hand-held security card server. When specified for the user’s password, the keywords “ACE” and “SAFEWORD” indicate Security Dynamics and Enigma Logic servers, respectively.

Usage: Ascend-Token-Immediate should only be used in ACE or SAFEWORD users file entries with User-Service=Login-User. It can have one of the following values:

- Tok-Imm-No (0) indicates that the password received from the user is ignored.

  Choose this value for security servers that issue a challenge entered by the user in his or her security card before deriving a password.
- Tok-Imm-Yes (1) specifies that the password received from the user is sent to the security server for authentication.

Example: The following example shows a users file entry that sends the password received from the login-user to the ACE server. The login-user derives this password from his or her hand-held security card:

```
qXUnit  Password="ACE", Ascend-Token-Immediate=Tok-Imm-Yes
        User-Service=Login-User,
        Login-Service=Telnet
```

Dependencies: The Ascend-Token-Immediate attribute does not work with CHAP authentication. It is sent in Authentication-Response packets.

See Also: "User-Service (Attribute 6)" on page 2-3.

Ascend-Require-Auth (Attribute 201)

Description: Ascend-Require-Auth specifies whether additional authentication is required, and applies only to calls that have been CLID authenticated.

Usage: You can set this attribute to one of the following values:

- Require-Auth (1) specifies that additional authentication is required.

  If you choose this value, the type of authentication desired must be specified in the Ascend-Send-Auth attribute.
- Not-Require-Auth (0) specifies that additional authentication is not required by this users file entry.

  However, terminal server users might be required to log in with their passwords as determined by the setting of the MAX's Security parameter.

In RADIUS, a single users file entry cannot perform both CLID authentication and name-password authentication; therefore, to avoid confusion, the attributes of the CLID authenticating entry and the name-password authentication entry should be the same.

Example: In this example, Ascend-Require-Auth is included in the CLID-authenticating users file entry:

```
5551212 Password="Ascend-CLID" User-Service=Dialout-Framed-User
          User-Name="real-user-name",
          Ascend-Require-Auth=Require-Auth,
          Ascend-Send-Auth=Send-Auth-CHAP,
          Framed-Protocol=PPP,
          Framed-Address=10.0.200.1,
          Framed-Netmask=255.255.255.0
```

Dependencies: Keep this additional information in mind:

- Ascend-Require-Auth applies to two types of CLID-authenticated calls:
  - Synchronous and asynchronous PPP calls

    Synchronous and asynchronous PPP calls that have been CLID authenticated undergo no further authentication unless the matching RADIUS entry has Ascend-Require-Auth=Require Auth. If Ascend-Require-Auth=Require Auth, the parameters of the call are initially set by CLID authentication, but are subject to change by any authentication that might follow.

    Asynchronous PPP operates through the MAX's terminal server. In some cases, the MAX prompts the caller for a password before beginning asynchronous PPP.
  - Terminal server calls

    Terminal server calls that have been CLID authenticated and that prompt the user for a password undergo authentication. If the matching profile is a RADIUS entry with

Ascend-Require-Auth=Not-Require-Auth, the parameters of the call are set by CLID authentication and are not changed by any authentication that might follow. If the matching profile is a RADIUS entry with Ascend-Require-Auth=Require-Auth, the parameters of the call are initially set by CLID authentication, but are subject to change by any authentication that might follow.

- The Ascend-Require-Auth attribute is sent in Authentication-Response packets.

See Also: The Security parameter in the *MAX Reference Guide*.

Ascend-Number-Sessions (Attribute 202)

Description: Ascend-Number-Sessions is used in conjunction with the Class attribute (25) to specify the number of active sessions of each class reported to the RADIUS accounting server. In the case of multichannel calls, such as MP+ calls, each separate connection counts as a session. The Sess Timer parameter sets the time period between accounting session reports.

The Ascend-Number-Sessions attribute is sent in Authentication-Response packets only when a customized RADIUS accounting daemon is in use. In the MAX, you can set the Sess Timer parameter to send accounting packets at regular intervals. These are non-standard accounting packets identified by the code number 33. Only accounting daemons modified to recognize this packet code respond. Other accounting daemons ignore it. Therefore, this attribute is ignored by the standard Livingston RADIUS daemon and by the Ascend accounting daemons.

Usage: The value of this attribute is the number of sessions that are active for the class specified by the attribute.

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.

See Also: The Sess Timer parameter in the *MAX Reference Guide*.

Ascend-Authen-Alias (Attribute 203)

Description: Ascend-Authen-Alias sets this MAX's login name during PPP authentication. If Ascend-Authen-Alias is not specified in a Dialout-Framed-User entry, the login name is set by the Name parameter in the System Profile.

Usage: The maximum number of characters you can specify for the attribute is 16.

Dependencies: The Ascend-Authen-Alias attribute is sent in Authentication-Response packets.

See Also: The Name parameter in the *MAX Reference Guide*.

Ascend-Token-Expiry (Attribute 204)

Description: Ascend-Token-Expiry sets the lifetime of a cached token—that is, the lifetime of hand-held security card authentication.

When the cached token is still alive, subsequent CACHE-TOKEN authentication requests from the same user are authenticated by CHAP without the use of a hand-held security card. When the cached token has expired, CACHE-TOKEN authentication requests are authenticated through the ACE or SAFEWORD server.

Dependencies: The Ascend-Token-Expiry attribute is sent in Authentication-Response packets.

See Also: "Ascend-Token-Idle (Attribute 199)" on page 2-20.

Ascend-Menu-Selector (Attribute 205)

Description: Ascend-Menu-Selector enables you to specify 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 (206), the terminal server displays this string when prompting the user to make a selection:

```
Enter Selection (1-n, q)
```

where `n` is the last number in the list. The terminal server code automatically determines the value of `n` by determining the number of items in the menu. The only valid user input is in the range 1 through `n`, 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-n, q)`.

Usage: Enter your specification using this format:

```
Ascend-Menu-Selector=string
```

`string` contains the text you want the terminal server to display when prompting the user for a menu selection. You can specify up to 31 characters.

Example: Suppose you set these attributes:

```
emma Password=“m2dan”, User-Service=Login-User
     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.

Dependencies: Ascend-Menu-Selector is sent in Authentication-Response packets.

See Also: “Ascend-Menu-Item (Attribute 206)” on page 2-24.

Ascend-Menu-Item (Attribute 206)

Description: Ascend-Menu-Item 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 users file entry 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
```

- `command` is the string sent to the terminal server when the user selects the menu item.

  The `command` specification must be in a format that the Ascend terminal server understands, and can contain up to 80 characters.
- `text` is the text displayed to the user.

  The maximum length for `text` is 31 characters.
- The first semi-colon (;) that appears acts as the delimiter between `command` and `text`.

Example: Suppose you set these attributes:

```
emma Password=“m2dan”, User-Service=Login-User
     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”
```

The terminal server displays this text:

```
1. Display IP Stats     3. Telnet to Ken’s machine
2. Ping server          4. Display ARP Table.
              Enter Selection (1-4, q)
```

Dependencies: The Ascend-Menu-Item attribute is sent in Authentication-Response packets.

See Also: “Ascend-Menu-Selector (Attribute 205)” on page 2-23.

Ascend-PW-Lifetime (Attribute 208)

Description: Ascend-PW-Lifetime enables you to specify on a per-user basis the number of days that a password is valid.

Usage: You can specify the Ascend-PW-Lifetime attribute on any line other than the Name/Password line of the users file entry. Use this format:

```
Ascend-PW-Lifetime=num
```

`num` is the number of days for which the user’s password is valid.

Example: You might make this specification:

```
emma Password=“m2dan”, User-Service=Login-User,
     Ascend-PW-Expiration=”Jan 1, 1996”
     Ascend-PW-Lifetime=30
```

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 (attribute 21).

  For example, suppose that Ascend-PW-Lifetime=30, Ascend-PW-Expiration=June 1, 1995, and today's date is October 1, 1995. If the user resets the password today, the value of Ascend-PW-Expiration becomes today's date + Ascend-PW-Lifetime, or October 31, 1995.
- If the password has not expired, the value of Ascend-PW-Expiration overrides the value of Ascend-PW-Lifetime.

  For example, if on October 1, 1995 you set Ascend-PW-Lifetime=30 and Ascend-PW-Expiration=October 15, 1995, the password expires on October 15, 1995. 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.
- The Ascend-PW-Lifetime attribute is sent in Authentication-Response packets.

Ascend-IP-Direct (Attribute 209)

Description: Ascend-IP-Direct specifies in a users file entry the IP address to which the MAX redirects packets from the user. When you include this attribute in a users file entry, 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's routing scheme.

Usage: For the Ascend-IP-Direct attribute, enter your specification in this format:

```
Ascend-IP-Direct=ipaddr
```

`ipaddr` is an IP address in dotted decimal notation. The default is 0.0.0.0; if you accept the default, the MAX does not redirect IP traffic.

Example: You might enter this specification:

```
emma Password="m2dan"
     Ascend-IP-Direct=200.3.45.69
     Metric=2
     Ascend-Bridge=No
     Framed-Protocol=PPP
```

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 users file entry contains the specification Ascend-Bridge=No.
  - Framed-Protocol is not set to COMB or FR.
- Do not set Ascend-IP-Direct and Ascend-FR-Direct in the same users file entry; if you do so, an error occurs.
- The Ascend-IP-Direct attribute is sent in Authentication-Response packets.

Ascend-PPP-VJ-Slot-Comp (Attribute 210)

Description: Ascend-PPP-VJ-Slot-Comp instructs the Ascend PPP code not to use slot compression when sending VJ-compressed packets.

When you set the parameter VJ Comp=Yes, 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. For this purpose, set the Ascend-PPP-VJ-Slot-Comp attribute to VJ-Slot-Comp-No (1). This attribute specifies that no slot compression take place. If you do not specify a value for Ascend-PPP-VJ-Slot-Comp and VJ Comp=Yes, slot compression occurs.

Usage: You specify this attribute in the users file entries where you want it to apply. Enter your specification using this format:

```
Ascend-PPP-VJ-Slot Comp=VJ-Slot-Comp-No
```

Dependencies: The Ascend-PPP-VJ-Slot-Comp attribute is sent in Authentication-Response packets.

See Also: The VJ Comp parameter in the *MAX Reference Guide*.

Ascend-PPP-VJ-1172 (Attribute 211)

Description: Ascend-PPP-VJ-1172 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: You specify this attribute in a users file entry. Enter your specification using this format:

```
Ascend-PPP-VJ-1172=PPP-VJ-1172
```

Dependencies: The Ascend-PPP-VJ-1172 attribute is sent in Authentication-Response packets.

Ascend-PPP-Async-Map (Attribute 212)

Description: Ascend-PPP-Async-Map 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: The value you specify is 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.

You specify this attribute in a users file entry. Enter your specification using this format:

```
Ascend-PPP-Async-Map=integer
```

`integer` is a map as defined in RFC 1548.

Example: Your specification might look like this one:

```
emma Password=m2dan”, User-Service=Login-User
     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.

Dependencies: The Ascend-PPP-Async-Map attribute is sent in Authentication-Response packets.

Ascend-Third-Prompt (Attribute 213)

Description: The 3rd Prompt parameter enables you to specify an additional prompt for user input after the login and password prompts. The MAX passes the information the user enters to the RADIUS server as the Ascend-Third-Prompt attribute. The Access-Request packet contains this attribute.

Usage: The Ascend-Third-Prompt attribute can contain up to 80 characters.

If the user enters more than 80 characters, the input is truncated to 80. If the user does enter any characters, the attribute is set to null.

Dependencies: The Ascend-Third-Prompt attribute is sent in Authentication-Response packets. The RADIUS server can ignore this attribute.

Ascend-Send-Secret (Attribute 214)

Description: Ascend-Send-Secret can be used in place of Ascend-Send-Passwd in outdial profiles. When Ascend-Send-Secret is used, the password is encrypted when passed between the RADIUS server and the MAX.

Dependencies: The Ascend-Send-Secret attribute is sent in Authentication-Response packets.

Ascend-Receive-Secret (Attribute 215)

Description: Ascend-Receive-Secret is received from a dial-in user and sent from the RADIUS server to your MAX. It is used to verify an encrypted password.

Usage: Ascend-Receive-Secret supports two types of authentication: CACHE-TOKEN and PAP-TOKEN-CHAP.

CACHE-TOKEN

CACHE-TOKEN 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 (204). During the lifetime of the token, subsequent calls by the user require only CHAP authentication without the use of a hand-held security card.

Although the dial-in user can be set up for CACHE-TOKEN authentication, it cannot force CACHE-TOKEN. The RADIUS users file must have the following elements for CACHE-TOKEN to work:

- A password of ACE or SAFEWORD
- An Ascend-Receive-Secret attribute set to the same password as the Send PW parameter in the Connection Profile that placed the call
- An Ascend-Token-Expiry attribute (204) set to a nonzero value

If an ACE or SAFEWORD entry exists but the value of Send PW in the calling profile does not match Ascend-Receive-Secret, the call is rejected. Similarly, if the Ascend-Token-Expiry is not in the users file entry or is set to 0, the call is rejected.

The following example allows CACHE-TOKEN authentication with a 90-minute token cache. Notice that the Ascend-Token-Expiry attribute must be placed on the first line of the entry, along with the user-name and ACE or SAFEWORD password:

```
nXUnit  Password="ACE", Ascend-Token-Expiry=90
        Ascend-Receive-Secret=“shared-secret”,
        User-Service=Framed-User,
        Framed-Protocol=PPP,
        Framed-Address=10.0.3.2,
        Framed-Netmask=255.255.255.0
```

PAP-TOKEN-CHAP

In PAP-TOKEN-CHAP, the Ascend-Receive-Secret attribute is used to transport a received password from the RADIUS server to your MAX in support of PAP-TOKEN-CHAP authentication. The password is encrypted on the Ethernet. This is the CHAP password that the answering unit uses to authenticate second and subsequent channels of an MP+ call.

The advantage of a PAP-TOKEN-CHAP call over a PAP-TOKEN call is that only the initial connection needs to be verified by a hand-held security card. Any additional channels are verified by CHAP. That is, whenever additional channels are added to a PAP-TOKEN-CHAP MP+ call, the calling unit sends the encrypted value of Aux Send PW (found in the Connection Profile used to dial the call), 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.

The following example shows the users file entry necessary for `rxUnit` to use an Enigma Logic server. After authentication, the user can open an MP+ (or PPP) session; the user receives the IP address 200.0.5.1 and netmask 255.255.255.0. Because this entry includes the attribute Ascend-Receive-Secret, additional channels can be authenticated through CHAP without having to go to the SAFEWORD server for authentication.

```
rXUnit  Password="SAFEWORD"
        User-Service=Framed-User,
        Framed-Protocol=MPP,
        Framed-Address=200.0.5.1,
        Framed-Netmask=255.255.255.0
        Ascend-Receive-Secret=b5XSAM
```

Dependencies: The Ascend-Receive-Secret attribute is sent in Authentication-Response packets.

See Also: The Aux Send PW and Send PW parameters in the *MAX Reference Guide.*

Ascend Frame Relay Attributes (219, 220, 221)

Description: These attributes affect frame relay operation:

- Ascend-FR-Direct (219) specifies whether the Connection Profile operates in frame relay redirect mode.

  Ascend-FR-Direct can have one of these values:

  - FR-Direct-No (0) specifies that the Connection Profile operates in the normal mode.
  - FR-Direct-Yes (1) specifies that the Connection Profile operates in frame relay redirect mode.

  Connection Profiles operating in the frame relay gateway mode are not specified in RADIUS because they are dial-out or nailed-up connections only.

- Ascend-FR-Direct-Profile (220) specifies the name of the Frame Relay Profile that carries this connection to the frame relay switch.

  This attribute is analogous to the FR Prof parameter.

- Ascend-FR-Direct-DLCI (221) specifies the DLCI that carries this connection to the frame relay switch.

  This attribute is analogous to the DLCI parameter.

Example:

```
ascend Password=”test”
    Ascend-FR-Direct=Fr-Direct-Yes,
    Ascend-FR-Direct-Profile=“montgomery”,
    Ascend-FR-Direct-DLCI=21,
    Metric=2,
    ...
```

Dependencies: The frame relay attributes are sent in Authentication-Response packets.

See Also: The DLCI and FR Prof parameters in the *MAX Reference Guide*.

Ascend-Handle-IPX (Attribute 222)

Description: Ascend-Handle-IPX specifies how the MAX handles NCP watchdog requests on behalf of IPX clients during IPX bridging.

Usage: This attribute can have one of the following values:

- Handle-IPX-None is equivalent to the None setting for the Handle IPX parameter.
- Handle-IPX-Client is equivalent to the Client setting for the Handle IPX parameter.
- Handle-IPX-Server is equivalent to the Server setting for the Handle IPX parameter.

Dependencies: The Ascend-Handle-IPX attribute is sent in Authentication-Response packets.

See Also: The Handle IPX parameter in the *MAX Reference Guide*.

Ascend-Netware-timeout (Attribute 223)

Description: Ascend-Netware-timeout sets 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 or routing connection. Responding to watchdog requests on behalf of clients is commonly called spoofing.

Usage: Setting Ascend-Netware-timeout=0 allows the MAX to respond to watchdog requests without a time limit. The default is 30 minutes. This attribute is analogous to the NetWare t/o parameter in the Connection Profile.

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, this timeout is cancelled.

Dependencies: Keep this additional information in mind:

- Ascend-Netware-timeout applies to IPX bridging connections only when the MAX is on the server LAN and not on the client LAN.
- Ascend-Netware-timeout applies to all IPX routing connections.
- Ascend-Netware-timeout is sent in Authentication-Response packets.

See Also: The NetWare t/o parameter in the *MAX Reference Guide*.

Ascend-IPX-Alias (Attribute 224)

Description: Ascend-IPX-Alias corresponds to the IPX Alias# parameter in the Connection Profile. This attribute is used only when connecting to IPX routers that require numbered interfaces.

Usage: The Ascend-IPX-Alias parameter is optional and has a default value of 0 (zero). Note that 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 users file.

Dependencies: The Ascend-IPX-Alias attribute is sent in Authentication-Response packets.

See Also: The IPX Alias# parameter in the *MAX Reference Guide*.

Ascend-Route-IPX (Attribute 229)

Description: Ascend-Route-IPX indicates whether IPX routing is allowed for the users file entry. It corresponds to the Route IPX parameter in the Connection Profile. In PPP and MP+, both ends of the connection must have matching settings to route IPX.

Usage: You can set these values for Ascend-Route-IPX:

- Route-IPX-No (0)
- Route-IPX-Yes (1)

The default value for Ascend-Route-IPX is Route-IPX-No.

Dependencies: The Ascend-Route-IPX attribute is sent in Authentication-Response packets.

See Also: The Route IPX parameter in the *MAX Reference Guide*.

Ascend-Data-Filter and Ascend-Call-Filter (Attributes 242 and 243)

Description: Unlike the Filter Profiles stored under the Filters menu, RADIUS filters are part of the outgoing or incoming RADIUS Connection Profile. In other words, within any RADIUS users file defining a Connection Profile, you can include values for Ascend-Data-Filter to define data filters for that profile, or 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, like subfilters in the Filter Profiles. Therefore, the order in which filter entries are entered is significant.

If you make changes to a filter in a RADIUS Connection Profile, the changes do not take effect until a call uses that profile.

IP filter entries

Use this format for an IP call filter entry:

```
Ascend-Call-Filter=“ip dir action [dstip n.n.n.n/nn][srcip n.n.n.n/nn]
[proto [dstport cmp value] [srcport cmp value] [est]]”
```

Use this format for an IP data filter entry:

```
Ascend-Data-Filter=“ip dir action [dstip n.n.n.n/nn][srcip n.n.n.n/nn]
[proto [dstport cmp value] [srcport cmp value] [est]]”
```

Note: Each entry must appear on one line; in this guide, some entries appear on two lines due only to space and formatting constraints.

These are the elements of an IP filter entry:

- `Call Filter` is the keyword that indicates a call filter entry.
- `Data Filter` is the keyword that indicates a data filter entry.
- `ip` is the keyword that indicates an IP filter entry.
- `dir` is set to `in` or `out` to indicate whether this entry is for an input filter or an output filter.
- `action` can be either `forward` or `drop`.
- `dstip` is the value following the keyword `dstip`, and specifies the destination IP address and mask.

  The address `n.n.n.n` in dotted decimal format is followed by `/nn`, which specifies the number of bits in the mask. If the address is unspecified, 0.0.0.0/00 is assumed.
- `srcip` is the value following the keyword `srcip`, and specifies the source IP address and mask.

  The address `n.n.n.n` in dotted decimal format is followed by `/nn`, which specifies the number of bits in the mask. If the address is unspecified, 0.0.0.0/00 is assumed.
- `proto` is the protocol.

  1, 6, 17, and 89 are legal values that correspond to ICMP, TCP, UDP, and OSPF, respectively.
- `dstport` is a keyword followed by `cmp` and `value`.

  `cmp` should be < (less than), == (equal), > (greater than), or != (not equal).

  `value` can be any number from 0 to 35565, or one of the following port names or numbers:

  - `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)`
  - `talk (517)`

  `value` can also be unspecified.

- `srcport` is a keyword followed by `cmp` and `value`.
- `est` is an optional keyword.

  When specified, this keyword indicates that the filter is applied only to connections for which TCP has been established.

Generic filter entries

Use this format for a generic call filter entry:

```
Ascend-Call-Filter=“generic dir action offset mask value [more]”
```

Use this format for a generic data filter entry:

```
Ascend-Data-Filter=“generic dir action offset mask value [more]”
```

These are the elements of a generic filter entry:

- `generic` is the keyword that indicates a generic filter entry.
- `dir` is set to `in` or `out` to indicate whether this entry is for an input filter or an output filter.
- `action` is either `forward` or `drop`.
- `offset` corresponds to the Offset parameter.
- `value` corresponds to the Value parameter.
- `more` is an optional keyword that corresponds to the More parameter.

Example: These are examples of IP 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: Each entry must appear on one line; in this guide, some entries appear on two lines due only to space and formatting constraints.

These are examples of generic 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”
```

Dependencies: The Ascend-Data-Filter and Ascend-Call-Filter attributes are sent in Authentication-Response packets.

See Also: The Call Filter, Data Filter, Dst Adrs, Dst Mask, Dst Port #, Dst Port Cmp, More, Offset, Protocol, Src Port #, Src Port Cmp, TCP Estab, and Value parameters in the *MAX Reference Guide.*

Ascend-Callback (Attribute 246)

Description: Ascend-Callback enables or disables callback. Callback occurs when the MAX answers a call and verifies a name and password against a users file entry. 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 (attribute 227)
- The password specified by Ascend-Send-Secret (attribute 214) or Ascend-Send-Passwd (attribute 232)
- Any other relevant attributes in the users file entry that authenticated the call

Usage: The Ascend-Callback attribute applies only to incoming calls and should not appear in dial-out users file entries (Dialout-Framed-User). Ascend-Callback takes the following values:

- Callback-No (0) specifies that the MAX answers in the normal manner after authentication.
- Callback-Yes (1) specifies that the MAX hangs up and calls back the caller after authentication.

Dependencies: The Ascend-Callback attribute is sent in Authentication-Response packets.

Ascend-PPP-Address (Attribute 253)

Description: Ascend-PPP-Address specifies the IP address reported to the calling unit during PPP IPCP negotiations.

Usage: If you do not specify a value for this attribute, or if you specify the value 0.0.0.0, IPCP negotiates with the value of the IP Adrs parameter in the Ethernet Profile. If a valid IP address is specified, IPCP negotiates with that IP address.

If you set the value of this attribute to 255.255.255.255, IPCP negotiates with the address 0.0.0.0. Note that you can assign Ascend-PPP-Address a value different from its true IP address, as long as the user requesting access understands that limitation.

Dependencies: The Ascend-PPP-Address attribute is sent in Authentication-Response packets.

See Also: The IP Adrs parameter in the *MAX Reference Guide*.

Cross reference of attributes and parameters

Table 2-3 cross-references the Ascend RADIUS dictionary’s attributes to parameters in the MAX’s menu-driven user interface. The table is arranged by parameter.

Table 2-3. Parameters and analogous attributes

Parameter	**Analogous attribute**
Answer/Connection Profiles (no attributes for COMB encapsulation)	
Active	No analogous attribute
Add Pers	Ascend-Add-Seconds
AnsOrig	No analogous attribute
Bill #	Ascend-Billing-Number
Bridge	Ascend-Bridge
Call Type	No analogous attribute
Call-by-Call	Ascend-Call-By-Call
Callback	Ascend-Callback
Data Svc	Ascend-Data-Svc
Dec Ch Cnt	Ascend-Dec-Channel-Count
Dial #	Ascend-Dial-Number
DLCI	Ascend-FR-Direct-DLCI
Dyn Alg	Ascend-History-Weigh-Type
Encaps submenu parameters in the Answer Profile Encaps parameter in the Connection Profile	Framed-Protocol
Force 56	Ascend-Force-56
FR Direct	Ascend-FR-Direct
FR Prof	Ascend-FR-Direct-Profile
Group	No analogous attribute
Handle IPX	Ascend-Handle-IPX
Idle	Ascend-Idle-Limit
Idle Pct	Ascend-MPP-Idle-Percent
Inc Ch Cnt	Ascend-Inc-Channel-Count
IP Direct	Ascend-IP-Direct
IPX Alias#	Ascend-IPX-Alias
LAN Adrs	Framed-Address

Table 2-3. Parameters and analogous attributes

Parameter	Analogous attribute
LAN Adrs	Framed-Netmask
Link Comp	Ascend-Link-Compression
Login Host	Login-Host
Login Port	Login-TCP-Port
LQM, LQM Min, LQM Max	No analogous attribute
Max Ch Count	Ascend-Maximum-Channels
Metric	Ascend-Metric
MRU	Framed-MTU
NetWare t/o	Ascend-Netware-timeout
Peer	Ascend-IPX-Peer-Mode
Pool	Ascend-Assign-IP-Pool
Preempt	Ascend-Preempt-Limit
PRI # Type	Ascend-PRI-Number-Type
Recv PW	Password (User-Password), Ascend-Receive-Secret
RIP	Framed-Routing
Route IP	Ascend-Route-IP
Route IPX	Ascend-Route-IPX
Sec Hist	Ascend-Seconds-Of-History
Send Auth	Ascend-Send-Auth
Send PW	Ascend-Send-Passwd, Ascend-Send-Secret
Station	User-Name
Sub Pers	Ascend-Remove-Seconds
Target Util	Ascend-Target-Util
Transit #	Ascend-Transit-Number
VJ Comp	Framed-Compression
Ethernet Profile	
Unless listed, Ethernet Profile parameters do not have analogous RADIUS attributes.	
Banner (terminal server users only)	Reply-Message

Table 2-3. Parameters and analogous attributes

Parameter	Analogous attribute
Host #1 Addr, Host #1 Text, Host #2 Addr, Host #2 Text, Host #3 Addr, Host #3 Text, Host #4 Addr, Host #4 Text	Ascend-Host-Info
IP Adrs	NAS-Identifier
Immed Telnet	Login-Host
Route Profile	
Route Profile entry	Framed-Route
Filter Profile	
Filter Profile parameters	Ascend-Data-Filter
Filter Profile parameters	Ascend-Call-Filter

Table 2-4 cross-references the Ascend RADIUS dictionary’s attributes to parameters in MAX’s menu-driven user interface. The table is arranged by attribute.

Table 2-4. Attributes and analogous parameters

Attribute	Attribute values	Attribute number	Analogous parameter
User-Name	[ ] (string)	1	Station
Password (User-Password)	[ ] (string)	2	Recv PW
Challenge-Response	[ ] (string)	3	No analogous parameter
NAS-Identifier	[ ] (ipaddr)	4	IP Adrs
NAS-Port	[ ] (integer)	5	No analogous parameter
User-Service	1 (Login-User) 2 (Framed-User) 5 (Dialout-Framed-User) (3, 4, and 6 are not supported)	6	No analogous parameter
Framed-Protocol	1 (PPP) 2 (SLIP) 256 (MPP) 257 (EURAW) 258 (EUUI) 260 (COMB) 261 (FR)	7	No analogous parameter
Framed-Address	[ ] (ipaddr)	8	LAN Adrs
Framed-Netmask	[ ] (ipaddr)	9	LAN Adrs

Table 2-4. Attributes and analogous parameters

Attribute	Attribute values	Attribute number	Analogous parameter
Framed-Routing	0 (None) 1 (Broadcast) 2 (Listen) 3 (Broadcast-Listen)	10	RIP
Framed-Filter	Not supported	11	No analogous parameter
Framed-MTU	[ ] (integer)	12	MRU
Framed-Compression	1 (Van-Jacobson-TCP-IP) (No other values supported)	13	VJ Comp
Login-Host	[ ] (ipaddr)	14	Immed Telnet, Login Host
Login-Service	0 (Telnet) 2 (TCP-Clear) (No other values supported)	15	TCP-Clear
Login-TCP-Port	[ ] (integer)	16	Login Port and the *port-number* field the in `telnet` and `tcp` commands of the terminal server interface
Change-Password	[ ] (string)	17	No analogous parameter
Reply-Message	[ ] (string)	18	Banner (terminal server users only)
Callback-Number	Not supported	19	No analogous parameter
Callback-Name	Not supported	20	No analogous parameter
Ascend-PW-Expiration	[ ] (date)	21	No analogous parameter
Framed-Route	[ ] (string)	22	Route Profile entry
Framed-IPX-Network	[ ] (integer)	23	IPX Net#
State	Not supported	24	No analogous parameter
Class	[ ] (string)	25	No analogous parameter
Vendor-Specific	Not supported	26	No analogous parameter
Client-Port-DNIS	[ ] (string)	30	No analogous parameter
Caller-Id	[ ] (string)	31	No analogous parameter
NAS-IP-Address	[ ] (string)	32	No analogous parameter
Acct-Status-Type	1 (Start) 2 (Stop)	40	No analogous parameter
Acct-Delay-Time	[ ] (integer)	41	No analogous parameter

Table 2-4. Attributes and analogous parameters

Attribute	Attribute values	Attribute number	Analogous parameter
Acct-Input-Octets	[ ] (integer)	42	No analogous parameter
Acct-Output-Octets	[ ] (integer)	43	No analogous parameter
Acct-Session-Id	[ ] (string)	44	No analogous parameter
Acct-Authentic	0 (None) 1 (RADIUS) 2 (Local)	45	No analogous parameter
Acct-Session-Time	[ ] (integer)	46	No analogous parameter
Acct-Input-packets	[ ] (integer)	47	No analogous parameter
Acct-Output-packets	[ ] (integer)	48	No analogous parameter
Ascend-Home-Agent-IP-Addr	[ ] (ipaddr)	183	no analogous parameter
Ascend-Home-Agent-Password	[ ] (string)	184	no analogous parameter
Ascend-Home-Network-Name	[ ] (string)	185	no analogous parameter
Ascend-Home-Agent-UDP-Port	[ ] (integer)	186	no analogous parameter
Ascend-Multilink-ID	[ ] (integer)	187	no analogous parameter
Ascend-Num-In-Multilink	[ ] (integer)	188	no analogous parameter
Ascend-First-Dest	[ ] (ipaddr)	189	no analogous parameter
Ascend-Pre-Input-Octets	[ ] (integer)	190	no analogous parameter
Ascend-Pre-Output-Octets	[ ] (integer)	191	no analogous parameter
Ascend-Pre-Input-packets	[ ] (integer)	192	No analogous parameter
Ascend-Pre-Output-packets	[ ] (integer)	193	No analogous parameter
Ascend-Maximum-Time	[ ] (integer)	194	No analogous parameter
Ascend-Disconnect-Cause	[ ] (integer)	195	No analogous parameter
Ascend-Connect-Progress	[ ] (integer)	196	No analogous parameter
Ascend-Data-Rate	[ ] (integer)	197	No analogous parameter
Ascend-PreSession-Time	[ ] (integer)	198	No analogous parameter
Ascend-Token-Idle	[ ] (integer)	199	No analogous parameter
Ascend-Token-Immediate	0 (Tok-Imm-No) 1 (Tok-Imm-Yes)	200	No analogous parameter
Ascend-Require-Auth	0 (Not-Require-Auth) 1 (Require-Auth)	201	No analogous parameter
Ascend-Number-Sessions	[ ] (string)	202	No analogous parameter

Table 2-4. Attributes and analogous parameters

Attribute	Attribute values	Attribute number	Analogous parameter
Ascend-Authen-Alias	[ ] (string)	203	No analogous parameter
Ascend-Token-Expiry	[ ] (integer)	204	No analogous parameter
Ascend-Menu-Selector	[ ] (string)	205	No analogous parameter
Ascend-Menu-Item	[ ] (string)	206	No analogous parameter
Ascend-PW-Lifetime	[ ] (integer)	208	No analogous parameter
Ascend-IP-Direct	[ ] (ipaddr)	209	IP Direct
Ascend-PPP-VJ-Slot-Comp	1 (VJ-Slot-Comp-No)	210	No analogous parameter
Ascend-PPP-VJ-1172	1 (PPP-VJ-1172)	211	No analogous parameter
Ascend-PPP-Async-Map	[ ] (integer)	212	No analogous parameter
Ascend-Third-Prompt	[ ] (string)	213	3rd Prompt
Ascend-Send-Secret	[ ] (string)	214	Send PW
Ascend-Receive-Secret	[ ] (string)	215	Recv PW
Ascend-IPX-Peer-Mode	0 (IPX-Peer-Router) 1 (IPX-Peer-Dialin)	216	No analogous parameter
Ascend-IP-Pool-Definition	[ ] (string)	217	Pool Start #1, #2, Pool Count #1, #2
Ascend-Assign-IP-Pool	[ ] (integer)	218	Pool
Ascend-FR-Direct	0 (FR-Direct-No) 1 (FR-Direct-Yes)	219	FR Direct
Ascend-FR-Direct-Profile	[ ] (string)	220	FR Prof
Ascend-FR-Direct-DLCI	[ ] (integer)	221	DLCI
Ascend-Handle-IPX	0 (Handle-IPX-None) 1 (Handle-IPX-Client) 2 (Handle-IPX-Server)	222	Handle IPX
Ascend-Netware-timeout	[ ] (integer)	223	NetWare t/o
Ascend-IPX-Alias	[ ] (string)	224	IPX Alias#
Ascend-Metric	[ ] (integer)	225	Metric
Ascend-PRI-Number-Type	0 (Unknown-Number) 1 (Intl-Number) 2 (National-Number) 4 (Local-Number) 5 (Abbrev-Number)	226	PRI # Type
Ascend-Dial-Number	[ ] (string)	227	Dial #

Table 2-4. Attributes and analogous parameters

Attribute	Attribute values	Attribute number	Analogous parameter
Ascend-Route-IP	0 (Route-IP-No) 1 (Route-IP-Yes)	228	Route IP
Ascend-Route-IPX	0 (Route-IPX-No) 1 (Route-IPX-Yes)	229	Route IPX
Ascend-Bridge	0 (Bridge-No) 1 (Bridge-Yes)	230	Bridge
Ascend-Send-Auth	0 (Send-Auth-None) 1 (Send-Auth-PAP) 2 (Send-Auth-CHAP)	231	Send Auth
Ascend-Send-Passwd	[ ] (string)	232	Send PW
Ascend-Link-Compression	0 (Link-Comp-None) 1 (Link-Comp-Stac)	233	Link Comp
Ascend-Target-Util	[ ] (integer)	234	Target Util
Ascend-Maximum-Channels	[ ] (integer)	235	Max Ch Cnt
Ascend-Inc-Channel-Count	[ ] (integer)	236	Inc Ch Cnt
Ascend-Dec-Channel-Count	[ ] (integer)	237	Dec Ch Cnt
Ascend-Seconds-Of-History	[ ] (integer)	238	Sec Hist
Ascend-History-Weigh-Type	0 (History-Constant) 1 (History-Linear) 2 (History-Quadratic)	239	Dyn Alg
Ascend-Add-Seconds	[ ] (integer)	240	Add Pers
Ascend-Remove-Seconds	[ ] (integer)	241	Sub Pers
Ascend-Data-Filter	abinary	242	Filter Profile parameters
Ascend-Call-Filter	abinary	243	Filter Profile parameters
Ascend-Idle-Limit	[ ] (integer)	244	Idle
Ascend-Preempt-Limit	[ ] (integer)	245	Preempt
Ascend-Callback	0 (Callback-No) 1 (Callback-Yes)	246	Callback
Ascend-Data-Svc	[ ] (integer)	247	Data Svc
Ascend-Force-56	0 (Force-56-No) 1 (Force-56-Yes)	248	Force 56
Ascend-Billing-Number	[ ] (string)	249	Bill #
Ascend-Call-By-Call	[ ] (integer)	250	Call-by-Call

Table 2-4. Attributes and analogous parameters

Attribute	**Attribute values**	**Attribute number**	**Analogous parameter**
Ascend-Transit-Number	[ ] (string)	251	Transit #
Ascend-Host-Info	[ ] (string)	252	Host #1 Addr, Host #1 Text, Host #2 Addr, Host #2 Text, Host #3 Addr, Host #3 Text, Host #4 Addr, Host #4 Text
Ascend-PPP-Address	[ ] (ipaddr)	253	No analogous parameter
Ascend-MPP-Idle-Percent	[ ] (integer)	254	Idle Pct

A

Access Request attributes 1-8
access response attributes 1-8
Access-Request packet 1-8
Access-Terminate-Session packets (RADIUS code 31) 1-29
Acct-Authentic (Attribute 45) 2-13
Acct-Delay-Time (Attribute 41) 2-12
Acct-Input-Octets (Attribute 42) 2-12
Acct-Input-packets (Attribute 47) 2-13
Acct-Output-Octets (Attribute 43) 2-12
Acct-Output-packets (Attribute 48) 2-14
Acct-Session-Id (Attribute 44) 2-13
Acct-Session-Time (Attribute 46) 2-13
Acct-Status-Type (Attribute 40) 2-12
ACE keyword password 1-16
ACE users 2-20
action parameter in filters 1-23
Ascend Frame Relay (attributes 219, 220, 221) 2-28
ascend keyword passwords 1-12
Ascend-Authen-Alias (Attribute 203) 2-22
Ascend-Callback (Attribute 246) 2-33
Ascend-Call-Filter (Attribute 243) 2-30
Ascend-CLID keyword password 1-14
Ascend-Connect-Progress (Attribute 196) 2-19
Ascend-Connect-Progress values 2-19
Ascend-Data-Filter (Attribute 242) 2-30
Ascend-Data-Rate (Attribute 197) 2-20
Ascend-Disconnect-Cause (Attribute 195) 2-17
Ascend-First-Dest (Attribute 189) 2-16
Ascend-FR-Direct (Attribute 219) 2-28
Ascend-FR-Direct-DLCI (Attribute 221) 2-29
Ascend-FR-Direct-Profile (Attribute 220) 2-29
Ascend-Handle-IPX (Attribute 222) 2-29
Ascend-Home-Agent-IP-Addr (Attribute 183) 2-14
Ascend-Home-Agent-Password (Attribute 184) 2-15
Ascend-Home-Agent-UDP-Port (Attribute 186) 2-15
Ascend-Home-Network-Name (Attribute 185) 2-15
Ascend-IP-Direct (Attribute 209) 2-25
Ascend-IP-Direct attribute 1-20
Ascend-IPX-Alias (Attribute 224) 2-30
Ascend-Maximum-Time (Attribute 194) 2-17
Ascend-Menu-Item (Attribute 206) 2-24
Ascend-Menu-Item attribute 1-19
Ascend-Menu-Selector (Attribute 205) 2-23
Ascend-Menu-Selector attribute 1-19
Ascend-Multilink-ID (Attribute 187) 2-15
Ascend-Netware-timeout (Attribute 223) 2-29
Ascend-Number-Sessions (Attribute 202) 2-22
Ascend-Number-Sessions attribute 1-29
Ascend-Num-In-Multilink (Attribute 188) 2-16
Ascend-PPP-Address (Attribute 253) 2-33
Ascend-PPP-Asynch-Map attribute 1-19
Ascend-PPP-Async-Map (Attribute 212) 2-26
Ascend-PPP-VJ-1172 (Attribute 211) 2-26
Ascend-PPP-VJ-1172 attribute 1-19
Ascend-PPP-VJ-Slot-Comp (Attribute 210) 2-26
Ascend-PPP-VJ-Slot-Comp attribute 1-19
Ascend-Pre-Input-Octets (Attribute 190) 2-16
Ascend-Pre-Input-packets (Attribute 192) 2-17
Ascend-Pre-Output-Octets (Attribute 191) 2-16
Ascend-Pre-Output-packets (Attribute 193) 2-17
Ascend-PreSession-Time (Attribute 198) 2-20
Ascend-PW-Expiration (Attribute 21) 2-8
Ascend-PW-Lifetime (Attribute 208) 2-24
Ascend-Receive-Secret (Attribute 215) 2-27
Ascend-Receive-Secret attribute 1-16
Ascend-Require-Auth (Attribute 201) 2-21
Ascend-Route-IPX (Attribute 229) 2-30
Ascend-Send-Secret (Attribute 214) 2-27
Ascend-Session-Timer packets (RADIUS code 33) 1-29
Ascend-Third-Prompt (Attribute 213) 2-27
Ascend-Third-Prompt attribute 1-19
Ascend-Token-Expiry (Attribute 204) 2-22
Ascend-Token-Idle (Attribute 199) 2-20
Ascend-Token-Immediate (Attribute 200) 2-20
ASCII users file, running daemon with 1-4
async control character map 1-19, 2-26
attributes
    Access-Request 1-8
    Access-Response 1-8
    Ascend-IP-Direct 1-20
    Ascend-Number-Sessions 1-29
    Ascend-Receive-Secret 1-16
    defined only in Ascend RADIUS dictionary 1-9
    frame relay operation 2-28
    Framed-Protocol 1-20
    Framed-Route 1-13, 1-14
    listing of RADIUS 2-2
    Login Service 1-18
    parameters and analogous 2-34
    RADIUS 1-8
    RADIUS accounting 1-27
    User-Name 1-11
    User-Service 1-17
    VJ compression 2-26
authentication
    ACE 2-27
    CACHE-TOKEN 1-16, 2-27
    CLID 1-14
    for multiple users 1-16
    PAP-TOKEN-CHAP 1-16, 2-28
    password for CLID 1-14
    passwords for external 1-15
    RADIUS supported 1-2
    reporting time of 2-20
    SAFEWORD 2-27
    specifying additional 2-21

authentication (*continued*)
- specifying incoming call 2-13
- user name for CLID 1-11
- value of Class 2-11

B

banner profile 1-12
billing information 1-26
bridging
- NCP watchdog requests during IPX 2-29
- numeric string identified with 2-13

bridging configuration 1-22
builddbm, options 1-6

C

CACHE-TOKEN authentication 1-16, 2-27
call filters 2-30
callback 2-33
called-party number 2-11
Caller-Id (Attribute 31) 2-11
calling-party number 2-11
calls
- authentication for incoming 2-13
- billing for 1-26
- defining protocol associated with 1-20
- defining type of service for 1-17
- reporting authentication completion of 2-20
- See also authentication
- specifying additional authentication for 2-21

CHAP-Password (Attribute 3) 2-2
Class (Attribute 25) 2-11
CLID authentication
- need for additional 2-21
- passwords for 1-14
- user name for 1-11

Client-Port-DNIS (Attribute 30) 2-11
clients file 1-7
configuration
- bridging 1-22
- for subset of terminal server commands 1-19
- IPX routing 1-22

connection
- specifying data rate of 2-20
- specifying reason for disconnecting 2-17
- specifying state of 2-19

Connection Profiles
- defining call filters for 2-30
- defining data filters for 2-30
- IPX Alias# parameter in 2-30

control character map 1-19

D

data filters 2-30
DBM mode 1-6
default profile 1-14
dialin user 1-17
dialout user 1-13
Dialout-Framed-User service 1-17
dir parameter in filters 1-23
dynamic IP address assignment 1-20

E

encrypted password 2-27
Ethernet interface internal number 2-10
expired passwords 1-16

F

filters
- defining 1-23
- described 1-22
- example for IP and ARP packets 1-24
- example generic 1-24
- example IP filter 1-22
- generic 1-24
- IP 1-22
- specifying direction of packets 1-23
- specifying whether to forward or drop packets 1-23

frame relay operation attributes 2-28
framed protocol specification 2-4
framed user service 2-3
Framed-Address (Attribute 8) 2-5
Framed-IPX-Network (Attribute 23) 2-10
Framed-Protocol (Attribute 7) 2-4
Framed-Protocol attribute 1-20
Framed-Route (Attribute 22) 2-9
Framed-Route attribute 1-13, 1-14
Framed-User service 1-17

G

gateway (nonzero) IP address 1-21
generic filters 1-24
generic keyword in filters 1-24

H

hand-held security cards
- lifetime of 2-22

host specification 2-5

I

incoming calls
- specifying authentication 2-13

incoming phone number 1-11
IP addresses
- assigning dynamically 1-20
- defining pools of 1-13

IP addresses (*continued*)
- identifying 2-2
- recording destination of packet 2-16
- redirecting user packets 2-25
- reported to calling unit 2-33
- specified for redirected IP packets 1-20
- specifying 2-9
- specifying MAX 2-2, 2-11
- specifying user 2-5

IP filters 1-22

ip keyword in filters 1-23

IPX Alias# parameter 2-30

IPX bridging 2-29

IPX routing
- allowed for users file entry 2-30
- response to NCP watchdog requests 2-29

IPX routing configuration 1-22

L

Login-Host (Attribute 14) 2-5

Login-Service (Attribute 15) 2-6

Login-Service attribute 1-18

Login-TCP-Port (Attribute 16) 2-7

Login-User service 1-17

M

Multilink bundle 2-16

multiple user authentication 1-16

N

NAS-Identifier (Attribute 4) 2-2

NAS-IP-Address (Attribute 32) 2-11

NAS-Port (Attribute 5) 2-3

NCP watchdog requests
- setting response time 2-29
- specifying response to 2-29

O

octets
- pre-authentication input 2-16
- pre-authentication output 2-16
- received during session 2-12
- sent during session 2-12

options for creating indexed users file 1-6

options for running RADIUS daemon 1-5

outdial users proifle 1-13

P

packets
- Access-Terminate-Session 1-29
- Ascend-Session-Timer 1-29
- IP address for redirected 1-20

packets (*continued*)
- pre-authentication input 2-17
- pre-authentication output 2-17
- received during session 2-13
- sent during session 2-14
- specifying IP address for user 2-25
- transmitted over static routes 1-21

PAP-TOKEN-CHAP authentication 1-16, 2-28

parameters
- analogous attributes and 2-34
- attributes and analogous 2-36
- IPX Alias# 2-30

passwords
- ACE 1-16, 2-27
- encrypted 2-27
- establishing RADIUS treatment of 2-20
- expiration of 1-16
- for CLID authentication 1-14
- for external authentication 1-15
- for pseudo-user profiles 1-12
- in a profile 1-14
- RADIUS client password 1-7
- SAFEWORD 1-16, 2-27
- specifying expiration for 2-8
- specifying lifetime of 2-24
- UNIX 1-15
- verifying 2-27

phone numbers
- specifying called-party 2-11
- specifying calling party 2-11

pools-name profile 1-13

port
- specifying connection to 2-7
- specifying user 2-3

PPP authentication 2-22

PPP encapsulation 1-20

PPP sessions
- async control character map for 2-26

profiles
- banner 1-12
- configured for subset of terminal server commands 1-19
- default user 1-14
- dialout 1-13
- enabling IPX routing 1-22
- outdial users 1-13
- passwords in 1-14
- pools-name 1-13
- pseudo-user 1-12
- route-n 1-13
- turning off IPX/IP routing 1-22
- user name in 1-11

prompts 1-20
- specifying additional 2-27

prompts 1-20 (*continued*)
- string for user input 2-23

pseudo-user profiles 1-12

R

RADIUS
- attributes listed 2-2
- configuration in the MAX 1-3
- installing and integrating 1-3
- requirements for using with MAX 1-2
- services provided by 1-2

RADIUS accounting
- attributes for 1-27
- described 1-25
- example records 1-25
- setting up 1-26
- support for 1-2
- when to use 1-26

RADIUS attributes 1-8

RADIUS clients file 1-7

RADIUS daemon
- extensions for custom 1-28
- options 1-5
- run in DBM mode 1-6
- run with ASCII users file 1-4
- same date as dictionary 1-3
- started in DBM mode 1-7

RADIUS dictionary
- Ascend attributes defined in 1-9
- default location 1-3
- described 1-3
- filter strings 1-22
- how daemon reads 1-3
- Livingston attributes defined in 1-8
- same date as daemon 1-3
- specifying a new location 1-5

Reply Messages
- customizing 2-8

Reply-Message (Attribute 18) 2-7

Reply-Message attribute 1-19

route-n profile 1-13

routing
- NCP watchdog requests and IPX 2-29
- numeric string identified with 2-13
- start packets sent 2-12
- stop packets sent 2-12
- users file entry allowed IPX 2-30

S

SAFEWORD authentication 2-27

SAFEWORD keyword password 1-16

SAFEWORD users 2-20

security cards
- lifetime of hand-held 2-22

Sess Timer 1-29

sessions
- attributes listed for 1-8
- login service for terminal server 1-18
- RADIUS supported authentication for 1-2

slot compression 1-19
- determining use of 2-26

spoofing 2-29

static IP routes 1-13, 1-21

static routes, adding 2-9

syntax
- for generic filter 1-24
- for IP filter 1-23
- for users file 1-11

T

TCP-Clear 1-18

Telnet setting 1-18

terminal server sessions
- additional options for 1-19
- allowing subset of commands 1-19
- indicating seconds logged in 2-13
- login service for 1-19
- numeric string identified with 2-13
- packets received during 2-13
- packets sent during 2-14
- specifying maximum time of 2-17

terminal service specification 2-6

token life 2-20

U

UNIX keyword password 1-15

Unspecified service 1-18

user input prompt 2-23

user name
- for CLID authentication 1-11
- in profile 1-11

user profile menu 2-24

User-Name (Attribute 1) 2-2

User-Name attribute 1-11

User-Password (Attribute 2) 2-2

users file
- creating indexed version of 1-6
- running daemon with ASCII 1-4
- session attributes listed 1-8
- setting up RADIUS 1-7
- specifying static IP route for 1-21
- syntax 1-11

User-Service
- specifying type of 2-3

User-Service (Attribute 6) 2-3

User-Service attribute 1-17

V

VJ compression 1-19
VJ compression attributes 2-26